



ROYAL KNIGHTS TECHS

CODING SUCCESS. ONE BYTE AT A TIME

FREE AUDIT GUIDE

Is Your IT Provider Actually Doing Their Job?

The Quick-Check Audit Across the 4 Areas That Matter Most

20+
Checks

4
Key Areas

10 min
To Complete

Free
Guide

Why This Guide Exists

Most small business owners trust their IT provider completely — because they have to. But blind trust is dangerous. Many businesses are paying for services they're not fully receiving, and only find out when something goes seriously wrong.

This guide gives you 20 targeted questions across the 4 areas where IT providers most commonly fall short. No technical knowledge required — just ask the questions and score the answers.

60%

of businesses hit by a major breach close
within 6 months

43%

of cyberattacks target small businesses

\$200K+

average ransomware cost for a small
business

How to Use This Guide

For each question, mark Yes, No, or N/A in the Status column. Use the Notes column to record specifics. Tally your score at the end using the scoring table. If your provider can't answer a question — that itself is a red flag.

01 Cybersecurity & Data Protection

Is your business actually protected from threats?

Cybersecurity is the #1 responsibility of any IT provider — and the area most likely to be glossed over with vague promises. These five questions cut through the noise.

Cybersecurity Checklist	Status	Notes
Is multi-factor authentication (MFA) enabled on all critical accounts? Email, remote access, cloud services, and all admin accounts. Non-negotiable.	☐ Yes ☐ No ☐ N/A	
Are employee devices protected with business-grade endpoint security? Consumer antivirus is not sufficient. Ask for the product name and vendor.	☐ Yes ☐ No ☐ N/A	
Have you had a written cybersecurity risk assessment in the last 12 months? A real assessment produces a written report with findings — not just a conversation.	☐ Yes ☐ No ☐ N/A	
Is your team receiving regular phishing/security awareness training? At minimum, simulated phishing tests once per quarter.	☐ Yes ☐ No ☐ N/A	
Do you have a documented incident response plan? Ask: 'What happens if we get hit with ransomware tomorrow?' They need a written answer.	☐ Yes ☐ No ☐ N/A	

■ Red Flags

- They can't name the specific security tools running on your systems
- You've never received a security report or risk assessment
- No MFA on email or remote access

02 Backup & Disaster Recovery

Could your business survive a major data loss event?

Many businesses believe they have backups — only to discover during a crisis that the backups were incomplete, corrupted, or had never been tested.

Backup & Recovery Checklist	Status	Notes
Do you know exactly what data is backed up and how often? Get a written list. 'Everything' is not an acceptable answer.	☐ Yes ☐ No ☐ N/A	
Are backups stored in at least two locations, including off-site or cloud? The 3-2-1 rule: 3 copies, 2 media types, 1 off-site.	☐ Yes ☐ No ☐ N/A	
Have backups been successfully restored in the last 90 days? A backup that has never been tested is not a real backup. Ask for written test results.	☐ Yes ☐ No ☐ N/A	
Do you know your Recovery Time Objective — how fast you'd be back up? If they can't give you a specific timeframe, your recovery plan doesn't exist.	☐ Yes ☐ No ☐ N/A	
Are backups encrypted and access-controlled? Backup data is a prime attack target — it must be protected too.	☐ Yes ☐ No ☐ N/A	

■ Red Flags

■	Backups have never been tested or restored
■	No off-site or cloud copy of your data exists
■	They can't tell you how long recovery would take

03 Monitoring & Maintenance

Are they fixing problems before you notice them?

A reactive IT provider only shows up when things break. A good IT provider monitors constantly and resolves issues before they ever affect your business.

Monitoring & Maintenance Checklist	Status	Notes
Are your systems monitored 24/7 with automated alerting? Ask what tool they use and what triggers an alert. Request a sample alert report.	☐ Yes ☐ No ☐ N/A	
Are OS and software patches applied within 30 days of release? Unpatched systems are the #1 attack vector. Ask for a patch compliance report.	☐ Yes ☐ No ☐ N/A	
Do you receive a monthly report on the health of your systems? If you've never seen a report, you don't know what's happening on your network.	☐ Yes ☐ No ☐ N/A	
Is there a documented asset inventory of all hardware and software? Your IT provider should know every device on your network — and so should you.	☐ Yes ☐ No ☐ N/A	
Are end-of-life systems flagged and planned for replacement? Outdated hardware and software are known security and reliability risks.	☐ Yes ☐ No ☐ N/A	

■ Red Flags

☐ You only hear from your IT provider when something breaks
☐ You've never received a health or maintenance report
☐ They don't have a current inventory of your devices

04 Communication & Reporting

Are you being kept informed and treated as a priority?

Poor communication is the top complaint small business owners have about IT providers. You shouldn't need to chase your IT team for updates or answers.

Communication Checklist	Status	Notes
Do you have a dedicated point of contact at your IT provider? You should know who to call and have a direct line — not just a generic helpdesk.	☐ Yes ☐ No ☐ N/A	
Are support tickets tracked with visible status and resolution times? Ask for a 90-day report showing average ticket resolution times.	☐ Yes ☐ No ☐ N/A	
Do you have at least quarterly IT strategy meetings? These should cover upcoming projects, risks, and 12-month technology planning.	☐ Yes ☐ No ☐ N/A	
Are major incidents communicated in real time with clear updates? You shouldn't find out about outages hours later. Ask about their comms protocol.	☐ Yes ☐ No ☐ N/A	
Is planned maintenance communicated and scheduled with your approval? Any maintenance causing downtime should be agreed in advance — never a surprise.	☐ Yes ☐ No ☐ N/A	

■ Red Flags

- You find out about outages and issues after the fact
- No regular meetings to discuss your IT strategy or roadmap
- Ticket resolution is slow with no visibility into progress

Scoring Your IT Provider

Count your 'Yes' answers across all four checklists (20 questions total).

Score	Rating	What It Means
17–20	Excellent ✓	Your provider is performing at a high standard. Keep auditing annually.
12–16	Good	Notable gaps exist. Schedule a meeting to address each 'No' answer with a clear deadline.
7–11	Average	Significant gaps. Your business faces real risk. Demand a remediation plan — or evaluate alternatives.
Below 7	Poor ✗	Your provider is falling far short. Seek an independent IT assessment immediately.



ROYAL KNIGHTS TECHS

CODING SUCCESS. ONE BYTE AT A TIME

Ready for a Free IT Assessment?

If this audit has raised concerns, Royal Knights Techs offers a free, no-obligation IT assessment for small businesses — covering all four areas with a full written report and a clear action plan tailored to your business.

Book your free assessment today — no commitment, no sales pressure.

www.royalknightstechs.com

© 2025 Royal Knights Techs · Coding Success, One Byte at a Time · Share freely.