FREE CHECKLIST

The IT Health Checklist

Ten systems every small business should be able to prove are working — and the red flag that tells you one isn't. Score yourself in fifteen minutes.

Most IT problems are not surprises. They are known weaknesses that nobody owned. This checklist covers the ten areas that account for the large majority of avoidable outages, data losses and security incidents in businesses under 100 staff.

> **How to use it.** Walk each row with whoever handles IT. Mark it **Yes** only if you can show evidence today — a report, a screenshot, a document. "I think so" counts as No. Total your Yes answers at the end.

The ten systems

System	What good looks like	Check how often	Red flag
1. Backups	Backup job completed in the last 24h; last successful restore test within 90 days.	Weekly check, quarterly restore test	A green job report nobody has ever restored from.
2. Patching	OS and third-party apps patched within 30 days of release; no unsupported OS versions in use.	Monthly	Any machine more than two patch cycles behind.
3. Endpoint protection	Every laptop, desktop and server reports into one console, and someone reads the alerts.	Weekly	Devices showing as 'not seen in 30 days'.
4. Identity and access	MFA on email, VPN and finance systems; a written joiner/leaver process.	Monthly	A leaver's account still active a week after they left.
5. Email security	SPF, DKIM and DMARC published and enforced; external-sender warnings on.	Quarterly	DMARC set to p=none and never revisited.
6. Network edge	Firewall firmware current, admin password rotated, remote access restricted by rule.	Quarterly	RDP or a management port exposed straight to the internet.
7. Asset inventory		Quarterly	

	One list of every device, its owner, its warranty date and its role.		Discovering devices during an incident that nobody knew existed.
8. Licensing and subscriptions	A list of every SaaS subscription, its seat count and its renewal date.	Quarterly	Paying for seats belonging to people who left.
9. Documentation	Network diagram, admin credentials in a vault, and a runbook for the top five failures.	Twice a year	The only person who knows how it works is on holiday.
10. Vendor and support cover	A named support path for each critical system with a response time in writing.	Annually	"We'll call the guy who set it up" as a disaster recovery plan.

Score yourself

One point per row you can evidence today. Ten points available.

Score	What it means	What to do first
9-10	Well run. Your exposure is in the detail — restore testing and leaver process are the usual survivors.	Book a restore test and a quarterly review. Stop there.
6-8	Reasonable, with gaps that will bite under pressure. Typically documentation, licensing and identity.	Fix identity first (MFA and leaver process). It is cheap and it is the common entry point.
3-5	Fragile. You are relying on nothing going wrong, and on one person's memory.	Backups and patching, in that order. Then write the network diagram down.
0-2	Exposed. An incident here is likely to be a business event, not an IT event.	Treat it as a project, not a to-do list. Get an inventory before anything else.

My score: _____ / 10 **Date:** _____

The three rows I marked No that worry me most:

1. _____
2. _____
3. _____

The order to fix things in

1. **Know what you have.** An inventory takes a day and makes every other fix cheaper.
2. **Make recovery real.** A tested restore beats a better backup product.
3. **Close the front door.** MFA everywhere, and a leaver process that actually runs.
4. **Get current.** Patch the estate and retire anything unsupported.
5. **Write it down.** Diagram, credentials in a vault, runbook for the top five failures.

> Working through this and finding more No answers than you expected? Our **IT Health & Risk Assessment** scores the same ground in depth across six domains, with a prioritised 90-day roadmap — and the fee is credited against any managed service you start within 30 days.
>
> eversourceitservices.com/it-health-risk-assessment/

EverSource IT Services · Dallas-Fort Worth · connect@eversourceitservices.com · This checklist is general guidance, not a security assessment of your specific environment.