IT HEALTH ASSESSMENT

The 12-Point IT Health Check

The same checklist we run on every new client network. Score your own setup in about 15 minutes and see exactly where the gaps are before they cost you a day of downtime.

01	**Backup and recovery questions most owners never ask**
02	**The 4 security gaps we find on nearly every unmanaged network**
03	**A simple scoring sheet to prioritise what to fix first**

Use this guide to assess where you are, identify the evidence you need, and turn the biggest gaps into a practical action plan.

Prepared by Brotherly Technology
Owner-led IT, security, and compliance support.

15-MINUTE ASSESSMENT

Start with the current state

Mark each item Yes, Partial, or No. A written policy only counts as Yes when the process is operating and you can show evidence.

[ ] Inventory: devices, users, software, vendors, licenses, and warranties are current.	[ ] Yes [ ] Partial [ ] No
[ ] Identity: every person has a unique account, MFA, and role-appropriate access.	[ ] Yes [ ] Partial [ ] No
[ ] Patching: supported operating systems, apps, firmware, and network devices are updated.	[ ] Yes [ ] Partial [ ] No
[ ] Endpoints: managed protection, encryption, screen lock, and device health reporting are active.	[ ] Yes [ ] Partial [ ] No
[ ] Email: anti-phishing controls, domain authentication, and suspicious-message reporting work.	[ ] Yes [ ] Partial [ ] No
[ ] Network: firewall, Wi-Fi, guest access, remote access, diagrams, and configuration backups are managed.	[ ] Yes [ ] Partial [ ] No
[ ] Backup: all critical onsite and cloud data is included, monitored, isolated, and retained.	[ ] Yes [ ] Partial [ ] No
[ ] Recovery: a documented restore test has proven the agreed RTO and RPO.	[ ] Yes [ ] Partial [ ] No
[ ] Monitoring: outages, capacity, security events, and failed jobs create owned alerts.	[ ] Yes [ ] Partial [ ] No
[ ] Support: users know how to get help and urgent issues have an escalation path.	[ ] Yes [ ] Partial [ ] No
[ ] Vendors and compliance: contracts, security responsibilities, BAAs, and evidence are tracked.	[ ] Yes [ ] Partial [ ] No
[ ] Continuity: incident, outage, and vendor-failure plans have owners and exercise dates.	[ ] Yes [ ] Partial [ ] No

Quick score: Yes = 2, Partial = 1, No = 0. Start with any No that could stop work, expose sensitive data, or create an avoidable contract cost.

SCORING

Use evidence to set priorities

Score each point 0 for absent, 1 for partial, and 2 for operating with evidence. Then apply business impact before choosing the work order.

Score	Meaning	Next move
20-24	Strong baseline	Close remaining exceptions and schedule recurring tests
14-19	Material gaps	Assign owners to No items and validate Partial items
8-13	High exposure	Address identity, backup, recovery, patching, and incident response first
0-7	Immediate risk	Stabilize critical systems and obtain qualified help
Any score	One critical No can outweigh the total	Prioritize by downtime, data, safety, compliance, and cost

Do not average away a critical failure. A score of 22 with an untested backup may be less resilient than a score of 17 with proven recovery.

BROTHERLY TECHNOLOGY

COMMON FINDINGS

Fix the four gaps we see repeatedly

These controls often look complete until someone asks for coverage reports, settings, or a real test.

1	MFA coverage: export a user-by-application report and close service-account, legacy-authentication, and exception gaps.
2	Administrator rights: separate daily and admin identities, reduce membership, and review privileged access.
3	Patch coverage: include third-party apps, firmware, network devices, and machines that rarely connect.
4	Recovery proof: restore an application in isolation and have a business user validate the result.
5	Re-score quarterly and after major hires, locations, migrations, applications, incidents, or vendor changes.

What to watch for

WATCH: A control is marked Yes because a product was purchased, not because coverage is proven.

WATCH: Nobody owns failed alerts or exceptions.

WATCH: The inventory omits cloud apps, shared accounts, and personally owned devices.

WATCH: The score is never reviewed with business leadership.

WATCH: Backup success is assumed from green status lights.

MAKE IT ACTIONABLE

Turn the worksheet into a 30-day plan

Do not try to solve everything at once. Assign one owner, one next action, and one date for each priority.

NOW	Name the owner and confirm the current state.	____________________
NEXT 7 DAYS	Fix the highest-risk gap or gather the missing evidence.	____________________
NEXT 30 DAYS	Complete the remaining quick wins and set review dates.	____________________
NEXT QUARTER	Test the process, document results, and assign improvements.	____________________

Notes / decisions / questions for your provider

____

____

____

____

____

Want a second set of eyes? Book a free consultation at brotherlytechnology.com/contact/ or call 404-907-1005.