FREE RESOURCE · DATA SECURITY STRATEGIST

IT Assessment Quick-Start

A fill-in form for your tech setup

Find gaps before they become outages or surprise costs.
About 45–90 minutes the first time.

Andre Brown · andrenbrown.com
Secure · Connect · Optimize

Who this is for

If you run a business (or help run the tech) and want a clear picture of your setup — before something breaks, an audit lands, or a surprise bill shows up — this workbook is for you. You don't need to be a tech expert. Fill in what you know. Leave blank what you don't.

How to use it

1. **Gather** — Section 1 with whoever knows your systems. 2. **Scan** — Section 2 for common weak spots. 3. **Write it down** — Section 3 findings. 4. **Choose** — Section 4 what to fix first.

Section 1 — Before you dig in

A. What you have

Item	Have it? (Yes / No / Partly)	Notes
List of main computers and servers (name, system type, rough age)		
How people connect (office network, Wi■Fi, work-from-home, cloud)		
Who can log into the firewall or main router (and where that password lives)		
List of cloud accounts (Microsoft 365, Google, Azure, AWS, and so on)		
Your website domain and where it's registered		
List of must-have apps (email, accounting, CRM, industry software)		

B. People and logins

Item	Have it?	Notes
Who uses your systems (or roughly how many people)		
Who has "full control" admin rights (real names)		
What happens to logins when someone leaves		

Item	Have it?	Notes
Shared passwords or shared logins? (Yes/No)		
Extra login step (MFA / authenticator app) on email and important apps?		

C. Backups

Item	Have it?	Notes
What gets backed up (files, servers, cloud, email)		
How often backups run		
Where backups are stored (on-site, cloud, or both)		
Last time you tested putting a file or system back from backup		
Who to call if everything is down tomorrow morning		

D. Basic security habits

Item	Have it?	Notes
Computers get updates on a regular schedule		
Antivirus or similar protection is turned on		
Someone looks at odd login alerts (even once in a while)		
A short written rule for how staff handle company data		
Any rules you must follow (insurance, customer forms, industry rules)		

E. Business snapshot

Question	Your answer
Biggest tech headache right now?	

Question	Your answer
What must keep working for the business to run?	
Rough spend on tech (tools, people, vendors)?	
Any audit, insurance, or customer security form coming up?	
Comfortable budget for a focused fix in the next 1–3 months?	

Section 2 — Ten common weak spots

For each row, mark **OK**, **Weak**, or **Don’t know**. Be honest — “Don’t know” is better than a lucky guess.

#	Weak spot	Why it matters	Your rating	Short note
1	Updates not applied	Old software fails more and is easier to break into		
2	Backups never tested	Having a backup is not the same as being able to restore		
3	Too many admins or shared admin logins	One stolen password can unlock almost everything		
4	No extra login step on email or remote access	Stolen passwords still cause many break-ins		
5	Apps nobody officially tracks	Company data can sit in tools you don’t manage		
6	Only one person knows how things work	Vacation, illness, or turnover can stop the business		
7	No clear list of what you own	Hard to protect or budget for what you can’t name		
8	Alerts that nobody reads	Warnings don’t help if no one checks them		
9	Old accounts still active (ex-staff, old vendors)	Forgotten access is an open door		
10	Spreadsheets acting as the “real” system	Easy to mess up versions and lose a clear history		

Quick score: Count Weak + Don’t know. 0–2: keep what works and write it down. 3–5: make a short fix list. 6+: fix only the top three first.

Your score

Section 3 — Write your findings

Short summary (3–5 sentences)

What did you learn about uptime, who has access, backups, and data risk?

Critical — fix or contain within a few days

Finding	What happens if you ignore it?	First fix to try	Who owns it?

High — handle within 30 days

Finding	What happens if you ignore it?	First fix to try	Who owns it?

Medium — plan for this quarter

Finding	What happens if you ignore it?	First fix to try	Who owns it?

What’s already working

Section 4 — What to do first

Score each Critical or High finding from 1 to 5. Do the high-value or high-risk items that are easier first.

Finding	Lowers risk?	Helps soon?	Effort (1=easy, 5=hard)	Do this first?

Your 30-day action list

Week	Action	Done?
Week 1		☐
Week 2		☐
Week 3		☐
Week 4		☐

Section 5 — Next steps

Do it yourself

- Finish Sections 1–4.
- Fix the top 1–3 Critical items you can safely handle.
- Schedule a backup restore test.
- Write down who has admin rights and remove one unused login.
- Open this workbook again in 90 days.

When to get help

- You’re not sure what is urgent vs. noise
- Changing access, backups, or security feels risky to do alone
- You need a clear write-up for leadership, insurance, or a customer
- You want someone to implement the fixes, not only list them

Ready for a guided assessment?

IT Management & Assessment · andrenbrown.com · Start your project