

Small Business Tech Risk Checklist

A 10-minute self-assessment of where your business is exposed

[Free Checklist](#)

Small Business Consulting Suite · smallbusinessconsultingsuite.com

Contents

1. How to Use This Checklist
2. Account Security & Access Control
3. Backups & Recovery
4. Updates, Patching & Devices
5. Vendor, SaaS & AI Tool Risk
6. Incident Basics & Your Score

How to Use This Checklist

Every growing business now runs on technology it doesn't fully control — vendors, cloud tools, AI features, and third-party platforms that can fail, get breached, or change terms without warning. This checklist gives you a fast, honest read on where your business is exposed. Set aside about 10 minutes, answer from how things actually work today (not how they're supposed to work), and be strict: a partial “sort of” counts as **No**.

What the columns mean

Column	How to fill it in
Sev (severity)	Pre-filled: H igh, M edium, or L ow — how much a gap here typically hurts a small business.
Status	Write Y (yes, true today), N (no), or ? (don't know — treat as N when scoring).
Notes	Who owns it, what tool is involved, or what you'd need to check.

The five areas you'll assess

- Account security & access control — who can get into what
- Backups & recovery — whether you could get your data back
- Updates, patching & devices — whether known holes stay open
- Vendor, SaaS & AI tool risk — what breaks when someone else fails
- Incident basics — what happens in the first hour of a bad day

These roll up to the six risk dimensions from our free scorecard: vendor & third-party exposure, data & privacy, cyber & ransomware, operational continuity, AI & automation, and regulatory & compliance risk. The final page turns your answers into a score.

This checklist is an educational self-assessment from Small Business Consulting Suite. It is not a formal risk audit, insurance coverage review, or legal/compliance opinion, and it does not evaluate any specific insurance policy or coverage need.

Account Security & Access Control

Most small-business incidents start with an account, not a server: a reused password, a shared login, or an ex-employee who could still get in. Mark each statement Y, N, or ?.

Check	Sev	Status	Notes
Multi-factor authentication (MFA) is turned on for email, banking, and your main business apps	H		
Every person has their own login — no shared accounts for email, CRM, or admin panels	H		
A password manager is in use; passwords are unique per site, not reused	M		
Someone maintains a list of who has admin rights on each critical system	M		
Access is removed the same day when an employee or contractor leaves	H		
Owner/admin accounts are separate from everyday working accounts	M		
Bank and payment-platform access is limited to the few people who truly need it	H		
Third parties (bookkeeper, agency, IT) have their own named accounts you can switch off	M		

If you marked N or ?

Start with MFA on email and banking — email is the master key to password resets everywhere else. Then close out departed-user access: list everyone who has left in the last two years and confirm each account is disabled.

Backups & Recovery

A backup you have never restored is a hope, not a plan. This section checks whether your data would survive ransomware, a deleted account, or a failed laptop — and how fast you'd be back.

Check	Sev	Status	Notes
You can name where every kind of critical data lives (files, accounting, CRM, email)	M		
Backups run automatically — no one has to remember to do them	H		
At least one backup copy is separate from your main systems (different account or provider)	H		
Cloud app data (e.g. accounting, CRM) is exported or backed up, not just “in the cloud”	M		
A test restore has actually been performed in the last 90 days	H		
You know roughly how long a full recovery would take, and who would do it	M		
Backups reach back far enough to survive a problem discovered weeks later (not just yesterday)	M		
Laptops and phones that hold business data are encrypted and backed up	L		

If you marked N or ?

The single highest-value move: schedule a 30-minute test restore this month. Pick one important file and one system, restore them to a spare location, and time it. Most gaps show up in the first attempt.

Updates, Patching & Devices

Attackers mostly reuse old, well-known holes. Keeping software current is unglamorous and cheap — and it removes a large share of realistic risk for a small business.

Check	Sev	Status	Notes
Operating systems on all work computers update automatically	H		
Browsers and email clients are current on every machine	M		
Website platform, plugins, and themes (if you run a site) are updated on a schedule	H		
Router / firewall firmware at the office has been updated in the last year	M		
No one is running software the vendor no longer supports (old OS, dead plugins)	H		
Antivirus / endpoint protection is on and current on every work device	M		
Personal devices used for work meet a stated minimum (passcode, encryption, updates)	M		
Someone is named as responsible for updates — it isn't “everyone”	L		

If you marked N or ?

Turn on automatic updates everywhere it's offered, then list anything that can't auto-update (website plugins, firmware, point-of-sale) and put a monthly 15-minute recurring task on someone's calendar to check them.

Vendor, SaaS & AI Tool Risk

Your risk now includes everyone else's. Ask of each tool: if it went down for 48 hours, changed its terms, or exposed our data, what would that do to us?

Check	Sev	Status	Notes
You have a written list of every vendor and SaaS tool the business depends on	M		
You know which vendors would stop revenue if they failed for 48 hours	H		
Critical vendor accounts are owned by the business (not an employee's personal email)	H		
You know which vendors hold customer data, and roughly what data	H		
You could export your data from each critical tool if you had to leave it	M		
Every AI tool that touches customer data or makes decisions for you is known and listed	M		
Staff know what may and may not be pasted into AI tools (customer data, credentials, contracts)	M		
You know which data-protection or contractual obligations apply to your customer data	M		

If you marked N or ?

Build the vendor list first — check bank and card statements for every recurring software charge; most owners find tools they'd forgotten. Star the ones that would stop revenue within 48 hours: those are the vendors worth a deeper look.

Incident Basics & Your Score

You don't need an enterprise incident-response plan — you need to not be inventing one at 7am on the day something breaks. These checks cover the first hour of a bad day.

Check	Sev	Status	Notes
Everyone knows who to tell first if they click something suspicious or lose a device	H		
Key contacts (IT help, bank fraud line, insurer, critical vendors) are written down and reachable offline	M		
Admin passwords and recovery codes are stored where a second trusted person can reach them	H		
Staff have basic guidance on spotting phishing and payment-change fraud	H		
You know how you'd operate for a day with your main system down, and how you'd tell customers	M		

Score yourself

Count each **N** or **?** on a High-severity row as a **High-exposure flag**; on Medium/Low rows, count it as a gap to schedule.

Section	Flags (High rows)	Gaps (Med/Low rows)	Your read (L/M/H)
Account security & access control			
Backups & recovery			
Updates, patching & devices			
Vendor, SaaS & AI tools			
Incident basics			
Totals			

- **0-2 flags:** solid footing — fix what you found, re-run twice a year.
- **3-6 flags:** real gaps worth mapping — do the three cheapest High-severity fixes this month.
- **7+ flags:** more exposed than most growth-stage businesses — make this a project with an owner and a deadline.

Want the fixes, not just the findings? The **SMB Technology Risk Playbook** gives you the single most useful fix for each risk dimension, each doable in under two weeks — under Tech Risk at smallbusinessconsultingsuite.com.