SUMMIT

The 5-Minute Security Gap Checklist for CPA Firms

Where are the blind spots hiding in your firm's everyday systems?

Answer each question with yes, no or not sure. Every **no** or **not sure** is a gap worth scoring on page 3. Take five minutes with it this week, ideally with whoever manages IT at your firm.

1 BLIND SPOT 1 I BACKUPS
Can we prove we can recover?

ASK YOURSELVES	YES	NO	NOT SURE
We have restored data from backup and used it this quarter.	☐	☐	☐
We know what is not in our backups today (Microsoft 365, cloud applications, laptops).	☐	☐	☐
We know how long a full restore would take in tax season, and how much data we could lose.	☐	☐	☐
At least one backup copy is offline, air-gapped or immutable (the last "1" in 3-2-1-1).	☐	☐	☐

2 BLIND SPOT 2 I ACCESS
Who can access what, and why?

ASK YOURSELVES	YES	NO	NOT SURE
Every former employee's access was removed on their last day, including tax software, client portals and remote access.	☐	☐	☐
Shared passwords (payroll, banking, portals) are rotated when someone leaves.	☐	☐	☐
Only people whose work requires it hold admin rights.	☐	☐	☐
Someone reviewed access and third-party app permissions this year, and signed off.	☐	☐	☐

3 BLIND SPOT 3 I AI TOOLS

What client information goes into AI tools?

ASK YOURSELVES	YES	NO	NOT SURE
We know which AI tools staff use with client data.	☐	☐	☐
Staff use firm-approved AI accounts, not free personal accounts.	☐	☐	☐
We have reviewed how our AI tools store and use what's entered.	☐	☐	☐
Our written security policy covers AI tools.	☐	☐	☐

4 BLIND SPOT 4 I VENDORS

Who else has access to our data?

ASK YOURSELVES	YES	NO	NOT SURE
We have a current list of vendors that hold client data.	☐	☐	☐
We know what data each vendor holds, and where.	☐	☐	☐
We know who on each vendor's side can access our data.	☐	☐	☐
Each vendor has told us how and when they'd notify us of an incident.	☐	☐	☐

5 BLIND SPOT 5 I VERIFICATION

Are our controls working?

ASK YOURSELVES	YES	NO	NOT SURE
MFA is enforced on every account, including admin accounts and older applications.	☐	☐	☐
Every device, including laptops, reports in to endpoint protection.	☐	☐	☐
A named person reviews security alerts and our IT provider's reports.	☐	☐	☐
Our Written Information Security Plan (WISP) is owned, reviewed and tested.	☐	☐	☐

ONE QUESTION TO ASK ACROSS EVERY AREA

What evidence shows this is working?

Having a control isn't the same as verifying it. Look for a tested restore, a signed-off access review or a current report, not a green checkmark.

Score and Prioritize Your Gaps

SCORE 1 (LOW) TO 3 (HIGH)

List each **no** or **not sure**. Score **Impact** (how much harm if it's exploited or fails), **Likelihood** (how likely it is to happen) and **Ease** (how quickly and affordably you can close it, where 3 is easiest). Then sort:

Fix now

High impact and high likelihood. Address these first.

Quick wins

Easy to close, even if smaller. Build momentum.

Plan it

High impact but harder to fix. Give it an owner and a date.

GAP WE FOUND	IMPACT 1–3	LIKELIHOOD 1–3	EASE 1–3	FIX NOW, QUICK WIN OR PLAN IT	OWNER	DUE

You can't address a gap you don't know exists.
Find it. Prioritize it. Verify it.

Want to go deeper?

Get practical steps for protecting client data in the cloud. Read our cloud security guide

Need help closing the gaps?

See how Summit hosts and protects your firm's applications. Explore application hosting

Tax practices are required to maintain a Written Information Security Plan (WISP) under the FTC Safeguards Rule, as the IRS reiterated in IR-2026-92 (Aug. 18, 2026). IRS Publication 5708 includes a sample WISP template.

This worksheet is general guidance, not legal advice. Confirm your firm's legal, regulatory and contractual obligations with qualified advisers.

Book a 20-minute review of what you found

Hello@SummitHQ.com →

SOC 2 TYPE 2

SUMMIT™

SummitHQ.com • **888-244-6559**