IT Compliance for CPA Firms: How to Avoid Costly Mistakes

If you lead a CPA firm, you already know this: you don't just protect your own business, you protect your clients' most sensitive financial data. That's exactly why attackers love targeting accounting firms, and it's why IT compliance for CPA firms isn't just "an IT thing." It's a leadership thing, a risk thing, and a reputation thing.

I talk with CPA firms all the time, and I see a pattern. Most firms don't *mean* to take risks. They're just busy. They're trying to get work done fast, especially during busy season. Going with the "quick and easy" choice because you're busy is often the thing that causes the biggest problems later.

Read on to learn the costliest mistakes I see, and what you can do to avoid them. No fear tactics. Just practical steps you can use.

The 3 Costliest Compliance Mistakes I See CPA Firms Make

1) No written, enforceable security program (yes, this is a big deal)

A lot of firms say, "We have IT." But "We have IT" is not the same as "We have policies, procedures, and evidence." If something goes wrong and your policies aren't written and followed, it's like they don't exist.

For CPA firms, a Written Information Security Program (WISP) is a requirement under IRS Publication 4557 and the FTC Safeguards Rule. Even if you're doing good technical work, your firm still needs the written plan.

2) Shared accounts and weak identity controls

Shared logins are common in tax software, portals, and admin tools. It feels convenient, until it isn't.

Shared accounts create two big problems:

- You can't prove who did what (that matters when something goes wrong).
- Offboarding gets messy (former employees may still have access).

Weak identity controls often show up as:

- No MFA on email or key platforms
- Loose admin access
- Inconsistent account management

3) Unmanaged remote work (especially personal devices)

Here's a common scenario: staff members connect from home on personal computers. Those devices aren't monitored. They aren't encrypted. They may have personal apps (or kids' games) right next to client data.

That's a major compliance and security risk, because you lose control of the environment where client data is being accessed.

The 5 "Non-Negotiable" Policies Every CPA Firm Should Have

If your firm wants to be serious about IT compliance, these policies are the basics. They're not fancy. They're the fundamentals that prevent expensive mistakes.

1) Access control + password policy

Access control and a strong password policy are the foundation of day-to-day security, and they're a must for compliance. Every person in the firm should have their own unique account (no shared logins, ever), so you can track activity clearly and shut off access quickly when someone leaves.

I also recommend requiring a password manager for everyone and setting a firm-wide minimum password length (I like 14+ characters) to reduce the risk of easy-to-guess or reused passwords. On top of that, multi-factor authentication (MFA) should be required anywhere it matters most, especially email (Microsoft 365 or Google Workspace), tax and accounting platforms, VPN and remote access tools, and any admin portals or client portals.

2) Endpoint + patch management policy

Endpoint and patch management is another must-have because your laptops and desktops are where daily work happens, and it's also where breaches often start.

In my view, CPA firms should require firm-owned devices only (no personal computers for client data), and every device should have full-disk encryption turned on (BitLocker is built into Windows, so there's no good reason to skip it).

Also, devices need EDR/next-gen antivirus and central management so your team can enforce security settings and confirm updates are actually happening. Set a clear patch timeline, while getting critical updates installed within 14 days is a solid baseline and goes a long way toward reducing preventable risk.

3) Incident response policy (written + practiced)

An incident response policy shouldn't be something you slap together after a scare. It should be written down, clear, and actually practiced. A strong incident response plan answers the big questions before a crisis hits: who leads the response, who communicates with clients, who works with your cyber insurer, attorney, or regulators, and exactly when client notifications should happen.

Here's the part most firms skip. You need to run at least one tabletop exercise every year to make sure the plan still works, the right people are involved, and the contact list isn't three years out of date.

4) Backup + disaster recovery policy
Backups and disaster recovery aren't optional. CPA firms need to assume ransomware is possible and plan like it could happen at the worst time (because it usually does).

A solid policy starts with the 3-2-1 backup rule, meaning you keep three copies of your data on two different types of storage, with one copy stored off-site. Just as important, at least one of those backups should be immutable or air-gapped, so ransomware can't encrypt it along with everything else.

Don't just "set it and forget it." Your firm should test restores and document the results at least quarterly, so you know the backups actually work when you need them most.

5) Acceptable use + device standards policy
This is how you stop "shadow IT," like when someone sets up a personal Dropbox because it feels faster in the moment. Your firm should have clear rules that only firm-approved tools can be used to store or transmit client data, plus minimum requirements that must be met before any device is allowed to access client information (things like encryption, EDR, and automatic screen locking).

It also helps to spell out simple guidance on printing, where documents can be printed, how physical files should be stored, and what's allowed to leave the office.

Putting together, these guardrails make daily work safer and are a big part of building a real, defensible IT compliance for your firm.

Where CPA Firms Drop The Ball (and how to fix it)

If there's one area where small gaps quickly turn into big incidents, it's email. I have noticed a few common failures repeatedly in CPA firms. The first is missing email authentication; either DKIM and DMARC aren't set up at all, or DMARC is left on "none" forever, which doesn't really protect you.

Another big issue is handling wire transfers or ACH instructions purely by email. That's a recipe for fraud when someone spoofs a client or partner and slips in new banking details. I also see firms allow external email forwarding, which is dangerous because if a mailbox gets compromised, an attacker can quietly forward messages out without anyone noticing.

The fix is to write the right best practices directly into policy, so the firm isn't relying on memory, good intentions, or "we'll deal with it if it happens." At a minimum, SPF, DKIM, and DMARC should be configured and reviewed at least annually, and external forwarding should be blocked by default. Any cloud app that supports it should require single sign-on

with MFA, and you should also have a clear procedure for bank changes and payment requests. That procedure should require out-of-band verification using a known phone number or an agreed method, not replying to the same email thread, and it should include dual approval for unusual requests or large transfers.

It also helps to give your team a simple way to respond fast: add a "Report Phish" button in Outlook and make reporting part of your culture, with the understanding that nobody gets in trouble for asking, "Is this suspicious?"

Training should be ongoing, and monthly security awareness and phishing simulations work best, especially when they look like real CPA-world scenarios (IRS notices, urgent partner messages, client portal alerts). It's a must that leadership also participates. When firm leaders bypass controls or skip training, everyone notices.

Client Data Handling: The "Easy" Mistakes That Create Huge Risk

CPA firms handle Social Security numbers, bank details, tax returns, and more. From a compliance perspective, these are the mistakes I see most often:

- Emailing full tax returns or SSNs unencrypted (because it's fast)
- Storing client data in personal OneDrive/Dropbox/USB drives
- Keeping everything forever "just in case" (over-retention increases breach impact)
- No clear rules about laptops, phones, printed copies, and what can leave the office
- Giving interns/temps broader access than they need

A simple fix is to define a data-handling process by stage:

- **Intake:** approved methods (portal, secure e-sign tools, encrypted links)
- **Processing:** approved storage locations only, least-privilege access
- **Delivery:** portal or encrypted delivery as standard
- **Retention:** clear schedule aligned with legal/regulatory needs
- **Disposal:** secure destruction and documentation

That structure makes IT compliance for CPA firms easier because it tells people exactly what to do without guessing.

Backup & Disaster Recovery: What "Audit-Ready" Looks Like

A compliant disaster recovery setup is more than "we have backups." You should have:

- Documented **RPO** (how much data can you lose) and **RTO** (how long can you be down)
- 3-2-1 backups with immutability
- Coverage of critical systems (including key cloud tools and don't assume the vendor has you covered)
- Documented restore testing (don't wait until a real incident to try your first restore)

- A disaster recovery playbook that includes:
    - who declares the disaster
    - where staff work
    - what comes back first
    - how you communicate with clients

Vendor + Cloud Management

One of the most common (and most expensive) mistakes I see is firms assuming their vendor is responsible for all security and compliance. They're not. Even if your data lives in the cloud or you use a big-name tax platform, your firm is still accountable for how client data is protected, who can access it, and what happens if there's an incident.

That's why your IT policies should spell out a simple but clear vendor management process. Start with a vendor inventory so you know exactly which tools and providers can access client data. Then tier vendors by risk (high, medium, or low) based on how sensitive the data is and how critical the vendor is to your operations. For higher-risk vendors, your policy should require due diligence, like reviewing SOC 2 Type II or ISO 27001 reports when available, using security questionnaires, and making sure breach notification terms are written into your contracts.

You should also require least-privilege access for vendors, meaning not everyone needs admin rights, and vendor staff shouldn't have global admin access unless it's truly necessary (and even then, it should be limited and tracked). Finally, build in an annual vendor review, so you're not making a one-time decision and never looking back.

A Practical 90-day Roadmap (if you're starting from scratch)

Days 1–30: Discover & stabilize

- Name an internal owner
- Map your key systems and where client data lives
- Turn on MFA everywhere immediately
- Verify backups are off-site/immutable and test a few restores
- Pick a baseline framework (IRS Pub. 4557, NIST, CIS Controls)

Days 31–60: Build the foundation

- Draft core policies (WISP, access control, remote work, data handling, backups, incident response, vendor management)
- Roll out key technical controls (managed endpoints, email protections, patch baselines)
- Start monthly awareness training and phishing simulations

Days 61–90: Operationalize & prove it

- Tighten permissions and access
- Build vendor governance

- Run a tabletop incident exercise
- Perform a documented restore test
- Set 2–3 measurable KPIs (MFA coverage, patch compliance, phishing click rate, etc.)

It Doesn't Have To Be Complicated

IT compliance for CPA firms doesn't have to be complicated, but it does have to be real. Written policies. Technical controls. Ongoing training. Testing. Documentation.

If you do those things, you dramatically reduce the chance that one "small" mistake turns into a costly breach, a client trust issue, or a regulatory headache.

If you want help building a clear plan (not a binder that gathers dust), that's exactly what my team at All in IT does.

Ready to tighten up IT compliance for CPA firms without slowing your team down? All in IT can help you build a practical, audit-ready compliance program (WISP, access controls, email security, backups, vendor risk, and more) that fits how CPA firms actually work. If you want a clear roadmap and real proof you're protected, contact us today to schedule a complimentary compliance check and next-step plan.

Matt Daniel, CEO & Founder

Matt Daniel is the Founder and CEO of All in IT, where he helps CPA firms strengthen IT compliance for CPA firms with practical, audit-ready security programs. He works with firm leaders to reduce risk around email and identity security, managed endpoints, backups and disaster recovery, and vendor oversight, so protecting client data becomes a clear, repeatable process instead of a last-minute scramble.