10-Point IT Risk Checklist for LA CPA Firms

> **A self-assessment for managing partners, firm administrators, and IT leads at CPA / accounting firms in Greater Los Angeles.** Ten questions every CPA firm should be able to answer about its IT and security posture — especially before tax season.

Author: George Bederyan · Verta IT Solutions LLC **Audience:** LA CPA / accounting firms · 5-25 staff **Use:** Self-assessment, pre-tax-season audit, vendor evaluation **Time to complete:** ~10 minutes

---

Why this checklist exists

CPA firms operate under a unique threat profile: you handle sensitive financial data for hundreds of clients, you have hard deadlines that don't move (IRS, FTB, etc.), and you become a high-value target during tax season specifically because criminals know your systems are under load and your team is stretched thin.

This checklist captures the questions a privileged client conversation would surface. Answer honestly. Where you don't know the answer, write "unknown" — that's information too.

The 10 questions

1. Tax season downtime exposure

If your case management system, M365, or accounting software goes down on March 15 at 3 PM, what's the recovery plan? How many billable hours are at risk?

Required answer: documented recovery process, primary and secondary contact for each critical system, written SLA with IT vendor for tax season response. If the answer is "we'd call our IT guy" — that's a single-point-of-failure plan that costs the firm tens of thousands in lost billable hours when (not if) it triggers.

Verta IT's recommendation: every CPA firm should have a written Tax Season Continuity Plan reviewed annually in December.

2. Client tax-data security under IRS Pub 4557

IRS Publication 4557 requires "Safeguards for Federal Tax Information" — does your firm have a written Information Security Plan (WISP) that meets the IRS's six required components?

If your answer is "we have antivirus and a password policy" — that's a partial control. IRS Pub 4557 requires specific written documentation including: - Designated security officer - Risk assessment - Safeguards inventory - Service provider oversight - Incident response procedures - Annual review

A missing WISP can expose the firm to PTIN penalties, increase audit risk, and is a documented control gap if data is breached.

3. Email security and CEO fraud

If a staff accountant received an email that looked like it was from the managing partner asking them to forward client tax returns to an outside email address, what would stop

them from doing it?

Required answer: (a) sender authentication (SPF/DKIM/DMARC), (b) anti-phishing controls in Microsoft 365 Defender or equivalent, (c) written policy that client data transfers require verbal verification.

Tax season specifically: CPA firms are the #1 target for tax-return-data theft. Business Email Compromise (BEC) targeting CPA firms doubled in tax season 2025 per FBI IC3 data.

4. Multi-factor authentication coverage

Is multi-factor authentication (MFA) required on every business login — M365, your tax software, your accounting platform, banking, e-filing portals — for every user including the managing partner?

The #1 cyber-insurance claim trigger in 2025 was a BEC on an executive who had MFA disabled "because it's annoying." If MFA isn't enforced firm-wide, your cyber insurance will likely pay less or nothing on a claim.

Plus: IRS Pub 4557 is moving toward requiring MFA on all systems handling taxpayer information. Compliance is also coming.

5. Backup and the "we lost a return" scenario

When was the last time your backup system was tested by actually restoring a workpaper, return, or mailbox — not just reading the green status indicator?

If the answer is "we've never tested it" or "I don't know" — your backup is theoretical, not actual. The risk: during tax season prep work, a workpaper system goes down, backup says it's fine, restore fails, that client's return is delayed or lost, the firm eats the staff time + the IRS penalty + the client relationship.

6. After-hours and tax-season coverage

If a ransomware attack hits your firm on April 14 at 6 PM — the day before extension deadline — who do you call? What's the response commitment?

Required: written incident response plan with named contacts, escalation paths, after-hours support arrangement specifically aware of tax-season criticality. "We'll figure it out" costs an extra day during the response window, and during tax season that day is unrecoverable.

7. Vendor and software inventory

Can you list every software application your firm pays for in the last 12 months — accounting platforms, tax prep software, document management, billing, payroll — the renewal dates, and who in the firm uses each?

Most CPA firms over-pay for software by 15-30% due to orphaned licenses (e.g., partner left, license still active), duplicate tools, and abandoned trials. An inventory typically saves $200-500/user/year. Plus: unmanaged SaaS subscriptions are an under-the-radar data exposure — a forgotten tool may still have client data in it.

8. Client data segregation and access controls

If a junior staff accountant queries your accounting platform, can they see ALL client records, or only the ones they're assigned to?

Role-based access controls are required for: (a) IRS Pub 4557 compliance, (b) general professional ethics, (c) defensible data security in the event of staff turnover or breach. If everyone has access to everything, you have an unaddressed control gap.

9. Document retention and IRS audit readiness

If an IRS audit notice arrives tomorrow requesting all firm records for a specific client back 7 years — could your firm produce them, in defensible format, within the required timeframe?

Required: documented retention policy aligned with IRS records-retention requirements (typically 7 years for client records, longer for some), M365 retention policies actually configured (not just claimed), and documented process for audit-driven record retrieval.

If retention isn't configured, you may have already deleted records the IRS expected you to preserve.

10. Cyber insurance and the policy-language audit

Read your cyber insurance application from this year. Did your firm answer "yes" to having MFA on all accounts, endpoint detection and response (EDR) deployed, backup tested in the last 90 days, written information security plan in place, and tax-season incident response procedures documented — and is each of those actually true?

Cyber insurance carriers are auditing post-claim with increasing rigor. A "yes" on the application that doesn't match reality at the time of claim is a fraud denial. The cost of a misaligned answer can be hundreds of thousands in unreimbursed breach response — at exactly the worst moment for the firm.

How to use this checklist

Score honestly: - [YES] **Yes, verified** = control is in place AND recently tested - [!] **Yes, but not tested** = control exists but you haven't validated it - [NO] **No / Unknown** = gap or you don't have visibility

A score of 7+ Yes-Verified = your firm has strong IT/security posture and is positioned well for IRS Pub 4557 compliance.

A score of 4-6 = typical small/mid-sized CPA firm. Real risk exposure exists — especially during tax season.

A score of 0-3 = high risk profile. A managed IT partner can bring you to 7+ within 90 days of onboarding, ideally before the next tax season ramp.

What Verta IT does about this list

Verta IT specializes in IT and security for LA CPA firms and law firms. We'll walk through this checklist with you on a no-cost 30-minute call — you get an honest read on where your firm sits, plus a written IRS Pub 4557 gap assessment if you want it. No pressure to engage. Most firms learn something useful regardless.

If you want that conversation:

George Bederyan Founder, Verta IT Solutions LLC - Email: george@vertait.com - Phone: (747) 444-0233 - Web: vertait.com

Sherman Oaks based. Serving Greater Los Angeles CPA practices and law firms.

This document is informational. It does not constitute legal advice, tax advice, IRS compliance attestation, or a formal IT audit. For a defensible IRS Pub 4557 WISP, engage qualified counsel for the legal and regulatory questions and a qualified IT partner for the technical controls.

— Verta IT Solutions LLC · 14320 Ventura Blvd, Unit #1093, Sherman Oaks, CA 91423