TRANSFORM 42 · IT FOR ACCOUNTING FIRMS

# 2026 IT Compliance Checklist for CPA Firms

A practical, section-by-section guide to meeting IRS, AICPA, and state board requirements — while protecting your clients and your reputation.

TRANSFORM 42 INC · MIAMI, FL · TRANSFORM42INC.COM

# Why IT Compliance Matters for Your Firm

Accounting firms manage some of the most sensitive financial data in existence — tax returns, Social Security numbers, bank accounts, payroll records. A single breach doesn't just cost money; it can end your practice.

| $4.88M | 73% | $50K+ |
| --- | --- | --- |
| AVG. COST OF A DATA BREACH (2024) | OF CPA FIRMS HIT BY PHISHING | IRS PENALTY PER VIOLATION |

In 2024, the IRS expanded its Written Information Security Plan (WISP) requirements, making it mandatory for all tax preparers — not just large firms. State boards are following suit, and cyber insurance carriers now require documented IT policies before issuing coverage.

> **This checklist covers 6 critical areas:**
>
> Data Protection & Encryption · Access Control · Network Security · Email & Phishing Defense · Backup & Disaster Recovery · Compliance Documentation

## How to Use This Checklist

Work through each section with your IT team or managed service provider. Check off items you've completed, flag gaps, and prioritize the highest-risk items first. A perfect score isn't the goal — knowing your gaps is.

# 01 Data Protection & Encryption

Client financial data must be encrypted everywhere — at rest, in transit, and on every device that touches it.

- ☐ **Full-disk encryption on all workstations and laptops** — BitLocker (Windows) or FileVault (Mac) enabled and centrally managed. Verify keys are escrowed.
- ☐ **Email encryption for client communications** — TLS 1.2+ minimum for SMTP. Use encrypted portals (e.g., ShareFile, Citrix) for tax documents — never plain email attachments.
- ☐ **File-level encryption for stored tax returns** — AES-256 on all client data at rest, including cloud storage. Verify your cloud provider's encryption certificate.
- ☐ **Encrypted file transfer portal** — Dedicated client portal for uploading/downloading sensitive documents. No Dropbox personal accounts.
- ☐ **Mobile device encryption enforced via MDM** — Every phone or tablet that accesses firm email or files must have device encryption and remote wipe capability.
- ☐ **Database encryption for practice management software** — Verify your tax prep and accounting software encrypts its database, not just the connection.
- ☐ **USB and removable media policy** — Block unauthorized USB drives. If needed for client data, require hardware-encrypted drives only.

> **IRS WISP Requirement**
>
> Section 7216 requires tax preparers to protect taxpayer data with "adequate data safeguards." The IRS specifically calls out encryption as a baseline expectation. Failure to encrypt is the #1 finding in IRS audits of small firms.

# 02 Access Control & Authentication

The principle of least privilege: every person sees only the data they need. No exceptions.

- ☐ **Multi-factor authentication (MFA) on all systems** — Email, cloud apps, VPN, practice management, tax software, and banking. SMS codes are minimum; authenticator apps or hardware keys are preferred.
- ☐ **Unique accounts per employee** — No shared logins. Every action must be traceable to an individual. This includes seasonal/contract preparers.
- ☐ **Role-based access controls (RBAC)** — Admins see admin data. Staff preparers see their clients only. Front desk doesn't access tax returns.
- ☐ **Password policy enforced** — Minimum 14 characters, complexity requirements, no reuse of last 12 passwords. Consider a managed password vault (e.g., 1Password Business).
- ☐ **Terminated employee off-boarding within 24 hours** — Disable all accounts, revoke VPN and cloud access, change shared credentials, retrieve equipment. Document the process.
- ☐ **Annual access review** — Audit who has access to what every January. Remove dormant accounts. Verify admin privileges are justified.
- ☐ **Visitor and vendor access logging** — Physical sign-in for office visitors. Vendor remote access sessions logged with start/end times.
- ☐ **Session timeout policies** — Auto-lock after 10 minutes of inactivity on all workstations. 15-minute timeout on cloud applications.

> **Quick Win**
>
> If you do nothing else today, turn on MFA for your email and tax software. These two changes block 99.9% of credential-based attacks.

# 03 Network Security

Your office network is the perimeter. If it's flat and unmonitored, a single compromised device gives attackers access to everything.

- ☐ **Business-grade firewall with active threat protection** — Consumer routers are not acceptable. Use a managed firewall (e.g., Fortinet, SonicWall, Meraki) with IDS/IPS enabled and firmware auto-updated.
- ☐ **Network segmentation** — Separate guest Wi-Fi from the business network. Isolate printers and IoT devices on their own VLAN.
- ☐ **Wi-Fi secured with WPA3 Enterprise** — Unique credentials per employee. No shared "office password" taped to the wall.
- ☐ **VPN for all remote access** — Staff working from home must connect through an encrypted VPN tunnel. Split tunneling disabled.
- ☐ **DNS filtering** — Block known malicious domains at the network level. Prevents malware callbacks even if a user clicks a bad link.
- ☐ **Endpoint detection and response (EDR) on every device** — Traditional antivirus isn't enough. EDR monitors behavior, not just signatures. Managed detection and response (MDR) is ideal for small firms.
- ☐ **Automated patch management** — OS updates, browser updates, and third-party software patched within 14 days of release. Critical vulnerabilities within 48 hours.
- ☐ **Network monitoring and logging** — Retain firewall, VPN, and access logs for minimum 12 months. Review anomalies weekly.

## 04 Email & Phishing Defense

- ☐ **Advanced email filtering** — Microsoft Defender for Office 365 or equivalent with anti-phishing, safe links, and safe attachments enabled.
- ☐ **DMARC, DKIM, and SPF configured** — Prevents attackers from spoofing your firm's email domain to trick clients.
- ☐ **Phishing simulation training** — Monthly simulated phishing emails for all staff. Track click rates; coach repeat offenders.
- ☐ **Client communication protocols** — Never email tax returns. Never send wire instructions via email. Establish a verbal verification policy for payment changes.
- ☐ **Email retention and archival** — 7-year retention for client communications per IRS and state board requirements.

## 05 Backup & Disaster Recovery

- ☐ **3-2-1 backup strategy** — 3 copies of data, on 2 different media types, with 1 offsite/cloud copy. Immutable backups preferred (ransomware-proof).
- ☐ **Daily automated backups** — All tax software databases, practice management data, client files, and email archived daily.
- ☐ **Backup encryption** — Backups contain the same sensitive data as production. Encrypt them with the same rigor.
- ☐ **Quarterly backup restore tests** — A backup you've never tested is not a backup. Restore a sample set quarterly and document results.
- ☐ **Documented disaster recovery plan** — Written plan covering: who does what, recovery time objectives (RTO), recovery point objectives (RPO), and communication procedures.
- ☐ **Tax season continuity plan** — Specific plan for a major outage during Jan 15 – Apr 15. Where do preparers work? How fast can systems be restored?

# 06 Compliance Documentation

If it's not documented, it didn't happen. Regulators, insurance carriers, and clients increasingly demand proof.

- ☐ **Written Information Security Plan (WISP)** — Required by IRS for all tax preparers (Publication 4557). Must be written, specific to your firm, and updated annually.
- ☐ **Incident response plan** — Step-by-step: detect, contain, eradicate, recover, notify. Include IRS notification (Form 14039), state AG notification timelines, and client communication templates.
- ☐ **Employee security training records** — Document completion of annual security awareness training for every employee. Keep certificates on file.
- ☐ **Vendor risk assessments** — Evaluate the security posture of every vendor who touches client data. Request SOC 2 reports. Document your review.
- ☐ **Annual risk assessment** — Formal assessment of threats, vulnerabilities, and controls. Update based on new threats, firm changes, and audit findings.
- ☐ **Cyber insurance policy** — Minimum $1M coverage. Review policy exclusions annually. Ensure your security controls meet the carrier's requirements.
- ☐ **Client data retention and destruction policy** — Define how long you keep data and how you destroy it. Shred physical; cryptographic erase digital.

## Score Your Firm

| ITEMS CHECKED | RATING | PRIORITY |
|---|---|---|
| 38–42 of 42 | **Excellent** — audit-ready | Annual review cycle |
| 28–37 of 42 | **Good** — minor gaps | Fix gaps within 60 days |
| 18–27 of 42 | **Fair** — significant exposure | Engage an MSP for remediation plan |
| Below 18 | **At Risk** — urgent action needed | Schedule assessment this week |

**Your Score: _____ / 42**

If you scored below 28, your firm has meaningful compliance gaps that could result in IRS penalties, insurance claim denials, or data breaches. A 30-minute assessment with Transform 42 can identify the fastest path to closing those gaps.

# Ready to Secure Your Practice?

Schedule a free 30-minute IT compliance assessment with Transform 42's team. We'll review your score and build a prioritized action plan.

**(305) 709-0050**

info@transform42inc.com

TRANSFORM42INC.COM