OmniTechPro

Is Your Firm WISP-Ready? A Self-Assessment for CPA Firms

Based on IRS Publication 4557 Requirements

Why this matters: The IRS requires all tax professionals to have a Written Information Security Plan (WISP). This checklist helps you quickly identify gaps in your firm's compliance. Check each item that's currently in place, tally your scores, and see where you stand.

Firm Name:	**Date:**
Completed By:	**Number of Employees:**

1. WISP Document ___/4

- [ ] Written WISP document exists
  Your firm has a formal, written security plan — not just informal practices
- [ ] Reviewed or updated in the last 12 months
  Someone has looked at the plan within the past year and confirmed it's still accurate
- [ ] Designated security coordinator
  One person is officially responsible for overseeing your firm's data security
- [ ] Employees sign acknowledgment of the WISP
  Staff sign a form confirming they've read and understand the security plan

2. Employee Security Training ___/4

- [ ] **Annual security awareness training for all staff**
  Every employee completes security training at least once a year
- [ ] **Phishing awareness training**
  Staff are trained to recognize fake emails designed to steal login credentials or data
- [ ] **Training on handling sensitive client data**
  Employees know proper procedures for handling Social Security numbers, tax returns, and financial records
- [ ] **New hire security onboarding**
  New employees receive security training before they get access to client data

3. Access Controls ___/5

- [ ] **Unique login for every user**
  No shared usernames or passwords — every person has their own login
- [ ] **Multi-factor authentication on all systems with client data**
  A second verification step (like a code on your phone) is required to log in to tax software, email, etc.
- [ ] **Role-based access — not everyone is admin**
  Staff only have access to the data and systems they need for their specific job
- [ ] **Former employee accounts disabled promptly**
  When someone leaves the firm, their computer and software access is removed the same day
- [ ] **Automatic screen lock (15 minutes or less)**
  Computers automatically lock themselves after a short period of inactivity

4. Password Policy ___/4

- [ ] **Strong passwords required (12+ characters)**
  All accounts require passwords that are at least 12 characters long
- [ ] **Password manager in use**
  Your firm uses a tool like LastPass, 1Password, or Keeper to securely store and generate passwords
- [ ] **No passwords on sticky notes or shared documents**
  Passwords aren't written down where others can see them or stored in shared spreadsheets
- [ ] **Passwords changed after suspected breach**
  If there's ever a suspected security incident, all affected passwords are changed immediately

5. Data Protection & Encryption ___/4

- [ ] **Full-disk encryption on all laptops**
  If a laptop is lost or stolen, the data on it can't be read without the password (e.g., BitLocker or FileVault)
- [ ] **Encrypted email for sending sensitive documents**
  Client tax docs and SSNs are sent using secure/encrypted email — not regular email
- [ ] **Secure client portal for document exchange**
  Clients upload and download documents through a secure online portal instead of email attachments
- [ ] **USB/removable media policy**
  There are rules about using USB drives — or they're blocked entirely to prevent data theft

6. Backup & Recovery ___/4

- [ ] **Regular automated backups**
  Your firm's data is automatically backed up on a regular schedule (daily or more often)
- [ ] **Backups stored off-site or in the cloud**
  Backup copies are kept somewhere other than your office — so a fire or flood won't destroy them too
- [ ] **Backup restoration tested in the last 12 months**
  Someone has actually tried restoring from backup to make sure it works when you need it
- [ ] **Documented recovery time objective**
  You know how long it would take to get back up and running after a disaster (and it's written down)

7. Network & Endpoint Security ___/5

- [ ] **Business-grade firewall**
  Your office uses a professional firewall — not just the one built into a consumer Wi-Fi router
- [ ] **Antivirus/threat protection on all computers**
  Every PC and laptop has security software that actively monitors for and blocks threats (sometimes called EDR)
- [ ] **Software updates applied within 30 days**
  When security patches are released for Windows, Office, or other software, they're installed promptly
- [ ] **Secure Wi-Fi with strong encryption**
  Your office Wi-Fi uses WPA2 or WPA3 with a strong, unique password
- [ ] **Guest Wi-Fi separated from business network**
  Visitors connect to a separate Wi-Fi network that can't access your business files or systems

8. Physical Security ___/5

- [ ] **Office locked when unattended**
  The office is always locked when no one is there — including after hours and weekends
- [ ] **Server/network equipment in a locked area**
  Your server, router, and network equipment are in a locked room or closet — not out in the open
- [ ] **Visitor log or escort policy**
  Visitors to your office sign in and/or are accompanied by an employee
- [ ] **Clean desk policy for sensitive documents**
  Client papers aren't left out on desks overnight — they're filed or locked away
- [ ] **Secure shredding for paper documents**
  Paper documents with client information are cross-cut shredded, not just thrown in the trash

9. Incident Response Plan ___/4

- [ ] **Written incident response plan**
  There's a documented step-by-step plan for what to do if a data breach or cyberattack happens
- [ ] **Staff know who to contact if breach suspected**
  Employees know exactly who to call or notify if they think something suspicious has happened
- [ ] **IRS reporting procedure documented**
  Your plan includes how to report a breach to the IRS using Form 14039 and contact the proper authorities
- [ ] **Cyber insurance policy in place**
  Your firm has an insurance policy that covers costs related to a data breach or cyberattack

10. Vendor & Remote Access ___/4

- [ ] **Vendor access reviewed annually**
  You review which outside companies have access to your systems at least once a year
- [ ] **Remote access uses VPN or secure connection**
  When working from home, staff connect through a VPN or other secure method — not just a regular internet connection
- [ ] **Personal device policy (BYOD)**
  There are clear rules about whether and how employees can use personal phones or laptops for work
- [ ] **Cloud services reviewed for security**
  Cloud tools your firm uses (Dropbox, Google Drive, etc.) have been checked to make sure they're secure enough for client data

Your Results

Total Score: _____ / 43

What Your Score Means

Score	Rating	What It Means
36–43	✅ Strong	Your firm has a solid security foundation. A few tune-ups may be needed to stay fully compliant.
25–35	⚠️ Moderate	There are significant gaps in your security posture. An action plan should be created soon to address them.
15–24	🔴 Weak	Your firm has major security exposure. Urgent remediation is recommended to avoid IRS penalties or a breach.
0–14	🚨 Critical	Your firm is non-compliant and at immediate risk. This needs to be addressed right away.

🚩 Red Flags — Immediate Attention Needed

If any of these apply to your firm, they should be your top priority regardless of your overall score:

- No written WISP document at all
- No multi-factor authentication on tax software or email
- No backups, or backups that have never been tested
- Shared admin passwords across the office
- No encryption on laptops

Want Expert Help Closing Your WISP Gaps?

Get a free 15-minute compliance review with an OmniTechPro security specialist. We'll help you understand your gaps and build a clear plan to get compliant.

Book Your Free Review →

📞 (410) 422-1099 | 🌐 www.omnitechpro.com | 📧 info@omnitechpro.com