SELF-ASSESSMENT

How Secure Is Your Firm?

Most accounting firms can't say with confidence where they're exposed. They have security in place, so it feels handled, until a cyberattack or a federal audit finds the one gap they missed.

This quick 10-point self-assessment helps you find the gaps first. **Give yourself one point for every statement that's true of your firm today.**

Your written security plan

- ☐ We have a Written Information Security Plan (WISP), and we've reviewed it in the last 12 months.
- ☐ A named person owns it, and our breach response steps are documented.

Why? A WISP is a federal requirement for tax preparers under the Gramm-Leach-Bliley Act and the FTC Safeguards Rule, not just a best practice.

Access to client data

- ☐ Multifactor authentication is on every system that touches client data, not just our main platform.
- ☐ Departing staff and contractors lose access the same day they leave.

Why? Most breaches start with a single compromised or lingering login, not a sophisticated hack.

Devices and email

- ☐ We run endpoint detection and response (EDR) on every device, not just servers.
- ☐ We can remotely wipe a lost or stolen device.

Why? Firewalls and antivirus stop entry-level attacks. They don't stop an attacker who slips past the perimeter.

Backup and recovery

- ☐ Our backups are independent of our primary software, and we've tested a restore.
- ☐ Our retention matches our record-keeping obligations.

Why? A backup you've never restored is a guess, not a recovery plan.

Your people and AI

- ☐ We run recurring Security Awareness Training with phishing simulations.
- ☐ We have a written AI usage policy that defines what client data can enter AI tools.

Why? People stop the attacks technology misses, but only if they're trained for how attacks actually look today.

What's your position?

Total: ______________________

8 to 10: Strong position
You're defending well. Keep pressure on the remaining gaps and review annually because the board keeps changing.

5 to 7: Exposed in the middlegame
You've got real protection, but an attacker or an auditor would find an open lane. Close your lowest-scoring area first.

0 to 4: King in check
Critical gaps are leaving client data and your compliance standing at risk. This needs attention now, not next quarter.

Our free Security Risk Quiz maps your firm against all five: WISP, access, devices and email, backup and recovery, and people and AI, and shows you exactly where you're exposed and what to fix first.

Take Assessment

rightworks.com