

Busy Season Ready Check

12 questions for CPA and tax firms, plus one on AI. About 10 minutes.



Human-Focused IT. Period. | kairosit.com
1280 SW 36th Ave #101, Pompano Beach, FL

Why this matters now: PTIN renewal opens in mid-October, and the PTIN application asks each preparer to acknowledge that paid tax return preparers are required by law to create and maintain a written information security plan (WISP). Under the FTC Safeguards Rule, tax and accounting professionals are financial institutions, regardless of size (IRS Pub. 5708).

How to score: give yourself 1 point for each honest “yes, and we could show you.” 11 to 13: you’re in good shape. 8 to 10: a few gaps to close before January. 7 or less: get the plan written and running before busy season.

#	QUESTION	YES / NO	BASED ON
1	One person owns it. Have you named someone in writing to run your security program, and do they report to the partners in writing at least once a year?	☐ / ☐	FTC 16 CFR 314.4(a), (i)†; Pub. 5708 (Data Security Coordinator)
2	The plan matches today. Is your WISP written, easy for staff to find, and updated in the last 12 months or since your last big change (new office, merger, new software)?	☐ / ☐	314.4(g); Pub. 5708
3	You know your risks. Do you have a written risk assessment that says what could go wrong and how you're handling each risk?	☐ / ☐	314.4(b)†
4	You know where client data lives, and you clear out what you don't need. Is there a current list of devices, systems, portals, and cloud apps that hold client data? Is old client data securely destroyed on a schedule?	☐ / ☐	314.4(c)(2), (c)(6); Pub. 5708
5	Only the right people get in. Does each person see only the client files they need, and are departing staff locked out the same day?	☐ / ☐	314.4(c)(1); Pub. 5708
6	MFA everywhere. Does every login to email, tax software, the client portal, and remote access require a second factor?	☐ / ☐	314.4(c)(5); Pub. 5708
7	Client data is encrypted. Is client data encrypted when you send it outside the firm and when it sits on laptops, servers, and in the cloud?	☐ / ☐	314.4(c)(3)
8	Backups you have actually restored. Do you back up client data to a secure separate location, and have you tested a restore in the last 6 months?	☐ / ☐	IRS Pub. 4557
9	Someone is watching. Is user activity logged and monitored, and do you have continuous monitoring or yearly penetration testing plus vulnerability scans every 6 months?	☐ / ☐	314.4(c)(8), (d)†
10	Staff are trained, and it's signed. Has everyone had security awareness training this year, with a signed and dated acknowledgment on file?	☐ / ☐	314.4(e); Pub. 5708
11	Vendors are checked. Do your contracts with tax software, portal, cloud, and IT vendors require them to protect client data, and do you review them periodically?	☐ / ☐	314.4(f)
12	There's a breach plan with names and numbers. Is there a written incident response plan that says who calls whom: your IRS Stakeholder Liaison, the FTC (within 30 days if 500 or more consumers are involved), Florida notices, and your cyber insurer?	☐ / ☐	314.4(h)†, (j); Pub. 4557; Fla. Stat. 501.171*
AI	AI tools have rules. Does your plan list which AI tools staff may use and what client data can and can't go into them?	☐ / ☐	KairosIT recommended practice* (supports 314.4(c)(1) and (f))

Score: ____ / 13

Want a second set of eyes? Our security team will walk through your answers in 30 minutes and send you a written top-three list. Call **(844) 352-4767** or reply to my email.

Also worth doing during filing season: check your e-File application and PTIN account weekly for the number of returns filed under your EFIN and PTINs (IRS Pub. 4557).

† Under 16 CFR 314.6, firms that hold customer information on fewer than 5,000 consumers are exempt from 314.4(b)(1) (the written risk assessment), (d)(2) (the continuous monitoring or pen test and scan schedule), (h) (the written incident response plan), and (i) (the annual written report). Check your count: many firms with 20 or more users are above 5,000.

* KairosIT recommended practice or a state law check, not FTC or IRS rule text. Florida breach notice duties (Fla. Stat. 501.171) apply separately; confirm with counsel.

Sources (verified Oct 2 and Oct 6, 2026): 16 CFR Part 314, sections 314.4 and 314.6 (ecfr.gov); FTC, Safeguards Rule notification requirement now in effect (ftc.gov); IRS Pub. 5708, Rev. 8-2024; IRS Pub. 4557, Rev. 6-2024; IRS Pub. 5293; Instructions for Form W-12, line 11; IRS PTIN FAQ; Fla. Stat. 501.171.

Not legal advice, an audit, or a certification. This is a general self-check to support a conversation with your counsel or compliance advisor.