WISPWolf · Free Guide

IRS WISP Audit Readiness Guide

The documents, evidence, and security controls auditors commonly expect to see — for tax preparers, accountants, bookkeepers, enrolled agents, and CPA firms.

Why this matters

Every paid tax preparer with a PTIN is required to maintain a Written Information Security Plan (WISP). IRS Publication 5708 provides the template; the FTC Safeguards Rule (16 CFR Part 314) makes it federal regulation. Since the 2024 PTIN renewal cycle, preparers attest annually that they maintain a WISP — and the IRS Stakeholder Liaison program is increasingly sampling those attestations and requesting documentation.

This guide explains what auditors commonly ask to see, the gap between having a WISP and following one, and the documentation and evidence firms should maintain to support their plan.

What auditors commonly request

• The current WISP document, dated within the last 12 months.

• A written risk assessment identifying threats to client data and controls.

• Employee security policies and signed acknowledgments.

• Documented incident response procedures with regulatory notification workflows.

• Vendor management records covering tax software, e-file transmitters, cloud storage, and IT support.

• Security awareness training completion logs.

• Evidence of implemented controls — MFA enforcement, encryption, endpoint protection.

• The most recent annual review attestation signed by the Data Security Coordinator.

Common WISP mistakes

• Downloading a generic template and never updating it.

• No documented annual review for the past 12 months.

• Missing risk assessment, or one that references systems no longer in use.

• Procedures referenced but not written down.

• Controls claimed in the document with no supporting evidence.

• A named Data Security Coordinator who has left the firm.

• Vendor list missing tax software, e-file transmitter, or cloud accounting platforms.

Documentation checklist

■ Current WISP document with date and version

■ Named Data Security Coordinator with authority to enforce policy

■ Written risk assessment dated within last 12 months

■ Data inventory: where client data lives, who can access it

■ Employee security procedures and training program

■ Incident response plan with regulatory contacts (IRS Stakeholder Liaison, FTC)

■ Vendor matrix with services, data types, and review dates

■ Annual review attestation signed by governing body or owner

Evidence checklist

■ MFA enforcement screenshots from identity provider, email, tax software, cloud accounting

■ Email security configuration: SPF, DKIM, DMARC in enforce mode

■ Encryption at rest: BitLocker / FileVault config; encrypted backups; encrypted cloud storage

■ Encryption in transit: TLS 1.2+, VPN for remote access, SFTP

■ Endpoint protection / EDR dashboard with managed-device inventory

■ Patch management compliance report

■ Security monitoring alerts with documented triage and closure

■ Quarterly access control review logs (least privilege enforced; no shared accounts)

■ Training completion certificates and phishing simulation results

■ Signed policy acknowledgments for all employees and contractors

Annual review requirements

The FTC Safeguards Rule requires the program to be reviewed at least annually and any time material changes occur. The Qualified Individual (or IRS Pub 5708's Data Security Coordinator) must:

• Evaluate the adequacy of the program against current risks.

• Document changes made during the year.

• Report findings to the firm's governing body or owner.

• Produce a signed and dated annual attestation.

Security controls firms often overlook

• Phishing-resistant MFA on email and admin consoles (authenticator app or FIDO2 — not SMS-only).

• Conditional access policies blocking legacy authentication.

• Email DLP rules preventing unauthorized forwarding of tax documents.

• Encrypted backups stored separately from primary systems, periodically restored.

• Mobile device management or screen-lock enforcement on personal devices used for work.

• Offboarding checklist that revokes access within 24 hours of termination.

• Annual tabletop exercise of the incident response plan.

• Written cyber insurance notification workflow (typical carrier requirement: 48–72 hours).

Template WISP vs. Living WISP

Template WISP

- Static document
- Self-attested
- No verification of controls
- Often forgotten between renewals

Living WISP

- Continuously updated as environment changes
- Evidence-backed for every control
- Reviewed and attested annually
- Supports audit readiness and insurance renewals

Next step: measure your current state

Use this guide to compare your current WISP and controls to what auditors commonly expect. For a personalized compliance scorecard mapped to IRS Publication 5708 and the FTC Safeguards Rule, take the free 15-question WISPWolf assessment at wispwolf.com/quiz.