

CPA & Tax Firm Written Information Security Program (WISP) Checklist

10 Mandatory Technical & Administrative Controls Required for PTIN Renewal, FTC Safeguards Rule (16 CFR Part 314), and 30-Day Breach Prevention.

\$51,744

Max Civil Penalty Per FTC Violation

4 Minutes

Emry 24/7 MDR Host Isolation SLA

< 24 Hours

CISA KEV Edge Gateway Patching

100% PTIN

Audit-Ready Live WISP Evidence



01. Designated Qualified Individual & Live WISP Binder (16 CFR 314.4(a))

☐ PASS ☐ GAP / REMEDIATE

Appoint a named Qualified Individual and maintain a live, system-backed Written Information Security Program updated continuously rather than an annual static Word template.



02. Phishing-Resistant FIDO2 MFA on Tax & Hosting Portals (16 CFR 314.4(c)(5))

☐ PASS ☐ GAP / REMEDIATE

Enforce hardware-bound FIDO2/WebAuthn MFA across Microsoft 365, CCH Axcess, UltraTax CS, Lacerte, Drake, QuickBooks Enterprise, SafeSend, and Citrix/RDP remote gateways.



03. Sub-24-Hour Emergency Edge Gateway Patching (CISA KEV Mandate)

☐ PASS ☐ GAP / REMEDIATE

Patch internet-facing VPNs, firewalls, and remote desktop gateways within 24 hours of CISA Known Exploited Vulnerability (KEV) disclosure to block 1-day ransomware entry.



04. 4-Minute 24/7 Human-Led MDR Host & Session Isolation

☐ PASS ☐ GAP / REMEDIATE

Replace 4-hour standard MSP ticket queues with 24/7/365 SOC monitoring and automated <4-minute endpoint quarantine and session-token revocation during tax season.



05. FTC 30-Day Breach Notification Readiness (500+ Consumers Rule)

☐ PASS ☐ GAP / REMEDIATE

Deploy centralized 365-day SIEM audit logging capable of proving whether unencrypted Taxpayer PII/SSN records were exfiltrated within the mandatory FTC reporting window.



06. Tax-Season Infrastructure Change Freeze (Jan 15 - Apr 15 & Sep 15 - Oct 15)

☐ PASS ☐ GAP / REMEDIATE

Lock production CCH/UltraTax/QuickBooks server schemas against disruptive maintenance windows while preserving emergency zero-day security containment.



07. Immutable Object-Locked Backups & 90-Day Verified Test Restores

☐ PASS ☐ GAP / REMEDIATE

Maintain air-gapped S3 Object-Locked backups immune to Domain Admin compromise, with timestamped bare-metal restoration certificates generated every 90 days.



08. Former Staff & Seasonal Preparer Zero-Minute Offboarding

☐ PASS ☐ GAP / REMEDIATE

Automate immediate credential revocation across tax portals, IRS e-Services, client portals, and M365 OAuth refresh tokens the moment a seasonal preparer departs.



09. Encrypted Taxpayer Data in Transit & At Rest (AES-256 / TLS 1.3)

☐ PASS ☐ GAP / REMEDIATE

Enforce BitLocker/FileVault full-disk encryption on all partner laptops and block unencrypted email attachments containing W-2, K-1, or 1040 schedules via automated DLP.



10. Annual Penetration Testing & Continuous Vulnerability Telemetry (16 CFR 314.4(d)(2))

☐ PASS ☐ GAP / REMEDIATE

Conduct annual third-party penetration testing plus continuous automated internal/external vulnerability scanning with documented remediation SLAs.