TAX & ACCOUNTING WISP COMPLIANCE QUICK SELF-AUDIT





10-POINT WISP COMPLIANCE SELF-AUDIT

Check each box that reflects your current setup:

Documented risk assessment of systems, devices, applications, and vendor access.
Data Encription (AES-256+)in storage and transmission.
Multi-factor authentication (MFA) across all systems and applications.
Annual security training for all staff and contractors.
Incident response plan for breaches and system compromises.
Secure, offsite backups with daily snapshots and version control.
Role-based access controls with least-privilege principles.
Secure remote access controls using enterprise-grade tools only.
WISP reviewed annually and after system/staffing changes.
Device policy covering personal equipment and remote work.
9–10 boxes checked: Vou're WISP-ready! Maintain your plan annually.
6-8 boxes checked: 1 Gaps exist—prioritize before peak season. <6 boxes checked: X Likely non-compliant, Immediate action recommended.



Even tech-savvy firms often miss these WISP-critical items:

- Backups stored locally but not encrypted or offsite
 If your backups are on the same network and lack encryption, a ransomware attack could wipe out your data and your recovery options.
- No centralized policy for contractor or part-time access
 Without access controls, temp staff and remote workers may have more system access than necessary, creating avoidable risk.
- No written incident response plan or breach documentation
 During an audit or breach event, not having a clear plan can lead to regulatory violations and a slower response time.
- Using personal devices for client work without controls
 Laptops or phones without remote wipe, antivirus, or VPN access become major liabilities when used for tax work.
- WISP written once, but never updated or reviewed
 Outdated WISPs may not reflect your current software, access setup, or staff responsibilities—leaving blind spots.
- Relying on "IT guys" without clear audit-ready records
 Having help is great, but you still need documented proof of security policies and safeguards.
- No proactive monitoring of all devices
 If issues aren't being logged or flagged in real-time, your firm may not catch vulnerabilities
 until it's too late.

If any of these sound familiar, Verito can help.



Your Next Step—Make WISP Compliance Easy VeritGuard by **verito** Gives You:

- 24/7 live technical support from specialists
- Daily encrypted backups with offsite storage for business continuity
- Data encryption at rest and in transit to protect sensitive client information
- System patching and maintenance to keep your environment secure
- Proactive security updates aligned with IRS Publication 4557 and FTC Safeguards Rule
- IT infrastructure built for always-on tax season performance