Accounting Firm IT Security & WISP Readiness Checklist

Is your firm's technology supporting its information security responsibilities?

Mark one response per question based on your current practices. Use Not Sure when you need evidence or clarification. Keep notes free of taxpayer data and passwords.

SECTION 1 OF 6

Security Planning & Responsibilities

01 Does your firm have a written, implemented Information Security Plan (WISP) tailored to its operations?

☐ Yes ☐ Needs Attention ☐ Not Sure

02 Has your firm designated a qualified person to own and coordinate its security program?

☐ Yes ☐ Needs Attention ☐ Not Sure

03 Do you maintain an inventory of sensitive taxpayer information, including where it is stored and who handles it?

☐ Yes ☐ Needs Attention ☐ Not Sure

04 Does your firm periodically assess risks to sensitive information and the effectiveness of its safeguards?

☐ Yes ☐ Needs Attention ☐ Not Sure

05 Is your WISP reviewed and updated when operations, technology, staffing, or risks change?

☐ Yes ☐ Needs Attention ☐ Not Sure

Notes / next steps

Accounting Firm IT Security & WISP Readiness Checklist

Mark one response per question: Yes / Needs Attention / Not Sure.

SECTION 2 OF 6

Account Security & Access Controls

06 Is multifactor authentication used to protect access to systems containing sensitive information, with any permitted alternatives formally reviewed and documented?

☐ Yes ☐ Needs Attention ☐ Not Sure

07 Does each employee use an individual account so access and activity can be attributed to the right person?

☐ Yes ☐ Needs Attention ☐ Not Sure

08 Is access limited to the information and systems each person needs for their role?

☐ Yes ☐ Needs Attention ☐ Not Sure

09 Do offboarding procedures promptly remove access and recover devices when employees or contractors leave?

☐ Yes ☐ Needs Attention ☐ Not Sure

10 Are passwords and privileged credentials securely stored, shared only when authorized, and reviewed when access changes?

☐ Yes ☐ Needs Attention ☐ Not Sure

Notes / next steps

Accounting Firm IT Security & WISP Readiness Checklist

Mark one response per question: Yes / Needs Attention / Not Sure.

SECTION 3 OF 6

Computers, Servers & Networks

11 Are operating systems and applications kept current through a managed security-update and patch process?

☐ Yes ☐ Needs Attention ☐ Not Sure

12 Are business computers and servers covered by endpoint threat protection that is kept current and monitored?

☐ Yes ☐ Needs Attention ☐ Not Sure

13 Is sensitive information appropriately encrypted when stored and transmitted, with any permitted alternatives reviewed and documented?

☐ Yes ☐ Needs Attention ☐ Not Sure

14 Are firewalls and remote-access methods securely configured, maintained, and restricted to authorized users?

☐ Yes ☐ Needs Attention ☐ Not Sure

15 Are systems and networks reviewed for vulnerabilities and insecure configurations on a defined schedule?

☐ Yes ☐ Needs Attention ☐ Not Sure

Notes / next steps

Accounting Firm IT Security & WISP Readiness Checklist

Mark one response per question: Yes / Needs Attention / Not Sure.

SECTION 4 OF 6

Email Security & Employee Education

16 Does your email protection address phishing, malicious attachments or links, and impersonation attempts?

☐ Yes ☐ Needs Attention ☐ Not Sure

17 Do employees receive recurring security awareness training relevant to their work with sensitive information?

☐ Yes ☐ Needs Attention ☐ Not Sure

18 Do employees know how and where to report suspicious messages or possible security incidents?

☐ Yes ☐ Needs Attention ☐ Not Sure

19 Does your team independently verify unusual payment, credential, or information requests through a trusted contact method?

☐ Yes ☐ Needs Attention ☐ Not Sure

Notes / next steps

Accounting Firm IT Security & WISP Readiness Checklist

Mark one response per question: Yes / Needs Attention / Not Sure.

SECTION 5 OF 6

Data Protection & Business Continuity

20 Are backup schedules documented for the information and systems your firm relies on?

☐ Yes ☐ Needs Attention ☐ Not Sure

21 Are backup copies protected against unauthorized access, destructive changes, and ransomware?

☐ Yes ☐ Needs Attention ☐ Not Sure

22 Are backup restorations tested, with results and follow-up actions documented?

☐ Yes ☐ Needs Attention ☐ Not Sure

23 Does your firm have a practical disaster recovery and business continuity plan with priorities and responsibilities?

☐ Yes ☐ Needs Attention ☐ Not Sure

24 Are information retention and secure disposal practices documented and followed for records, devices, and media?

☐ Yes ☐ Needs Attention ☐ Not Sure

Notes / next steps

Accounting Firm IT Security & WISP Readiness Checklist

Mark one response per question: Yes / Needs Attention / Not Sure.

SECTION 6 OF 6

Incident Response & Service Providers

25 Does your firm have a documented process for identifying, containing, responding to, and recovering from security incidents?

☐ Yes ☐ Needs Attention ☐ Not Sure

26 Are appropriate IRS and regulatory notification contacts documented and accessible during an incident?

☐ Yes ☐ Needs Attention ☐ Not Sure

27 Has your firm reviewed applicable breach-notification obligations and assigned responsibility for determining when and how to notify?

☐ Yes ☐ Needs Attention ☐ Not Sure

28 Does your firm evaluate outside technology providers and oversee the safeguards protecting information they handle?

☐ Yes ☐ Needs Attention ☐ Not Sure

29 Are security safeguards periodically reviewed and tested to check that they remain effective?

☐ Yes ☐ Needs Attention ☐ Not Sure

30 Are identified security weaknesses assigned an owner, prioritized, corrected, and checked for completion?

☐ Yes ☐ Needs Attention ☐ Not Sure

Notes / next steps

Turn your answers into next steps.

Needs Attention and Not Sure responses may indicate areas warranting further review. Start by confirming what is in place, identifying gaps, and agreeing who will address each priority. A Yes response should be supported by current practices and evidence; it is not a compliance finding.

A practical follow-up

• Choose your most important open questions and gather supporting information.

• Assign an owner and target date for each next step.

• Review findings with your security program owner and relevant IT, legal, or regulatory advisers.

• Update your security program as changes are implemented and reassess regularly.

Schedule an IT Security Readiness Conversation

The CI Guys can help you review the technology supporting your security program and identify practical improvements.

computerinnovations.net/contact/ | 417-882-7788

Official guidance

IRS Publication 4557: Safeguarding Taxpayer Data

IRS Publication 5708: Creating a Written Information Security Plan

FTC Safeguards Rule: What Your Business Needs to Know

Guidance reviewed November 3, 2026. Consult current official sources and determine which requirements apply to your firm. Some exceptions affect specific provisions, not the entire security program.

This checklist is an educational self-assessment resource. It is not a complete WISP, legal advice, a formal security assessment, or a determination of regulatory compliance.