AdvancedBITS | Business IT Solutions

AI Readiness Guide for Accounting Firms

How to adopt AI without putting client confidentiality, your WISP, or your professional standing at risk

> **About this guide.** The statistics cited here come from third-party research and are not AdvancedBITS client results. The firm described in Section 8 is an illustrative composite, not a single client, and carries no performance figures. This guide is general information about technology readiness. It is not legal, tax, or professional standards advice.

Executive Summary

Your staff are probably already using AI, so AI readiness for an accounting firm starts with seeing, protecting, and governing that use, not with buying a tool. The firms that get hurt are rarely the ones that avoid AI. They are the ones where client data, tax return information, or payroll files reach tools nobody reviewed.

AdvancedBITS provides managed IT, cybersecurity, and AI guardrails for accounting and tax firms. This guide gives you the AdvancedBITS AI Readiness Model, a Microsoft 365 and Copilot data-foundation checklist, human-review standards by task risk, a vendor checklist, and a six-month roadmap.

Key takeaways

- **Use is widespread and often unmanaged.** 98% of accounting professionals report using AI (Karbon, 2026), while 90% of firms in one vendor survey had no written AI policy (Financial Cents, 2026).
- **No new AI law is needed to create exposure.** IRS OPR Alert 2026-19, IRC Section 7216, the FTC Safeguards Rule, and the AICPA Code already apply to AI use.
- **Permissions come before Copilot.** Microsoft states that Copilot uses data a person already has permission to access (Microsoft Learn).
- **A person stays accountable.** AI output needs documented review by a named professional before it reaches a client, a return, or a filing.
- **Six months is a realistic runway.** A staged plan can take a firm from unmanaged to governed, scheduled around busy season.

1. Why does AI readiness matter for accounting firms now?

AI is already in use at most accounting firms, but governance has not kept pace. In Karbon's 2026 report, 98% of accounting professionals report using AI, and concern about data security rose to 83%. Counts vary because surveys measure different things: estimates range from 18% to 98% depending on whether the survey counts firms, workers, or tax professionals specifically (Atlas CPA Index, 2026).

The tax side is moving fast. Blue J and CPA.com found that 60% of tax professionals use AI for tax research at least weekly, up from 33% a year earlier (CNBC, 2026). And staff often bring their own tools: Microsoft and LinkedIn found that 78% of AI users bring their own AI tools to work (Work Trend Index, 2024).

Table 1. What independent research shows

Finding	Source	What it means for your firm
98% of accounting professionals report using AI, and 83% are concerned about data security.	Karbon, State of AI in Accounting 2026 (software vendor)	Assume AI is already in use at your firm.
60% of tax professionals use AI for tax research at least weekly, up from 33%.	Blue J and CPA.com survey of 1,000+ tax professionals, June 2026	Research prompts can carry client facts.
78% of AI users bring their own AI tools to work.	Microsoft and LinkedIn Work Trend Index, 2024	Personal accounts, not firm-managed tools.
90% of 486 surveyed professionals had no written AI policy, and 20% reported measurable ROI.	Financial Cents, 2026 (vendor survey, mostly small firms)	Policy lag is common, and so is unproven value.
92% of organizations with an AI-related breach lacked proper AI access controls.	IBM Cost of a Data Breach 2026, all industries, via eDiscovery Today	Access control is where AI incidents start.

Surveys are self-reported, use different samples, and several come from software vendors. None is an AdvancedBITS client result.

2. What rules already apply to AI use at an accounting firm?

No AI-specific statute is needed to create exposure, because existing tax, privacy, and professional rules already apply to AI use. On June 24, 2026, the IRS Office of Professional Responsibility issued Alert 2026-19, introductory guidelines for responsible AI use in federal tax practice. It says a tax professional using generative AI must carefully review what the technology produces, and trade coverage reports it maps six existing Circular 230 duties onto AI: diligence, technological competence, fee transparency, written advice standards, client data confidentiality, and firm-level supervision (Verito, 2026).

Table 2. Existing obligations and what they mean for AI use

Rule	What it says	What it means for AI use
IRS OPR Alert 2026-19 and Circular 230	Applies existing duties of diligence, competence, confidentiality, and supervision to AI. As reported, the professional who signs the return owns the result.	Review all AI output, know the tools your firm uses, supervise staff use, and protect client data.

Rule	What it says	What it means for AI use
IRC Section 7216 and Section 6713	Restrict disclosing or using tax return information without consent or an exception, with criminal and civil penalties, according to commentators.	Commentators read sending return information to an AI provider as a disclosure and say removing names is not a safe harbor. Whether any exception covers AI is unsettled. Ask counsel.
FTC Safeguards Rule (16 CFR Part 314) and your WISP	Requires a written security program with nine elements, including a risk assessment, MFA, encryption, service provider oversight, and incident response. The IRS states a WISP is required by law.	AI vendors are service providers, and AI use is a risk to assess. Add both to your WISP.
AICPA Code of Professional Conduct	Confidential Client Information Rule (ET 1.700.001) and General Standards Rule (ET 1.300.001): competence, due care, supervision, confidentiality.	The Code applies to AI as written. The AICPA offers a Small Firm Generative AI Policy Template and a 2026 practice aid for auditors.
State rules	CPA boards, privacy laws, and breach laws differ by state.	Confirm requirements with counsel for every state you serve.

What is still unsettled. The IRS alert does not say whether using an AI tool requires Section 7216 consent, and it does not require telling clients when AI is used, according to CNBC's reporting. The AICPA is advising firms to err on the side of disclosure. Ask your attorney or professional liability insurer how this applies to your firm.

3. What is the AdvancedBITS AI Readiness Model?

The AdvancedBITS AI Readiness Model has five areas, See, Protect, Govern, Review, and Prove, and a firm is ready when it can answer one question in each.

Table 3. The five areas of AI readiness

Area	The question you must answer	What ready looks like
See	Which AI tools, accounts, and features are in use, and by whom?	A current inventory that includes AI features inside approved software, personal accounts, browser extensions, and meeting note-takers.
Protect	Can AI reach only the data it should?	MFA everywhere, least-privilege access, cleaned Microsoft 365 permissions, encryption, and no broad sharing of client or payroll data.
Govern	What is allowed, with which data, and who decided?	A written AI policy, an approved tool list, a consent and disclosure process reviewed with counsel, vendor review, and an updated WISP.
Review	Who checks the output before it reaches a client or the IRS?	Human-in-the-loop standards by task risk, with a named reviewer and documented sign-off.

Area	The question you must answer	What ready looks like
Prove	Can you show it to a regulator, insurer, or client?	Dated evidence: tool inventory, training records, access reviews, logs, and the updated WISP.

Firms move through four stages: **Unmanaged** (use is invisible), **Aware** (an inventory exists and rules are informal), **Governed** (written policy, approved tools, trained staff), and **Operational** (output is reviewed, monitored, and evidenced every year). For context on adoption, a BILL and NewtonX survey of 207 accounting firm leaders placed 10% at awareness, 34% in early adoption, 38% in active adoption, and 18% at maturity (Atlas CPA Index, 2026).

4. How do you prepare Microsoft 365 for Copilot at an accounting firm?

Fix permissions before you turn on Copilot, because Copilot uses data a person already has permission to access (Microsoft Learn). That means loose sharing becomes loose answers. Microsoft's deployment blueprint has three steps: remediate oversharing, set up guardrails, and meet regulations. It notes that SharePoint Advanced Management is included with a Copilot license and that foundational Microsoft Purview capabilities are included in Microsoft 365 E3. Microsoft also states that your data is not used to train its foundation models.

Table 4. Where oversharing hides at accounting firms

Where it hides	Why it matters	What AdvancedBITS does
Client folders and tax workpapers	Old engagements stay open to staff who never worked on them.	Reviews site and folder permissions, restricts by engagement team, and archives closed files.
Payroll, HR, and partner compensation	Highly sensitive and often shared more broadly than intended.	Restricts libraries and applies sensitivity labels where licensed.
Broad group and link sharing	One link or group can expose a whole library.	Finds broad sharing, removes it, and sets safe defaults for new sites.
Departed, seasonal, and guest accounts	Access outlives the person.	Runs a joiner, mover, and leaver review and removes guests on a schedule.
Personal accounts and unmanaged devices	Client data leaves firm control.	Enforces MFA and device management and sets clear rules on personal AI accounts.
Backups and recovery	AI mistakes and ransomware both need a clean restore.	Tests a timed restore of Microsoft 365 and client data.

5. What does human-in-the-loop review look like?

Human-in-the-loop means a named professional verifies AI output against source documents or authority before it affects a client, a return, or a filing. The IRS alert tells tax professionals to review AI-generated work carefully, and an AICPA column warns that AI

models are not infallible and can produce incorrect output that reads as confident. Faster output should not mean thinner review.

Table 5. Review standards by task risk (AdvancedBITS recommendation)

Task	Risk	Minimum review standard
Internal drafting or meeting notes with no client information	Low	The author reads and edits the result.
Summarizing public guidance or standards	Medium	Check every citation and figure against the primary source.
Extracting data from client documents	High	Tie each figure to the source document and sample-check the rest.
Tax or technical research	High	Verify the conclusion in primary authority before relying on it.
Anything that includes tax return information	High	Use only approved tools, and only after your consent process and counsel's guidance.
Client-facing advice, workpaper conclusions, or return positions	Highest	A reviewing professional signs off, and the signing preparer or partner remains accountable.

Keep a short record of who reviewed what. That record is part of the evidence you may need later.

6. What does a six-month AI adoption roadmap look like?

A six-month roadmap moves a firm from unmanaged to governed by taking the steps in order: see, protect, govern, pilot, train, and prove. Schedule the work around your filing deadlines and avoid go-live dates in your busiest weeks.

Table 6. Six-month AI adoption roadmap

Month	Focus	Outputs
1	See	Tool and account inventory, shadow AI discovery, and leadership decisions on what is allowed.
2	Protect	MFA review, Microsoft 365 permissions cleanup, encryption and device checks, and a tested restore.
3	Govern	Written AI policy, approved tool list, consent and disclosure process with counsel, vendor review, and an updated WISP and risk assessment.
4	Pilot	Two or three low risk use cases with named reviewers and the review standards applied.
5	Train	Role-based training for partners, staff, and seasonal hires, with an acceptable use acknowledgment.
6	Prove and plan	An evidence file, the first policy review, and a roadmap for the next use cases.

7. How do you evaluate an AI vendor before staff use it?

Evaluate every AI tool against the same questions before staff use it with client data, because your agreement with the vendor, not the tool's brand, determines how data is handled. The AICPA column advises reading each tool's terms and privacy policy, noting that a vendor may disclaim liability for a security incident, and the Safeguards Rule expects oversight of service providers. Ask:

- Does the vendor train models on your data, and can you turn that off in writing?
- Where is data stored and processed, and how long is it kept?
- Can you delete your data, and can the vendor show that it did?
- Does the tool support single sign-on, MFA, and audit logs?
- Does the vendor have independent security evidence, such as a SOC 2 Type II report, and will it sign appropriate data protection terms?
- How and when will the vendor notify you of a security incident?
- Is use with tax return information consistent with your consent process and your counsel's advice?

8. What does this look like in practice? An illustrative example

> **Illustrative composite.** This example is not a single client and carries no performance figures.

Consider a 40-person regional CPA firm preparing for the next busy season. The partners believe staff use AI only through the tax research platform the firm licensed. An assessment finds something different:

- Staff use free chatbots on personal accounts to draft client emails and summarize documents, and AI note-takers join video calls. Nobody has a list of tools.
- Client, payroll, and partner folders are broadly shared after years of inherited permissions.
- There is no written AI policy, and the WISP was last updated before staff began using generative AI.
- The partners are unsure whether client consent is needed for any of it.

Over six months the firm follows the roadmap in Table 6. It builds a tool inventory, enforces MFA, tightens Microsoft 365 permissions, tests a restore, writes an AI policy and approved tool list, works out a consent and disclosure process with its attorney, updates its WISP, pilots two low risk uses with named reviewers, and trains every employee.

By month six, the firm can answer all five readiness questions. It knows which tools are in use, AI can reach only what it should, the rules are written and trained, output is reviewed, and the evidence exists. It did not promise clients that AI is risk-free, and it did not skip review because the output looked polished.

9. What should you do in the next 30 days?

Start with visibility and ownership, because you cannot govern what you cannot see.

1. Ask staff, without blame, which AI tools they use, including note-takers and browser extensions.
2. Name an owner for AI governance, such as your WISP Qualified Individual.
3. Pause new AI tools until they have been reviewed.
4. Confirm MFA on email, remote access, practice management, and Microsoft 365 admin accounts.
5. List the client, payroll, and HR folders that are shared broadly.
6. Ask your attorney or insurer how Section 7216 consent and client disclosure apply to your AI use.
7. Add AI tools to your WISP risk assessment and service provider list.
8. Choose two low-risk pilot uses and the people who will review them.
9. Schedule a timed restore test of your Microsoft 365 and client data.

Frequently asked questions

What is AI readiness for an accounting firm?

AI readiness is a firm's ability to use AI while keeping client information confidential, meeting its professional and security obligations, and keeping a person accountable for every result. The AdvancedBITS AI Readiness Model measures it in five areas: See, Protect, Govern, Review, and Prove.

Can accountants use ChatGPT with client data?

Existing rules do not ban AI, but they expect you to control where client data goes. Commentators read sending tax return information to an AI provider as a disclosure under IRC Section 7216, and the IRS has not said whether general-purpose AI tools fit an exception. Use firm-approved enterprise tools, avoid personal accounts, and ask your attorney or professional liability insurer before putting return information into any AI tool.

Do I need client consent to use AI on tax returns?

The IRS has not said. Its June 2026 AI alert does not address whether clients must be told, and the AICPA is advising firms to err on the side of disclosure, reportedly in a separate document and not a clause in the engagement letter. Ask your attorney to confirm what applies to your firm and your states.

Does our WISP need to cover AI?

In practice, yes. The FTC Safeguards Rule requires a written security program with a risk assessment and oversight of service providers, and AI tools are both a risk and a service provider. AdvancedBITS helps firms update the technical sections of the plan, and your Qualified Individual and counsel own the final document.

Is Microsoft Copilot safe for an accounting firm?

It can be, once permissions are clean. Microsoft states that Copilot uses data a user already has permission to access, so broad sharing becomes broad answers. AdvancedBITS reviews and tightens Microsoft 365 permissions, MFA, and sharing before Copilot is turned on.

What is shadow AI at an accounting firm?

Shadow AI is the use of AI tools, accounts, browser extensions, or meeting note-takers that the firm has not reviewed or approved, often a staff member's personal chatbot account. The firm cannot see what client information is entered or what the provider does with it.

What should an accounting firm's AI policy include?

A firm policy should cover approved and prohibited tools, what client data may and may not be entered, the consent and disclosure process, who reviews AI output and how, training, vendor review, and how often the policy is reviewed. The AICPA publishes a Small Firm Generative AI Policy Template as a starting point.

How long does it take to become AI-ready?

A focused six-month roadmap can take many firms from unmanaged to governed, depending on size, starting point, and busy-season calendars. AdvancedBITS builds the plan around your deadlines.

How much does an AI readiness assessment cost?

AdvancedBITS offers a complimentary Accounting Technology & Compliance Readiness Assessment at no cost, with no obligation.

Does AdvancedBITS provide legal, tax, or professional-standards advice?

No. AdvancedBITS provides technology, cybersecurity, and AI readiness services and works alongside your attorney, accountant, and insurance broker. Your counsel decides what the rules require of your firm.

Next step: a complimentary readiness assessment

> ### Schedule Your Free Accounting Technology & Compliance Readiness Assessment
>
> An AdvancedBITS specialist will review your sign-in protection, Microsoft 365 permissions, devices, backups, vendor access, and AI use, and give you a plain-language list of priorities against the five readiness areas. No cost, no obligation.
>
> **[Schedule My Free Assessment]** Call **561-300-3015** | sales@advancedbits.com | www.advancedbits.com

About AdvancedBITS. AdvancedBITS provides managed IT, cybersecurity, and AI guardrails for accounting and tax firms, with 11+ years of managed services experience, a SOC 2 Type II examined security practice, a 98% client retention rate, and regional offices in Florida, North Carolina, Texas, and Oregon.

Related AdvancedBITS resources: Accounting and tax firm landing page; IT Spend Playbook for Accounting Firms; WISP compliance guide; Accounting firm cybersecurity case study.

Sources

Checked October 26, 2026. Secondary sources are labeled. Verify legal and regulatory points with the primary source and your counsel.

1. Karbon. The State of AI in Accounting Report 2026 (accounting practice-management vendor). https://karbonhq.com/resources/ebooks/state-of-ai-accounting-report-2026/
2. CNBC. Can your tax preparer use AI without telling you? (August 4, 2026), reporting the Blue J and CPA.com June 2026 survey and AICPA comments. https://www.cnbc.com/2026/08/04/ai-tax-preparers.html
3. Atlas CPA Index. AI at Accounting Firms in 2026 (August 17, 2026), summarizing Federal Reserve, Thomson Reuters, Blue J and CPA.com, and BILL and NewtonX data. https://atlascpaindex.com/news/ai-adoption-accounting-firms-2026
4. Financial Cents. The State of AI in Accounting and Bookkeeping 2026 (vendor survey of 486 professionals). https://financial-cents.com/resources/guides/the-state-of-ai-in-bookkeeping-accounting/
5. Microsoft. 2024 Work Trend Index (May 8, 2024). https://news.microsoft.com/source/2024/05/08/microsoft-and-linkedin-release-the-2024-work-trend-index-on-the-state-of-ai-at-work/
6. eDiscovery Today. 2026 Cost of a Data Breach Report by IBM (July 30, 2026). https://ediscoverytoday.com/2026/07/30/2026-cost-of-a-data-breach-report-by-ibm-cybersecurity-trends/
7. IRS Office of Professional Responsibility. Issue 2026-19, Introductory Guidelines for Responsible AI Use in Federal Tax Practice (June 24, 2026). https://www.irs.gov/pub/opr-taxpros/issue-number-2026-19-introductory-guidelines-for-responsible-ai-use-in-federal-tax-practice.pdf
8. Verito. Do Tax Preparers Have to Disclose AI Use to Clients? (August 14, 2026; secondary reporting on OPR Alert 2026-19). https://verito.com/blog/ai-tax-preparer-disclosure-requirements/
9. Sanitize. Can tax preparers use ChatGPT? Section 7216, WISP and AI rules (updated October 9, 2026; secondary commentary). https://sanitizedocs.com/guides/tax-preparers-ai-client-data.html
10. IRS. Written Information Security Plans are essential for tax pros, Tax Tip 2026-49 (June 16, 2026). https://www.irs.gov/newsroom/written-information-security-plans-are-essential-for-tax-pros
11. IRS Office of Professional Responsibility. Issue 2026-22, How to Be a Careful WISP(er) (July 22, 2026). https://www.irs.gov/pub/opr-taxpros/issue-number-2026-22-how-to-be-a-careful-wisper.pdf
12. ComplianceDocsHQ. WISP and the FTC Safeguards Rule for Tax and Accounting Firms (updated October 21, 2026; secondary summary of 16 CFR 314.4). https://compliancedocshq.com/guides/wisp-ftc-safeguards
13. Prometheus. AICPA Ethics Framework for AI Use at CPA Firms (updated October 26, 2026; secondary review). https://www.prometheusconsulting.ai/guide/ai-aicpa-ethics-framework
14. Journal of Accountancy. AI and the audit: AICPA publishes practice aid to assist auditors (October 13, 2026). https://www.journalofaccountancy.com/news/2026/oct/ai-and-the-audit-aicpa-publishes-practice-aid-to-assist-auditors/
15. AICPA column by Sarah Beckett Ference, CPA. What are the risks of accounting firms using generative AI? https://www.cpai.com/Education-Resources/My-Firm/Data-Security-Risk-Management/Generative-AI-and-risks-to-CPA-firms
16. Microsoft Learn. Configure a secure and governed foundation for Microsoft Copilot. https://learn.microsoft.com/en-us/microsoft-365/copilot/configure-secure-governed-data-foundation-microsoft-365-copilot

17. Microsoft. Secure and Govern Microsoft 365 Copilot, foundational deployment guidance (March 2026). https://download.microsoft.com/download/6f833c52-da53-4ec6-99ac-84d6540f8479/Secure%20and%20Govern%20M365%20Copilot%20blueprint_PDF_vMar24.pdf

Publishing and reviewer notes (not part of the guide; remove before publishing)

Title tag (54 characters): AI Readiness Guide for Accounting Firms | AdvancedBITS

Meta description (153 characters): A practical AI readiness guide for accounting and tax firms: the rules that apply, Microsoft 365 and Copilot prep, human review, and a six-month roadmap.

URL slug: /resources/ai-readiness-guide-accounting-firms (canonical must match the live address).

H1: AI Readiness Guide for Accounting Firms. Use one H1, render each section heading as an H2 and each FAQ question as an H3, and show “Last updated” near the top.

Primary keywords: AI readiness for accounting firms, AI policy for CPA firms, AI governance for accounting firms, Copilot for accounting firms.

Secondary keywords: shadow AI accounting firms, Section 7216 AI consent, WISP AI, Microsoft 365 permissions Copilot, human in the loop accounting, AI vendor evaluation for CPA firms.

Schema: Article + FAQPage + Organization in the companion file AdvancedBITS_AI_Readiness_Guide_Accounting_JSONLD.html, built from the same 10 FAQ answers. Validate before release.

Internal links: Link the Related resources line to the published pages, and link back from the Accounting landing page card. That card currently names this guide “AI Governance for Accounting Firms”; use one name everywhere.

Confirm the model: The five-area model (See, Protect, Govern, Review, Prove) and four stages were written for this guide from the Accounting card’s description. If AdvancedBITS already has an official AI Readiness Model, align the names before publishing.

Confirm facts: The 11+ years, SOC 2 Type II wording, 98% retention figure, and offices line are repeated from your other pages and need your confirmation. Accounting is not on the approved industries-served list, so this guide makes no client claims; the example is a labeled composite.

Counsel review: Have counsel review Table 2, the Section 7216 statements, and the FAQ answers on consent and disclosure. The Section 7216 and FTC points rest on secondary commentary, and the AICPA ethics points on a secondary review, so verify against the primary sources.

Conflict to resolve: Sources disagree on what PTIN renewal requires about a WISP, so this guide states no PTIN requirement. Your Accounting landing page and earlier WISP content may state one; verify with the IRS.

Vendor sources: Karbon, Financial Cents, and Verito sell related software or services. The Financial Cents result covers mostly small firms. The IBM figure covers all industries.

Brand facts: Phone 561-300-3015, 11+ years. Your Accounting landing page still shows 20+ years and 561-300-3030.