Accounting Firm AI Governance Checklist

Summit Guard

A practical checklist for accounting firms using or considering ChatGPT, Claude, Microsoft Copilot, Gemini, AI-enabled tax and accounting software, client portals, document tools, workflow tools, and practice-management platforms.

Use this checklist to create a clear starting point for AI visibility, client-data boundaries, human review, vendor settings, Microsoft 365 exposure, and leadership evidence.

> **Governance-only note:** This resource provides practical AI governance guidance. Firms should use qualified advisers for legal, tax, accounting, professional, or client-specific obligations.

How to use this checklist

For each item, mark:

- **Done:** documented and evidence available.
- **In progress:** partly defined but incomplete.
- **Action needed:** unclear, informal, or not reviewed.

Assign an owner and due date for every action needed.

1. AI tool visibility

- ■ We have a current register of AI tools and AI-enabled features used by the firm.
- ■ The register includes ChatGPT, Claude, Gemini, Microsoft Copilot, tax software, accounting software, payroll tools, client portals, document tools, CRM tools, meeting assistants, and browser extensions.
- ■ We can distinguish personal accounts from firm-managed accounts.
- ■ Each tool has an approved, restricted, under-review, or not-approved status.
- ■ Each approved or restricted tool has a business owner and review date.
- ■ Staff know how to request a new AI tool or feature before using it with firm or client information.

Notes / owner / due date:

2. Client-data boundaries

- ■ Staff have plain-English rules for information that must not be entered into open or unapproved AI tools.
- ■ The rules cover client financial statements, management accounts, tax context, tax file numbers, payroll data, bank records, transaction files, working papers, reconciliations, forecasts, valuations, correspondence, and portal records.
- ■ Client-specific restrictions can be recorded and checked before AI use.
- ■ Approved use cases explain when information must be de-identified, summarised, replaced with synthetic examples, or approved first.
- ■ Staff know who to ask when a use case is unclear.

Notes / owner / due date:

3. Approved use cases

Start with useful lower-risk use cases.

- ■ Drafting internal checklists from firm-approved templates.
- ■ Improving readability of non-sensitive client education material.
- ■ Summarising vendor documentation or software release notes.
- ■ Creating internal meeting agendas from non-confidential notes.
- ■ Drafting training material for review.
- ■ Preparing first-draft internal process notes.

Restricted use cases should need extra review before use.

- ■ Client-specific financial commentary.
- ■ Tax-related drafts or research support.
- ■ Reports, recommendations, or management letters.
- ■ Calculations, formulas, reconciliations, or spreadsheet analysis.
- ■ Payroll, employee, or personal information.
- ■ Client documents, portal records, or email threads.

Notes / owner / due date:

4. Human review before client use

- ■ AI-generated material is checked by an accountable person before it influences client work.
- ■ Reviewers check numbers, formulas, assumptions, source data, context, and limitations.
- ■ Reviewers check whether the output overstates certainty.
- ■ Reviewers check confidentiality, privacy, and client-specific restrictions.
- ■ Higher-impact work receives stronger review.
- ■ Important client-facing outputs have review evidence that can be inspected later.

Notes / owner / due date:

5. Vendor and SaaS settings

For each approved or restricted tool, ask:

- ■ What firm or client data is processed by the AI feature?
- ■ Is data used to train or improve vendor models?
- ■ Can training or product-improvement use be switched off for firm data?
- ■ Where are prompts, files, outputs, transcripts, and logs stored?
- ■ How long is information retained?

- ■ What administrator controls, user-management features, exports, and logs are available?
- ■ How is access removed when a user leaves or changes role?
- ■ How are material feature changes communicated?

Notes / owner / due date:

6. Microsoft Copilot and Microsoft 365 exposure

If Copilot is being piloted or considered, review what licensed users can access.

- ■ Copilot rollout scope is documented by users, teams, and service lines.
- ■ High-risk SharePoint sites, Teams spaces, OneDrive folders, mailboxes, and shared mailboxes are identified.
- ■ Client folders, archived content, HR, finance, leadership, templates, pricing, and internal methodology repositories are included where relevant.
- ■ Broad groups, inherited permissions, old sharing links, and guest access are reviewed for high-risk locations.
- ■ Staff understand that Copilot can work with content a user can already access.
- ■ Permission review actions are tracked before pilot expansion.

Notes / owner / due date:

7. Incident and exception handling

- ■ Staff know how to report accidental or unclear AI use.
- ■ The firm records which tool was used and what data may have been entered.
- ■ Client, personal, payroll, or financial information issues have a clear escalation path.
- ■ Exceptions record who approved the use and why.
- ■ Repeat issues are used to update guidance and training.

Notes / owner / due date:

8. Leadership evidence pack

Leadership should be able to inspect:

- ■ AI tool register with owners and review dates.
- ■ Approved, restricted, and prohibited use cases.
- ■ Client-data boundary guidance.
- ■ Vendor setting notes.
- ■ Copilot permission review notes.
- ■ Human review examples for important outputs.
- ■ Staff guidance or briefing material.
- ■ Exception and incident log.

- ■ Action tracker for unresolved risks.

Notes / owner / due date:

30-minute leadership agenda

1. Confirm which AI tools and AI-enabled software are already in use.
2. Identify the top three client-data boundary risks.
3. Pick one client-facing workflow and define the required human review step.
4. Assign an owner for vendor setting checks and Copilot exposure review.
5. Agree the next governance action: register, policy refresh, workflow review, or focused triage.

Need a practical starting point?

Summit Guard helps accounting firms turn AI usage into visible governance, clear data boundaries, human review points, and leadership-ready evidence.

Contact Summit Guard:
https://summitguard.com.au/contact?source=/insights/accounting-firm-ai-governance-checklist