SUMMIT GUARD CHECKLIST

Professional Services AI Governance Checklist

A practical Phase 1 check for law, accounting, advisory, and consulting firms using ChatGPT, Claude, Copilot, Gemini, and AI-enabled SaaS.

Governance-only disclaimer: This checklist provides practical governance guidance only. Firms should use qualified advisers for legal, professional, or assurance obligations.

1. Tool visibility

- ■ Current list of approved AI tools, including ChatGPT, Claude, Copilot, Gemini, and AI-enabled SaaS features.
- ■ Known teams, matters, client segments, or service lines using each tool.
- ■ Intake path for staff to request a new AI tool or feature before use with firm or client information.
- ■ Clear distinction between personal accounts and firm-managed accounts.
- ■ Nominated owner for keeping the AI tool register current.

2. Client-data boundaries

- ■ Plain-English rules for what client, confidential, personal, privileged, financial, commercial, or sensitive information must not be entered into open AI tools.
- ■ Approved use cases explain what data may be used, what must be removed, and when synthetic or de-identified examples are preferred.
- ■ Client-specific restrictions can be recorded and surfaced before work enters an AI tool.
- ■ Process exists for accidental data entry into an AI tool, with a named escalation point.

3. Human review before client use

- ■ AI-generated material is reviewed by an accountable person before use in client work, analysis, reports, correspondence, calculations, or deliverables.
- ■ Review expectations are proportionate to risk; higher-impact client work receives more careful checking.
- ■ Reviewers check accuracy, context, sources, assumptions, confidentiality, tone, and client-specific requirements.
- ■ The firm can show where human review was performed for important client-facing outputs.

4. Vendor, logging, and retention questions

- ■ What data is sent to the vendor or model provider, and is it used to train or improve models?
- ■ Can training or product-improvement use be switched off for firm data?
- ■ Where are prompt, file, output, and user activity histories stored, and for how long?
- ■ What administrator controls, access logs, export options, and user-management features are available?
- ■ What happens when a user leaves the firm or changes role, and how are service changes communicated?

5. Evidence leadership should be able to show

- AI tool register with owner, status, approved use cases, and review date.
- Short staff guidance covering approved tools, restricted data, and escalation points.
- Records showing who approved higher-risk AI use cases and why.
- Examples of human review steps for important client-facing outputs.
- Vendor notes covering data use, retention, logging, access controls, and account administration.
- A simple incident and exception log for accidental use, unclear cases, or control gaps.
- Leadership review notes showing decisions, open risks, and next actions.

6. Next-step triage

GREEN: usable with routine controls	AMBER: use only after extra review	RED: pause until boundaries are set
• Firm-managed tool or approved SaaS. • Low-sensitivity input data. • Clear human review before client use. • Known vendor settings and retention behaviour. • Evidence can be produced without a scramble.	• Client information may be involved. • Output may influence client decisions or firm recommendations. • Vendor logging or retention settings are unclear. • Personal accounts or unsanctioned tools are in use. • Human review is informal or hard to evidence.	• Confidential, privileged, sensitive, or high-impact material may be exposed. • No clear owner, approval path, or review process exists. • Vendor data-use position is unknown. • The firm could not explain how the AI output was checked. • Client restrictions may apply and have not been considered.

Suggested 30-minute leadership agenda

- Confirm which AI tools and AI-enabled SaaS features are already in use.
- Identify the top three client-data boundary risks.
- Pick one client-facing workflow and define the required human review step.
- Assign an owner for tool visibility and vendor setting checks.
- Agree the next governance action: register, policy refresh, workflow review, or targeted triage.

Need a practical starting point? Contact Summit Guard: https://summitguard.com.au/contact

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