Axiom Sovereign

TECHNOLOGY SOVEREIGNTY ADVISORY

7-STEP IMPLEMENTATION CHECKLIST — CPA FIRMS, LAW FIRMS, MEDICAL PRACTICES

AI Governance Checklist for Professional Services

Shadow AI · Policy Framework · Ethics Alignment · Technical Controls

v1.0 — 2026

Axiom Sovereign LLC · Severna Park, MD · info@axiomsovereign.com · axiomsovereign.com

AI Governance Checklist for Professional Services

About This Document

This checklist provides a 7-step AI governance framework designed specifically for CPA firms, law firms, medical practices, management consultancies, and other professional services organizations deploying AI tools. It was developed by Axiom Sovereign based on emerging regulatory requirements from AICPA, the American Bar Association, HHS Office for Civil Rights, the EU AI Act, and the NIST AI Risk Management Framework, combined with practical experience implementing AI governance programs for mid-market professional services clients.

AI governance in professional services is not optional. It is a professional ethics obligation. AICPA ET Section 1.700 (Confidential Client Information), ABA Model Rule 1.6 (Confidentiality), and HIPAA's minimum necessary standard all create firm obligations that apply when AI tools process client or patient data. This checklist helps you meet those obligations systematically.

The Core Problem This Checklist Solves

Most professional services firms have staff using AI tools that were approved for a different purpose entirely — personal productivity — but are being used with client data, patient records, and legally privileged communications. The firm has taken on legal and ethical liability it does not know about. This checklist gives you a structured method to discover that exposure, establish governance, implement controls, and create a defensible, documented program.

How to Use This Checklist

Work through the seven steps in sequence. Each step builds on the previous one — you cannot effectively write an AI use policy (Step 4) without first knowing what tools are in use (Step 1) and what data they process (Step 2). Complete each step before moving to the next.

For each checklist item, mark: **Complete** (implemented and documented), **In Progress** (partially implemented), or **Not Started** (action required). Items marked Not Started in Steps 1–4 should be treated as urgent — these represent your most immediate governance and liability gaps.

STEP 1: DISCOVER WHAT AI IS ACTUALLY BEING USED

You cannot govern what you do not know exists. Most professional services organizations discover — often through an anonymous survey or network traffic analysis — that staff are using 5 to 10 AI tools that leadership had no knowledge of. The most dangerous are tools that ingest client data: summarization tools that receive case files, AI assistants that read

email, transcription tools that record client meetings, and tax or audit software with embedded AI that trains on input data.

■ Shadow AI Discovery Survey

Survey all staff asking specifically about ChatGPT (free and Plus), Microsoft Copilot, Google Gemini, Grammarly, Otter.ai, Harvey AI, Clio Duo, Thomson Reuters CoCounsel, and any other AI tools they use for work. Make clear this is not punitive — the goal is understanding, not discipline. Anonymous surveys consistently yield more complete results.

■ AI Tool Inventory Creation

Document every AI tool identified: vendor name, what it does, what data it processes, whether client data is entered, subscription cost, who is using it, and whether any formal approval was sought. This inventory becomes the foundation of your governance program.

■ Initial Risk Classification

Classify each tool in your inventory into one of three categories: Approved (cleared for use with or without restrictions), Conditional (approved with specific restrictions on data types), or Prohibited (banned from use with client, patient, or matter data until reviewed and approved).

STEP 2: ASSESS YOUR DATA EXPOSURE

Once you know what tools are in use, the next step is understanding what data has been — and is being — processed by those tools. This step often produces the most uncomfortable findings. Staff routinely paste client tax data into ChatGPT for formatting help, upload patient records to AI transcription services, and enter legal matter details into AI research tools, without realizing the data retention, training, and third-party sharing implications of doing so.

■ Data Type Mapping by Tool

For each tool in your inventory, identify the types of data that staff enter or upload: client PII (names, SSNs, addresses, financial data), protected health information (PHI), legally privileged communications, tax return data, audit workpapers, or trade secrets. Map each tool to the data types it processes.

■ Vendor Terms of Service Review

Review the terms of service and privacy policies for each AI tool. The four critical questions: (1) Does the vendor train on your inputs? (2) How long does the vendor retain your data? (3) Can you opt out of training, and if so, how? (4) Who at the vendor can access your data? Document your findings for each tool.

■ Professional Obligation Conflict Assessment

Map your professional confidentiality obligations against each tool's data handling. AICPA ET 1.700.001 prohibits disclosure of confidential client information. ABA Model Rule 1.6 prohibits disclosure of client information without informed consent. HIPAA's minimum necessary standard limits PHI use. Flag any tool whose data handling conflicts with these obligations as Prohibited until contractual protections are established.

STEP 3: ESTABLISH GOVERNANCE STRUCTURE

AI governance requires ownership. Without a named individual or committee with authority to approve and prohibit AI tool use, any policy you write will be unenforceable. This step establishes the governance infrastructure that all subsequent steps depend on.

■ Designate an AI Governance Owner

Assign a named individual responsible for AI governance — typically the managing partner, COO, chief compliance officer, or a fractional DPO or vCISO. This person has authority to approve AI tools, enforce the acceptable use policy, and respond to AI-related incidents. Without named ownership, AI governance programs fail consistently.

■ Establish an AI Governance Committee (Firms Over 20 People)

For firms with 20+ staff, form a small AI governance committee (2–4 people) representing operations, compliance, and practice leadership. This committee reviews new tool requests, monitors the AI landscape, and updates policy. For smaller firms, the governance owner handles these functions.

■ Define Evaluation Criteria for New Tools

Document the criteria a new AI tool must meet before approval: independent security review completed, data processing agreement or BAA executed, confirmed opt-out of training on client data, U.S. data residency where required by client contracts or regulations, and vendor SOC 2 report available. These criteria prevent ad hoc tool adoption.

STEP 4: WRITE AND DEPLOY CORE POLICIES

With your inventory complete and governance structure in place, you can now write AI policies that are grounded in reality — addressing the actual tools your staff use, the actual data your organization handles, and the actual professional obligations that apply to your practice. Policies copied from the internet that do not reflect your specific environment are not enforceable and provide no meaningful protection.

■ AI Acceptable Use Policy

This is your primary AI governance document. It must cover: the approved AI tool list (by name), categories of data that may never be entered into any AI tool (client SSNs, PHI, privileged communications), when and how to disclose AI use to clients, reporting obligations for suspected AI-related data incidents, and consequences for violations. All staff must sign acknowledgment. Annual re-certification required.

■ AI Vendor Evaluation and Approval Procedure

A documented process for how new AI tools are evaluated, approved, and added to the approved list — or rejected. This procedure should specify who can request a new tool, what evaluation steps are required, who has approval authority, and how long the review process takes. Without this, the approved list becomes stale within months.

■ Client Disclosure Policy

Determine when and how AI use is disclosed to clients. ABA Formal Opinion 512 (2023) requires that attorneys maintain competence in AI technologies used in their practice. AICPA guidance is evolving rapidly. Determine your disclosure position — proactive disclosure in engagement letters is increasingly the professional standard.

STEP 5: IMPLEMENT TECHNICAL CONTROLS

Policy without technical controls is aspirational, not operational. Staff — particularly remote staff — will use unapproved tools unless those tools are technically blocked or monitored. Technical controls also provide the audit evidence you need to demonstrate to regulators, insurers, and clients that your AI governance program is real.

■ DNS-Level or Web Filtering for Unapproved AI Tools

Configure your web content filtering or DNS filtering solution to block access to unapproved AI services from organization-managed networks and devices. For remote workers, this requires the filtering to operate at the endpoint level, not just the office network perimeter.

■ Data Loss Prevention (DLP) Configuration

Configure DLP policies in Microsoft 365 Purview, Google Workspace DLP, or your endpoint security solution to detect and alert on — or block — the transmission of sensitive data categories (SSNs, account numbers, PHI identifiers) to external AI services. DLP provides both a preventive control and an audit trail.

■ Microsoft 365 Copilot Configuration (If Applicable)

If your organization uses or plans to deploy Microsoft 365 Copilot, configure data access controls before deployment. Copilot accesses all data the user can access — if your permissions are not correctly scoped, Copilot can expose data to users who should not have access. Enable Copilot interaction logging for audit purposes.

STEP 6: TRAIN YOUR STAFF

Governance programs fail when staff do not understand why the rules exist. A signed policy acknowledgment without training is a paper exercise. Effective AI governance training explains the professional and regulatory context, not just the rules. Staff who understand why client data cannot go into public AI tools are far more likely to comply than staff who have simply been told not to.

■ Initial AI Governance Training

All staff complete AI governance training before being authorized to use any approved AI tool. Training must cover: the approved tool list and how to request additions, data types that may never be entered into AI tools and why, how to recognize and report a potential AI-related data incident, and applicable professional obligations for the practice area. Document completion by individual with date and training content.

■ AI-Enhanced Phishing and Social Engineering Awareness

AI-generated phishing emails are indistinguishable from legitimate correspondence in most cases. AI can now clone voices and generate deepfake video. Update your security awareness training to cover AI-enhanced threats — particularly business email compromise and voice cloning fraud targeting wire transfers and client account changes.

■ Annual Recertification

Require annual policy recertification by all staff. The AI landscape changes faster than any other technology domain — new tools, new regulations, and new threat vectors emerge continuously. Annual training with updated content maintains program effectiveness and demonstrates ongoing diligence to regulators and insurers.

STEP 7: MONITOR, AUDIT, AND CONTINUOUSLY IMPROVE

AI governance is not a one-time project. Vendors change their terms of service. New tools emerge. Regulations evolve. Staff circumstances change. Your governance program must include ongoing monitoring, periodic audits, and a formal update cycle to remain effective.

■ Quarterly AI Tool Inventory Review

Review your approved tool list quarterly. Check for: changes to vendor terms of service or ownership, new AI tools that have emerged that staff may be using, tools that have been deprecated or acquired, and changes in the regulatory status of tools you have approved. Remove or restrict tools that no longer meet your criteria.

■ Incident Tracking and Post-Incident Review

Establish a log for AI-related incidents and near-misses: staff who entered prohibited data into an unapproved tool, vendor breaches involving your data, and client concerns about AI use. Each incident is an opportunity to improve your controls. A post-incident review should identify the root cause and update policy or controls accordingly.

■ Annual Regulatory Update Assessment

Monitor AICPA, ABA, state bar, HHS OCR, and EU AI Act developments at least annually. Subscribe to regulatory bulletins from your professional associations. The regulatory landscape for AI in professional services is moving faster than most compliance programs can track without dedicated monitoring.

PROFESSIONAL ETHICS QUICK REFERENCE

The following table summarizes the key professional ethics obligations that intersect with AI governance for the primary professional services sectors. These obligations exist regardless of whether your organization has an AI governance program — governance is how you meet them.

Profession	Governing Body	Primary AI-Relevant Rule	The Core Obligation	Key AI Risk
CPA / Accounting	AICPA	ET Section 1.700 — Confidential Client Info	Must not disclose or use confidential client information without consent.	Client tax/financial data entered into AI tools that train on inputs or share with third parties.

Profession	Governing Body	Primary AI-Relevant Rule	The Core Obligation	Key AI Risk
Law	ABA / State Bars	Model Rules 1.1, 1.6, 5.3	Competence in technology used in practice. Confidentiality of all client information.	Privileged matter data in AI tools. Inadequate supervision of AI-generated work product.
Healthcare	HHS OCR	HIPAA Privacy & Security Rules	Minimum necessary standard for PHI. BAA required for all PHI processors.	PHI in AI transcription, documentation, or diagnostic tools without a BAA.
All	FTC / State AGs	Section 5 — Unfair or Deceptive Practices	Material representations about data practices must be accurate.	Stating "we protect your data" while using AI tools that train on that data.

Ready to Implement This Framework?

Axiom Sovereign deploys AI governance programs for professional services firms — not just advisory, but hands-on execution. We author your policies, configure your technical controls, deliver staff training, establish your governance structure, and manage ongoing compliance. Most engagements complete initial implementation within 60–90 days.

Schedule a complimentary discovery call: calendly.com/cmissimore-6zkc/30min

Email: info@axiomsovereign.com · **Web:** axiomsovereign.com