Axiom Sovereign

TECHNOLOGY SOVEREIGNTY ADVISORY

SELF-ASSESSMENT FRAMEWORK — PROFESSIONAL SERVICES ORGANIZATIONS

Technology Sovereignty Risk Assessment

AI Vendor Risk · Regulatory Exposure · Cybersecurity Maturity

v1.0 — 2026

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

Technology Sovereignty Risk Assessment

About This Assessment

The Technology Sovereignty Risk Assessment is a structured evaluation tool developed by Axiom Sovereign to help mid-market professional services organizations quantify their exposure across three interconnected risk domains: AI vendor dependency, regulatory compliance, and cybersecurity program maturity. Unlike generic security checklists, this tool is designed specifically for the risk profile of CPA firms, law firms, medical practices, NGOs, and similar organizations that hold sensitive client data but typically lack dedicated security leadership.

Technology sovereignty — the strategic ability to control your technology decisions and understand the implications of your vendor dependencies — has emerged as a critical business risk. The rapid proliferation of AI tools, expanding privacy regulations, and growing sophistication of cyber threats have created a compounding risk environment that most mid-market organizations are unprepared to navigate. This assessment gives you a scored, actionable baseline so you know exactly where you stand.

Why This Matters Now

72% of professional services firms have employees using AI tools without formal governance. A single AI governance failure can trigger AICPA ethics violations, attorney-client privilege breaches, HIPAA penalties of up to $50,000 per violation, or GDPR enforcement actions. The average cost of a professional services data breach is $4.9 million. This assessment helps you identify where you stand before those failures occur.

How to Use This Assessment

This assessment consists of three scored sections. Complete each section honestly — optimistic scoring defeats the purpose. If you are uncertain whether a control exists, score it 0.

Step 1 — Score Each Control: For each item, assign: 0 (not addressed — no policy, process, or control exists), 1 (partially addressed — something exists but is informal, incomplete, or inconsistently applied), or 2 (fully addressed — documented, implemented, and regularly reviewed).

Step 2 — Note Priority Gaps: Mark every item scored 0 in the Notes column. These are your highest-priority remediation targets regardless of your total score. A zero on MFA or incident response represents more immediate risk than your aggregate score may suggest.

Step 3 — Calculate Your Total: Sum all three sections and compare to the Risk Rating table at the end of this document. Your rating maps to a recommended action level.

Step 4 — Act on Your Results: Schedule a complimentary 30-minute discovery call with Axiom Sovereign to discuss your results, receive a prioritized roadmap, and determine whether and how we can help. No obligation.

Recommended cadence: Complete annually and after any significant technology change, regulatory development, or security incident.

SECTION 1: AI VENDOR DEPENDENCY & GOVERNANCE RISK

This section evaluates whether your organization knows what AI tools are in use, what data they process, and whether appropriate governance, contractual protections, and response capabilities are in place. For professional services firms, AI governance is a professional ethics obligation under AICPA, ABA, and healthcare regulations — not merely a technology question.

#	Control Item	Why It Matters	Score (0–2)	Notes
1.1	Complete, current inventory of all AI tools in use — including unapproved tools (shadow AI). Reviewed quarterly.	You cannot govern what you do not know exists. Most firms have 3–5x more AI tools in use than leadership believes.		
1.2	Each AI vendor evaluated for data residency and regulatory jurisdiction (U.S.-controlled vs. foreign).	Foreign-controlled AI creates geopolitical risk. TikTok bans and Schrems II show data jurisdiction has real consequences.		
1.3	Terms of service reviewed for all AI tools. We know whether each vendor trains on our data, retains inputs, or shares with third parties.	Most professionals using ChatGPT have never read OpenAI's data use terms. Enterprise plans often have opt-outs that free plans lack.		
1.4	Formal approved AI vendor list exists. New tools require evaluation and approval before staff use them.	Without an approval process, any employee can introduce any tool — including ones with no data protection, no BAA, and no security controls.		
1.5	Shadow AI addressed via policy, technical controls (DNS/DLP), or regular staff communication. Unapproved tool usage can be identified.	Policy alone does not stop shadow AI. Technical controls are needed, especially for remote staff.		
1.6	Data Processing Agreements (DPAs) or Business Associate Agreements (BAAs) with all AI vendors that process personal data or PHI.	Using an AI tool that processes PHI without a BAA is a per se HIPAA violation. GDPR requires DPAs for all data processors.		
1.7	Geopolitical and sovereignty risk assessed for key AI vendors — ownership structure, government access obligations, cross-border implications.	NIST AI RMF and EU AI Act require vendor risk assessment that goes beyond security to include governance and systemic risk.		

#	Control Item	Why It Matters	Score (0–2)	Notes
1.8	Process defined for responding to AI vendor security incidents — identifying client data exposure, notifying affected parties, replacing the vendor.	When an AI vendor is breached, you are a secondary victim. Most HIPAA/GDPR notification deadlines cannot be met without a pre-existing plan.		
	SECTION 1 TOTAL	Maximum: 16 points		

SECTION 2: REGULATORY EXPOSURE & COMPLIANCE POSTURE

Mid-market professional services firms face an expanding web of overlapping regulatory requirements: HIPAA for healthcare data, GDPR for EU data subjects, CPRA and state privacy laws for U.S. residents, and emerging AI-specific regulations including the EU AI Act. The cost of non-compliance is not abstract — HIPAA penalties reach $50,000 per violation, and GDPR enforcement has exceeded billions in cumulative fines. This section evaluates whether your compliance posture is documented and defensible.

#	Control Item	Why It Matters	Score (0–2)	Notes
2.1	All applicable regulations formally identified based on industry, client types, geographic operations, and data types handled.	Many organizations discover GDPR or HIPAA obligations only after a complaint — not proactively. Identification is the foundation of compliance.		
2.2	AI governance policies specifically address how AI tools may be used with client/patient data, referencing applicable regulations (AICPA, ABA, HIPAA, EU AI Act).	Generic acceptable use policies predating AI are not sufficient. Regulators, insurers, and sophisticated clients now expect AI-specific provisions.		
2.3	HIPAA Security Risk Analysis completed within past 12 months with current Risk Management Plan. (Mark N/A if HIPAA does not apply.)	HIPAA §164.308(a)(1) makes risk analysis mandatory. It is the most-cited HIPAA violation in OCR audits. Many practices have never completed one.		
2.4	Current data inventory maintained: what personal data we hold, where stored, who can access it, how long retained. ROPA maintained for GDPR-covered organizations.	You cannot respond to data subject rights (access, deletion, portability) without knowing what data you hold. This is foundational under GDPR and CPRA.		
2.5	Documented procedures for DSARs — access, deletion, correction, opt-out — within regulatory timeframes (30 days GDPR; 45 days CPRA).	DSAR volume is increasing. Without procedures, organizations routinely miss deadlines, creating additional violations on top of the underlying issue.		
2.6	Cross-border personal data transfers to non-EU countries covered by SCCs, adequacy decisions, or equivalent mechanisms. (Mark N/A if no EU subjects.)	Post-Schrems II, transferring EU personal data to the U.S. via AI tools without legal mechanisms is a GDPR violation frequently overlooked by U.S. firms.		

#	Control Item	Why It Matters	Score (0–2)	Notes
2.7	U.S. state privacy law obligations assessed — CPRA (CA), VCDPA (VA), CPA (CO), and others applicable to our operations.	As of 2026, 19+ states have enacted comprehensive privacy laws. U.S. organizations can no longer treat privacy as a GDPR-only issue.		
2.8	Cyber insurance policy current, coverage limits appropriate, and all carrier-required security controls are actually implemented.	Carriers are increasingly denying claims based on misrepresentation — controls stated on the application that were not actually in place.		
	SECTION 2 TOTAL	Maximum: 16 points		

SECTION 3: CYBERSECURITY PROGRAM MATURITY — NIST CSF 2.0

NIST Cybersecurity Framework 2.0 (published February 2024) is the most widely adopted cybersecurity framework in the United States and is referenced by cyber insurance carriers, government contractors, and enterprise procurement teams. A mature cybersecurity program does not require an enterprise IT department — it requires clear ownership, documented policies, and consistent execution of a defined set of controls appropriate to your risk profile. This section evaluates your program against all six CSF 2.0 functions.

#	Control Item	CSF Function & Rationale	Score (0–2)	Notes
3.1	Documented cybersecurity policy reviewed and approved by leadership within past 12 months. Defines security objectives, governance, roles, and violation consequences.	GOVERN: Policy is the foundation. Without a documented, leadership-approved policy, all other controls are ad hoc. Annual review ensures currency with the threat landscape.		
3.2	Current asset inventory of all hardware, software, cloud services, and data repositories used by the organization.	IDENTIFY: You cannot protect what you do not know you have. Asset inventory is prerequisite for vulnerability management, patching, and access control.		
3.3	MFA enforced (not just recommended) for all staff on all systems: email, cloud services, VPN, remote access, and privileged accounts.	PROTECT: MFA is the single highest-impact control for preventing unauthorized access. Most ransomware and business email compromise attacks exploit accounts without MFA.		
3.4	All staff complete documented security awareness training annually. Covers: phishing, AI tool governance, data handling, incident reporting.	PROTECT: Human error causes 74%+ of security incidents. Training with documentation is required by HIPAA, expected by cyber insurers, and reduces incident frequency.		
3.5	Automated monitoring and alerting for security events — failed logins, large exports, admin changes, malware. Alerts reviewed by a responsible person.	DETECT: Modern threats operate inside environments for weeks before discovery. Automated alerting shortens detection time from months to hours.		
3.6	Documented and tested incident response plan with roles, escalation, external contacts (IR firm, legal, insurer), and regulatory notification requirements. Reviewed annually.	RESPOND: Unplanned incident response costs 3–5x more than planned response. Most regulatory notification deadlines (GDPR: 72 hours, HIPAA: 60 days) require pre-existing plans.		

#	Control Item	CSF Function & Rationale	Score (0–2)	Notes
3.7	Backups performed regularly, stored separately from production (offline or immutable cloud), encrypted, and tested for restoration quarterly.	RECOVER: Untested backups are not backups. Ransomware specifically targets and destroys backup systems. Immutable backups are the primary ransomware recovery mechanism.		
3.8	Regular vulnerability assessments or penetration testing of external-facing systems. Critical findings remediated within defined timeframes.	IDENTIFY: Known vulnerabilities in external systems are the most common initial attack vector. Regular scanning identifies these before attackers do.		
3.9	Formal vendor risk management process including security questionnaires, contractual security requirements, and periodic review of vendors with data access.	GOVERN: Most data breaches involve a third party. Vendor risk management is required under HIPAA, expected under GDPR, and a standard cyber insurance requirement.		
3.10	Privileged access managed with least-privilege principles. Admin accounts separate from daily-use accounts. Access reviewed quarterly and revoked promptly when no longer needed.	PROTECT: Over-privileged accounts are the preferred lateral movement path for attackers. Quarterly access reviews are an industry standard expected by auditors and insurers.		
	SECTION 3 TOTAL	Maximum: 20 points		

SCORING GUIDE & RISK RATING

Total your scores from all three sections. Your overall score is a starting point, not a complete picture. Review individual zero-scored items alongside your total — a zero on MFA or incident response represents critical risk regardless of your aggregate score.

Score (max 52)	Risk Rating	What It Means	Recommended Action
45 – 52	LOW RISK	Program is mature and well-documented. Gaps are minor or in advanced controls.	Annual reassessment. Monitor regulatory changes. Maintain program currency.
35 – 44	MODERATE RISK	Program exists but meaningful gaps are present. Regulatory exposure is likely in one or more domains.	Address zero-scored items within 90 days. Consider vCISO engagement to accelerate remediation.
20 – 34	HIGH RISK	Significant gaps across multiple domains. Regulatory exposure is material. Incident probability is elevated.	Immediate program development required. Engage a vCISO or security advisor within 30 days.
0 – 19	CRITICAL RISK	Program is absent or severely underdeveloped. Exposure is acute across all three domains.	Emergency engagement recommended. Contact Axiom Sovereign immediately for rapid assessment.

MY ASSESSMENT RESULTS

Section 1 — AI Vendor Dependency: _____ / 16

Section 2 — Regulatory Exposure: _____ / 16

Section 3 — Cybersecurity Maturity: _____ / 20

TOTAL SCORE: _____ / 52 **RISK RATING:** _____

Zero-scored items requiring immediate action:

_____

_____

_____

NEXT STEPS

Regardless of your score, Axiom Sovereign recommends these immediate actions:

- Review all items scored 0 first — these are your highest-probability failure points.
- Schedule a complimentary 30-minute Technology Sovereignty Discovery Call to review your results and receive a prioritized remediation roadmap specific to your organization.
- Share this assessment with firm leadership — cybersecurity and AI governance are business leadership responsibilities, not IT issues.
- Revisit this assessment in 90 days after beginning remediation to measure improvement.

Schedule Your Complimentary Discovery Call

The Technology Sovereignty Discovery Call is a 30-minute engagement with Cory Missimore, CISSP, AIGP, CIPP/E, CIPP/US, CIPM — Founder of Axiom Sovereign. No sales team. No obligation. We review your results, identify your highest-priority gaps, and give you an honest assessment of what it would take to address them.

Book online: calendly.com/cmissimore-6zkc/30min

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