501CISO
501C CYBERSECURITY LEADERSHIP
Powered by ClearTone Consulting, LLC

501CISO AI Security & Governance Assessment

A Structured One-Time Engagement for Associations and Nonprofits

The Problem

Most associations and nonprofits have deployed Microsoft Copilot, Claude, or ChatGPT without a corresponding security review. The result is a consistent and predictable set of exposures:

- Unaudited Data Access: AI tools connected to SharePoint and OneDrive before permissions were reviewed - making previously obscure files easily discoverable by anyone in the organization
- Data Ingestion Risk: Employees using unauthorized personal AI accounts to process donor records, grant materials, and member PII - risking sensitive information becoming training data for public models
- Legal Liability: Ungoverned AI interactions creating discoverable records - chat histories, connector activity logs, and agentic task outputs - that may be subject to subpoenas or legal holds
- Expanded Attack Surface: Unauthorized access to an AI agent grants an attacker deep, aggregated access to association context and data that would otherwise take weeks to piece together manually
- Licensing Gaps: M365 licensing that does not include the controls required to effectively govern Copilot - a gap most organizations discover after deployment, not before

What the Assessment Covers

The 501CISO AI Security & Governance Assessment evaluates 77 controls across 8 domains, with 18 controls designated critical. It covers Microsoft Copilot, Claude, and OpenAI/ChatGPT - with Microsoft 365 and Entra ID treated as the foundational security layer for all three platforms.

Assessment Domain	What Gets Evaluated
Identity & Access Foundation	Entra ID configuration, MFA, Conditional Access, admin account hygiene
M365 Licensing & AI Entitlement	License tier vs. available AI security controls; Copilot add-on posture
Microsoft Copilot Configuration (if used)	Data access scoping, SharePoint permissions, sensitivity labels, Copilot Studio governance
Microsoft Purview & DLP	DLP policies covering AI interactions, retention, information barriers
Claude Admin & Connector Governance (if used)	Plan tier controls, MCP connector allowlisting, shadow AI exposure, SSO/SCIM status
OpenAI / ChatGPT Controls (if used)	Enterprise vs. personal account risk, GPT Store governance, API key sprawl
Shadow AI & Endpoint Controls	Personal account usage, CASB/SWG coverage, tenant restriction headers, device policy

What Clients Receive

Deliverable	Description
AI Security Score	Composite score (0-100) across all 8 domains with per-domain breakdown
Critical Findings Report	Prioritized findings table with plain-language risk descriptions and remediation steps
PowerPoint Findings Deck	Executive-ready presentation with domain scores, critical failures, and a 90-day roadmap
Controls Reference	Full 77-control workbook with pass/fail status and remediation notes for IT follow-through

Who It's For

This assessment is designed for:

- Trade associations, professional societies, and membership organizations
- Nonprofits with 25 to 300+ staff running Microsoft 365 with Copilot, Claude Team/Enterprise, or ChatGPT Business/Enterprise
- Organizations with limited internal IT security capacity - typically supported by an MSP or a small IT team without a dedicated security function
- Leadership teams that know AI governance is a gap but lack the internal resources or framework to address it

Contact us to schedule a discovery call and discuss whether the AI Security & Governance Assessment is a fit for your organization.