AI Security

Secure Your AI Transformation. End to End.

From risk assessment and shadow AI discovery to red teaming and agent governance — AUZA helps you adopt AI confidently, securely, and at speed.

5 Service Tracks
AI Security Coverage

360° Risk View
Models · Data · Agents · Shadow AI

Microsoft-Aligned
Agent 365. Purview. Defender. Copilot

AI IS RESHAPING CYBER RISK. ARE YOU PREPARED?

AI transforms how your business operates — and how attackers target it. Prompt injection, data oversharing, and shadow AI sprawl are the new frontier of enterprise risk. **AUZA** governs AI security at every layer, aligned to Microsoft's security framework, so your AI adoption stays protected and compliant.

OUR FIVE AI SECURITY SERVICE TRACKS

01 AI Risk Assessment
Know Your AI Risk Before It Knows You

End-to-end review of models, apps, agents, and data flows. Scored against NIST AI RMF & OWASP LLM Top 10 with a prioritised remediation roadmap.

KEY OUTCOMES
- AI risk register & heat map
- NIST AI RMF gap analysis
- Remediation roadmap

02 DataSecurityAssessment for AI
Powered by Microsoft Purview

Map sensitive data exposed to Copilot and agents. Identify oversharing across SharePoint, Teams & Exchange. Enforce DLP and labelling controls.

KEY OUTCOMES
- Sensitive data exposure report
- Oversharing risk identification
- Purview DLP enforcement

03 Agent 365 Enablement & Evaluation
Deploy Agents Secure by Design

Assess readiness, design least-privilege agent architectures, and operationalise Microsoft 365 Copilot agents across HR, Finance, Legal & IT.

KEY OUTCOMES
- Agent readiness assessment
- Secure architecture design
- Team rollout playbook

04 Shadow AI Discovery & Governance
See Everything. Govern Everything.

Discover unsanctioned AI apps, autonomous agents, and exposed MCP servers. Quantify risk and build a governance framework that balances innovation with control.

KEY OUTCOMES
- Shadow AI & MCP inventory
- Risk-scored app catalogue
- Governance policy & controls

05 AI Red Teaming
Attack Your AI Before Adversaries Do

Adversarial testing across your gen AI models, apps and agents — covering prompt injection, jailbreaking, data exfiltration, and agentic chain abuse.

KEY OUTCOMES
- Adversarial test report
- OWASP LLM Top 10 coverage
- Continuous eval pipeline

HOW WE ENGAGE - SIMPLE, STRUCTURED, BUILT AROUND YOUR BUSINESS

1 Discover & Scope
A no-cost scoping call to map your AI landscape, priorities, and risk appetite.

2 Assess & Report
Structured assessment in 2–4 weeks with executive briefing and technical findings.

3 Remediate & Govern
Hands-on implementation of controls, policies, and continuous monitoring.

FRAMEWORKS AND STANDARDS

NIST AI RMF · OWASP LLM TOP 10 · ISO 42001 · MAS TRM · Singapore PDPA · Microsoft RAISE

WHY FOR AI SECURITY? BECAUSE AI RISK REQUIRES MORE THAN TRADITIONAL SECURITY PLAYBOOK

Purpose-Built for AI Risk
Designed specifically to address the unique risks of AI adoption — not adapted from legacy security models.

Seamlessly Integrated
Works within your existing Microsoft environment with no disruption to operations or productivity.

Continuously Managed
Ongoing monitoring, governance reviews, and policy enforcement that evolve with your AI footprint.

GET STARTED - CONTACT US!

👉 Request a Demo | 👉 Get a Free Assessment | 👉 Contact Our Team

AUZA
Your Partner in Security, From Strategy to Execution

EMAIL
sales@auza.cc

WEBSITE
WWW.AUZA.CC