QUISITIVE

Copilot & Generative AI Security Readiness Assessment

Quisitive's **Copilot & Generative AI Security Readiness Assessment** provides organizations with an in-depth understanding of how best to adopt Copilot and Generative AI without putting their organization at risk. This assessment will help ensure your data is protected and not inadvertently exposed.

Copilot Potential Risks:

- **Data Exposure Risks:** Sensitive information might be exposed due to poor data governance.
- **Compliance Issues:** Data oversharing or exposure to unauthorized parties will fail complex data privacy and protection compliance requirements or regulations.
- **Unauthorized Access:** Preventing unauthorized data access or oversharing is critical.
- **Integration Challenges:** Integrating AI tools with existing security infrastructure without disruptions.

Benefits:

Implementing Copilot securely can dramatically boost your productivity and efficiency. This assessment helps you identify, prioritize and prepare to deploy Copilot with complete confidence and peace of mind.

Avoid Data Exfiltration
Validate that your sensitive data is protected and not inadvertently exposed.

Align with Regulatory Compliance
Evaluate that data protection regulations such as GDPR or HIPAA are not compromised.

Insight on Optimal Access Controls
Provides insight on access controls to ensure employees have the access necessary for their roles.

Regarded by Microsoft as **#1 Partner** for security assessments

Scope

- **Data Protection and Governance Workshops:** provide insight into building a safe resilient and trustworthy AI deployment.
- **Zero Trust Security Mapping Workshop:** Identifies environment weakness that may put AI initiatives at risk.
- **Sensitive Data Inventory:** Scan the environment to identify pockets of data that might put your AI ambitions at risk and provides clear recommendations on how to prevent data leaks.

Deliverables:

At the end of the assessment, stakeholders will receive:

- Review of analysis and findings
- Actionable and prioritized roadmap
- Written assessment report
- Detailed recommendations for next steps

Timeframe

Time: A typical Copilot & Generative AI Security Readiness Assessment is completed within 3–4 weeks. We'll review the results with you in person and discuss potential next steps.

Cost: $30K