JourneyTeam

# JourneyTeam AI Security Risk & Exposure Assessment

## *SECURE YOUR ENVIRONMENT BEFORE AI FINDS YOUR WEAKNESSES*

$8,000
5-Day Engagement



Everyone is moving quickly to adopt AI tools, and the upside is easy to see: fast answers, better productivity, and new ways to work. But AI also raises the stakes: it doesn't create security issues, but it does expose the ones already sitting in your environment.

Here's how: If your users have more access than they need, or if files are shared too broadly, or if old collaboration habits are still shaping your environment, AI will surface those gaps faster. Content that was technically available but rarely found can now appear instantly in a prompt response, a summary, or an AI-generated recommendation.

***That's why successful, safe AI adoption starts with knowing what your environment already allows AI to reach.***

## Before you scale AI, make sure your security posture can support it.

| AI EXPOSURE | DATA EXPOSURE | IDENTITY RISK | COPILOT READINESS |
|---|---|---|---|
| 73% are already using AI | Most companies can't locate all sensitive data | Legacy sharing is making data broadly accessible | Security leaders need AI governance answers |

## Secure AI Starts with Knowing Where You Are...

**Every organization is at a different stage in their AI journey.** Some are actively deploying others are still evaluating. But be aware, your employees are using it. Wherever you are, our AI Security Risk & Exposure Assessment of your Microsoft stack will identify your risks and potential exposures. Once you've pinpointed and secured those gaps, your teams can begin using AI in ways that are ***safer, smarter,*** and ***aligned with your business goals.***

# How Our Assessment Works

Our AI Security Risk & Exposure Assessment is a structured review of your Microsoft environment to identify areas where AI might be amplifying **existing** security, access, governance, or compliance issues so you can build a practical roadmap. We focus on:

- Clear business findings
- Prioritized recommendations
- Actionable next steps



## 1. DISCOVERY

We work with your team to identify where AI is already being used, what initiatives are planned, and where leadership needs greater visibility.

## 2. ENVIRONMENT REVIEW

We review identity, data sharing practices, administrative controls, and governance policies to understand where AI may be amplifying risk.

## 3. RISK ANALYSIS

We analyze findings and prioritize recommendations based on business impact, risk reduction, and implementation effort so you can focus on the quick wins.

## 4. ROADMAP AND READOUT

Finally, we deliver a practical roadmap and action plan for improving security posture while supporting your AI initiatives.

## Business Value

Move from discussion to direction with practical findings you can actually use.

- Leadership gets clear insight to plan, prioritize, and move on their AI initiatives.
- Teams have a strong foundation and path forward.

## Gain clarity. Reduce risk. Move forward with confidence.

JourneyTeam helps you navigate AI adoption securely and confidently across Microsoft 365, Dynamics 365, Azure, Fabric, Power Platform, and Copilot. We bring together the data, collaboration, and security sides of your environment so you can support AI adoption with strong alignment, control, and zero blind spots.

JourneyTeam

CONTACT US