

MOBIUS COPILOT FOR MICROSOFT 365 - SECURITY & READINESS ASSESSMENT



MOBIUS
CONSULTING

Actualising change

WHAT COULD COPILOT BE ASKED TO DO IN YOUR ORGANISATION?

Even with the best intentions, generative AI can surface sensitive or inappropriate information if not properly governed.

Your employees may prompt Copilot with:

- Show me last month's salary review across the team.
- List everyone flagged for underperformance in the last year.
- What was the budget overrun on the Cape Town project?
- Summarise the disciplinary cases logged in HR this quarter.
- Are there any planned restructures or retrenchments in our business unit?
- What external partners are we currently in contract negotiations with?

Now imagine:

If access permissions are misconfigured or sensitive content is overshared in SharePoint or Teams, these prompts may yield real results, exposing confidential HR data, financial insights, or business strategies.

WHY MOBIUS

We bring deep expertise in security assessments and governance frameworks across Microsoft 365 environments. Our approach is technology-aware, but not technology-bound. We help you understand your unique risk landscape, ensure that AI deployments are privacy-aware and policy-aligned, and deliver clear actions to build security into your digital journey.

BENEFITS



INFORMED AI DECISIONS

Gain insights into your primary data and access risks prior to Copilot deployment.



ALIGN TO EMERGING AI STANDARDS

Stay ahead of the curve by aligning with ISO 42001 and the EU AI Act.



INCREASE SECURITY & TRUST

Ensure that generative AI tools uphold compliance and data governance standards.



BUILD AI RESILIENCE

Establish a strong foundation for safe and scalable AI integration into business workflows.



REDUCE EXPOSURE

Identify and mitigate risks of overshared data and improve permissions proactively.



MOBIUS COPILOT FOR MICROSOFT 365 - SECURITY & READINESS ASSESSMENT



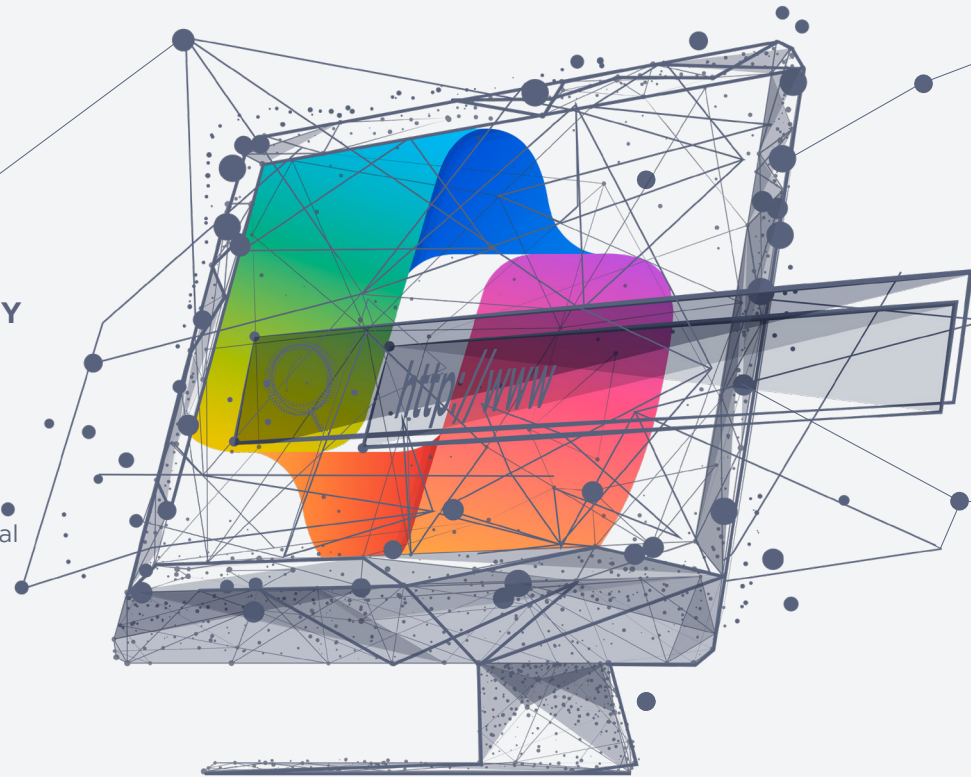
MOBIUS CONSULTING APPROACH

Our structured approach aligns closely with our standard security methodology and includes three key phases:



1. PLANNING AND DISCOVERY

- Understand your current Copilot usage and M365 licensing (E3/E5).
- Review AI adoption drivers and internal information governance requirements.
- Establish the broader organisational context for secure Copilot integration.



2. CURRENT STATE ASSESSMENT

- Assess security controls, access governance, and monitoring capability.
- Identify overshared and sensitive content in SharePoint, Teams, and OneDrive.
- Evaluate your environment against Microsoft Secure Score and Defender Score.
- Determine AI-related risks based on internal data usage and sensitivity.



3. DEVELOP HIGH-LEVEL ROADMAP

- Provide actionable recommendations to improve readiness and close control gaps.
- Highlight compliance alignment areas with ISO/IEC 42001, EU AI Act, POPIA, & GDPR.
- Deliver a prioritised, business-aligned roadmap for secure Copilot enablement.

THE END RESULT

You will gain a clear view of your readiness for Copilot, an understanding of AI-related security risks, and a custom roadmap to enable generative AI safely in your Microsoft 365 environment. Whether you are just starting your AI journey or have already begun deployment, this assessment ensures your controls evolve to meet new challenges.

SECURING DIGITAL **TRUST**



SECURE YOUR DIGITAL JOURNEY

Have confidence in your
secure digital risk landscape.



DEVELOP YOUR DIGITAL RESILIENCE

We work with you to develop
sustainable data risk resilience
into your business systems.



KNOW YOUR RISK LANDSCAPE

Let us confidently accelerate
your digital journey by helping
you know your risk landscape.