# Copilot for Microsoft 365 Security Accelerator

## Plan your data, privacy and security requirements for Copilot for Microsoft 365

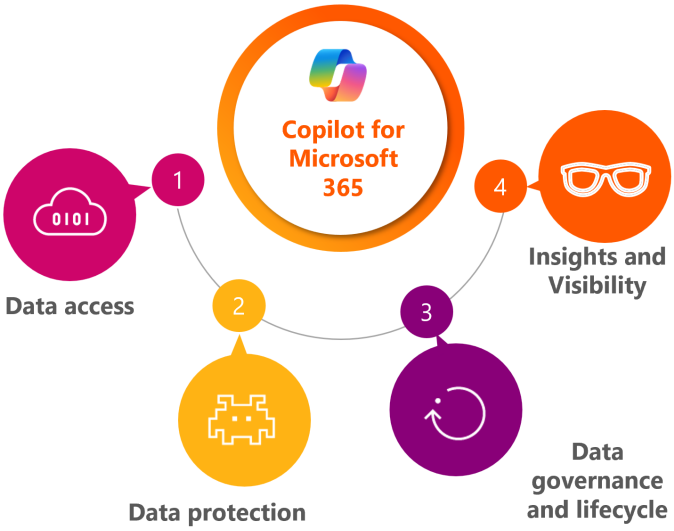
### It is recommended to have solid content management practices in place prior to Copilot for Microsoft 365 adoption.

**Evaluate oversharing:** Copilot for Microsoft 365 only surfaces organizational data to which individual users have at least view permissions. It's important that organizations are using the permission models available in Microsoft 365 services, such as SharePoint, to help ensure the right users or groups have the right access to the right content within the organization.

**Implement information protection:** A properly implemented document and data classification program leveraging Microsoft Purview can ensure that data is protected. When you have data that's encrypted by Microsoft Purview Information Protection, it won't be returned by Copilot for Microsoft 365 unless the user is granted at least the view usage right.

## How do we solve it

**Our Copilot for Microsoft 365 security accelerator covers multiple security & data governance topics; data access and permissions, data protection, data governance & life cycle, as well as insights and visibility. The assessment identifies instances and associated risks of "data oversharing" and provides ways to address.**




**Data Access**
Review various sources of data for data access including Sharepoint, Teams, public and private sites.

**Data Protection**
Review how sensitive data is reviewed and monitored. Data loss prevention policies review and recommendations

**Data Governance & lifecycle**
Access lifecycle management overview (e.g., groups, users, sites). Overview of obsolete data

**Insights & visibility**
Discover Sensitive Interactions in Copilot and other Gen AI Apps (preview). Observe and identify risky behaviour over time (preview). Identify Insider Risks

avanade

# Copilot for Microsoft 365 Security Accelerator

## Secure your journey to Copilot for Microsoft 365

### Establish a security mindset

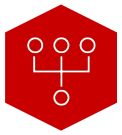
Over a 3-to-6-week period, we'll help you evaluate your existing security controls that support roll out of Copilot for Microsoft 365. We will deliver a set of recommendations and plans to remediate gaps and uplift deficiencies to support a secure Copilot for Microsoft 365 implementation.

**OVERVIEW**

Provide customers with an overview of Copilot and the impact of data oversharing.

**DISCOVERY**

Perform data discovery across Microsoft Online Services, identifying sensitive data across Teams, SharePoint and One Drive.



**DEFINE**

Identify instances of "data oversharing" and provide an overview of Teams and SharePoint lifecycle governance.

**REPORT & STRATEGIZE**

Receive a complete report and define next steps.

## Final deliverables

Report on discovered risks and detail on resolutions. Recommended initiatives or actions for technology and organizational improvements needed to unlock the value of Copilot for Microsoft 365

Next Steps Roadmap highlighting approach for fixing gaps and deficiencies, identifying quick wins and plans for longer term intiaitves.

**Get in touch with us:**

Sarah Rench
Global Gen AI Security Lead
Sarah.Rench@avanade.com

avanade