KPMG

Microsoft 365 Copilot Readiness Assessment

Microsoft 365 Copilot Adoption Framework

Microsoft 365 Copilot adoption framework comprises a standard set of building blocks each yielding distinct outcomes for ROI analysis and roadmap strategy definition.

KPMG Powered M365 Copilot

01

Business Case

Defining the business case for Copilot ROI and definition of an implementation roadmap

- Efficiency gain assessment based on use cases – threshold tracker
- Roadmap for maximized ROI based on user groups
- ‘ A Day in the Life of’ and Persona assessment.

02

Adoption Preparation

Assess client environment and data for successful adoption

- Content management / permissions best practice implementation
- Ensure the relevant licensing level, Identity and data protection requirements are met

03

Technical Rollout

Activating Copilot in the tenant being available for users according to roadmap

- Assign relevant Microsoft 365 licenses
- Assign Copilot licenses for relevant user groups

04

Data Integration

Identification of data sets to be integrated while being outside of the Microsoft ecosystem

- Assess data repositories for Copilot data integration
- Create data integration roadmap (connectors, plugins)

05

Change Management

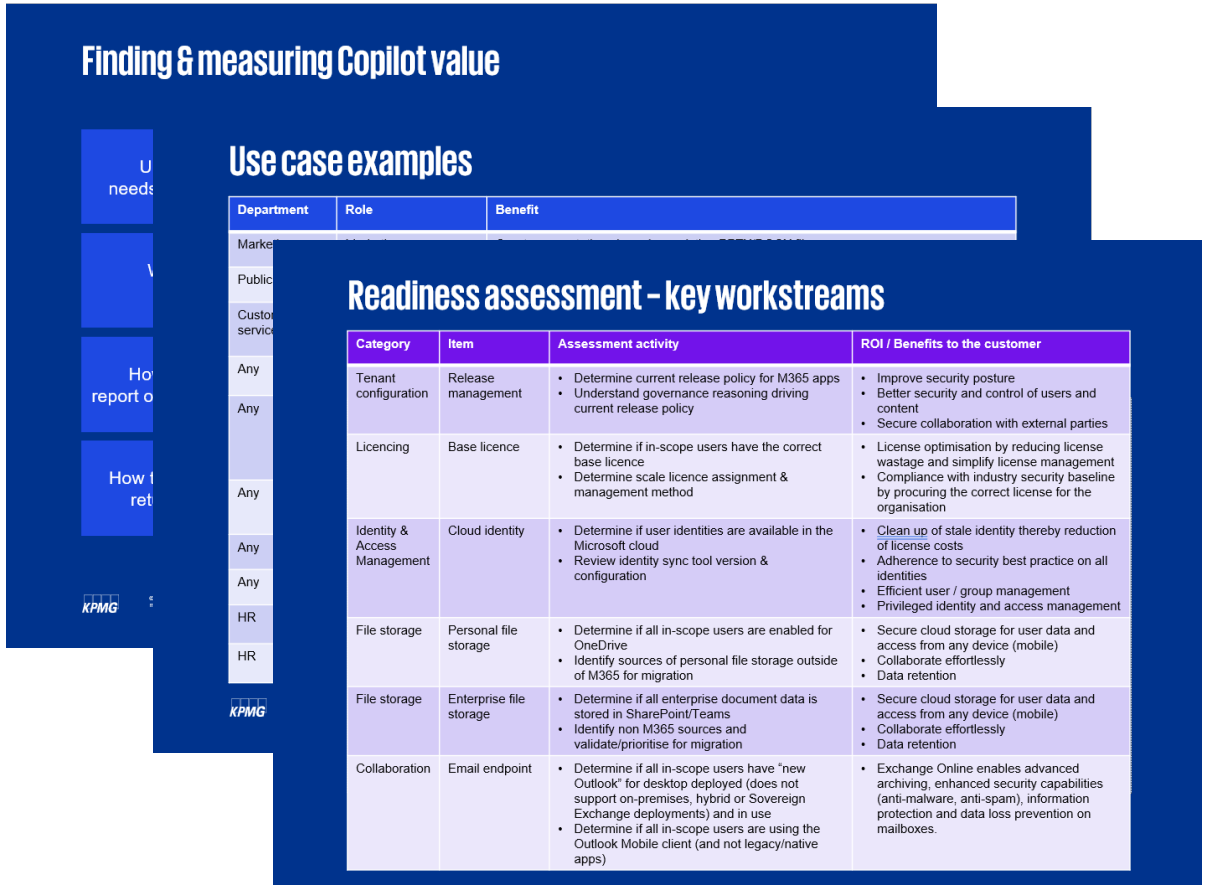
Training employees and create relevant risk awareness for GenAI usage

- Create user onboarding according to roadmap and use cases
- Run risk awareness training
- Establish CoE for internal knowledge sharing

KPMG Powered Copilot Advantages

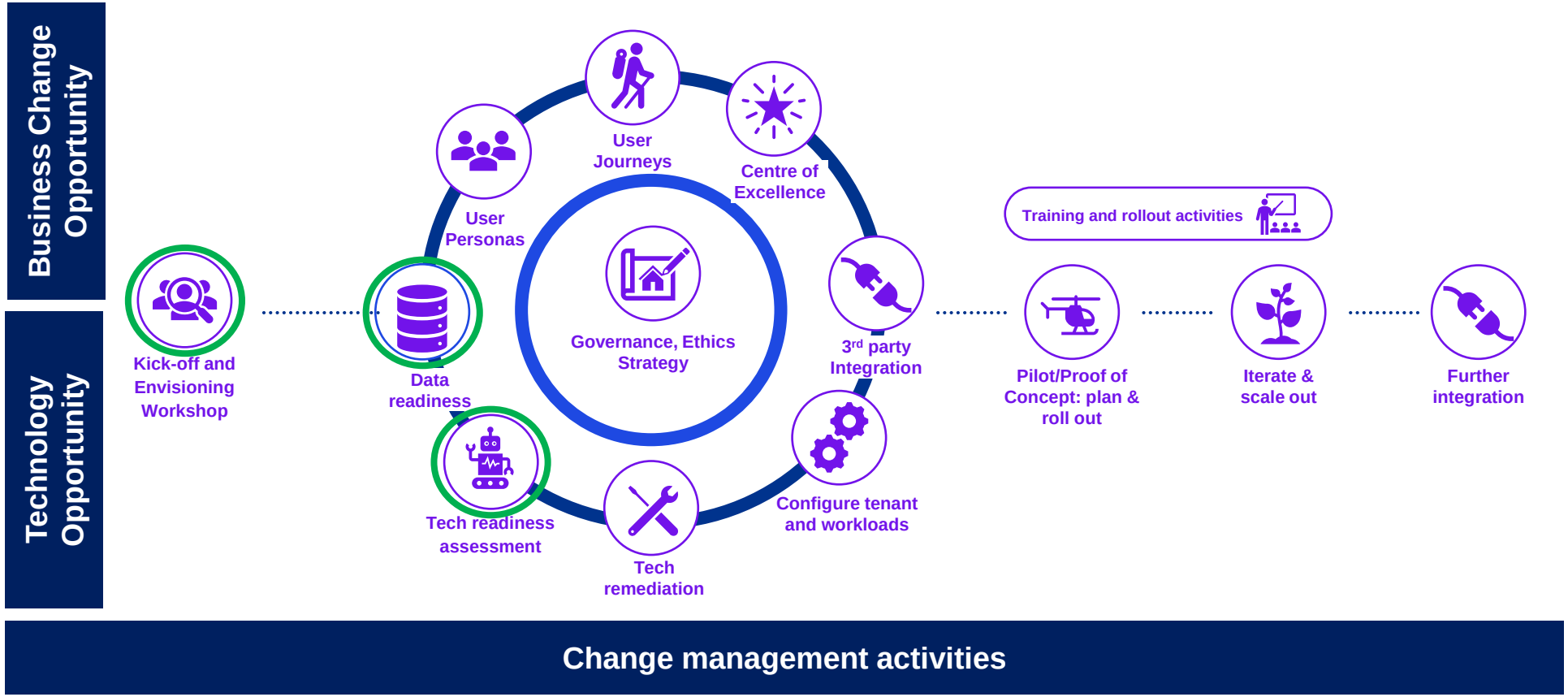
Enhance your Microsoft 365 Copilot journey with KPMG's Powered framework.

1. Leverage on KPMG's industry experience.
2. Comprehensive readiness assessments to enhance your confidence.
3. Future proof your identity and data security portfolio.
4. Achieve secured and efficient productivity.
5. Further your journey towards Data Protection Trust Mark (DPTM).



KPMG Powered Copilot Approach

A cohesive approach supporting implementation of Microsoft 365 Copilot along the overall framework, focusing on all aspects of an implementation project, supporting various business functions and can be replicated to member entities. This engagement will focus on the 3 items highlighted below.



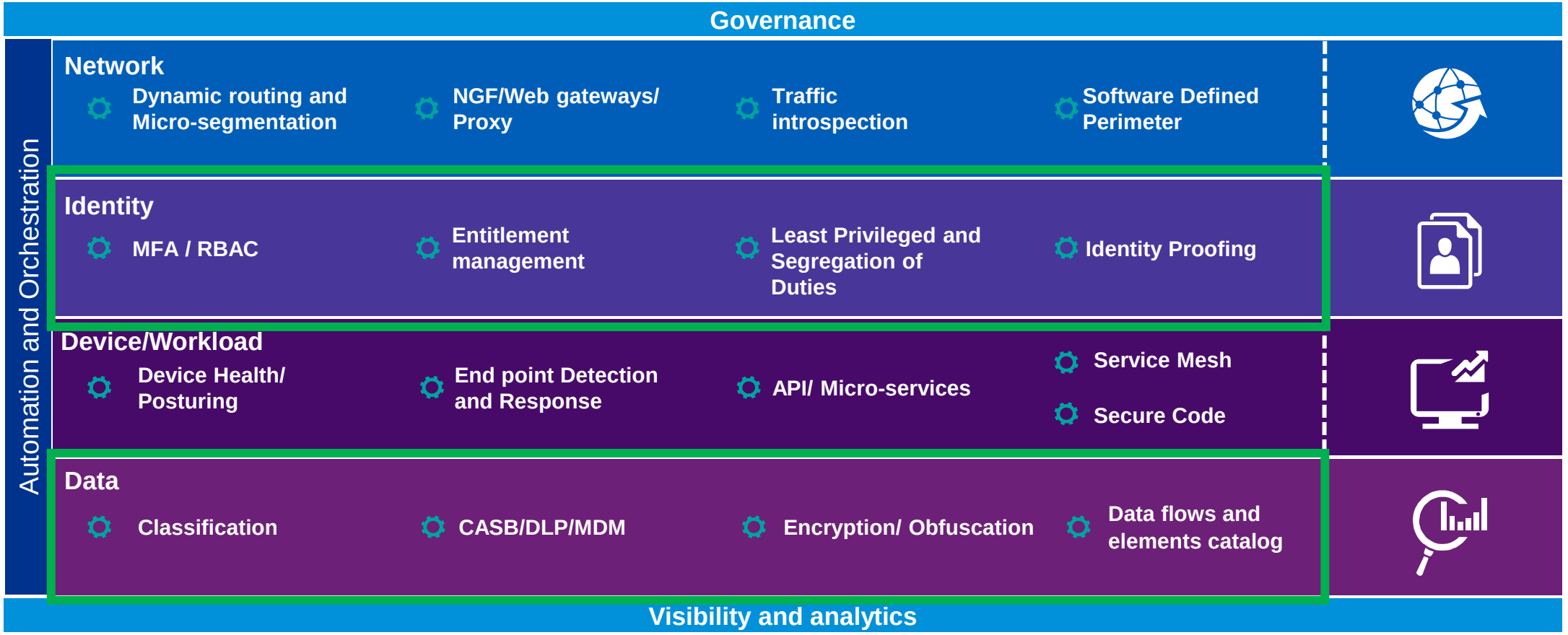
Envisioning Workshop Scope

A 2 hours session will be conducted post Kick-off with the core working team members on the items listed below to familiarize participants with the Microsoft 365 Copilot journey.

SN	Agenda	Description
1	Day in the Life	• Understanding how core components of Microsoft 365 Copilot can be leveraged by users in their daily work lives • Walkthrough of common scenarios
2	Persona Assessment and Business Use Cases	• Understanding of Personas in Microsoft 365 Copilot • Walkthrough of various specific business use cases for Microsoft 365 Copilot
3	Data Confidentiality	• Understanding how Microsoft 365 Copilot handles organisations' data • Ensuring that the organisation is aligned with Microsoft's Responsible AI guidelines
4	Microsoft 365 Copilot Pre-requisite	• Sharing of the pre-requisite checklist for roll-out of Microsoft 365 Copilot

KPMG's Zero Trust Framework

KPMG has identified key pillars within the Zero Trust framework with identified processes, controls and metrics to be considered for Cybersecurity initiatives. The scope for the Copilot assessment will cover Identity and Data highlighted below.



Data Protection Process and Controls Assessment

Scope Details

- User Group – 1 Department (Focus Group)
- Application Coverage of M365 Suite:
  - Word, Excel, PowerPoint, Outlook, Teams, Power BI, OneDrive, OneNote, SharePoint.
- Document type coverage
  - Word, Excel, PowerPoint, Outlook, PDF
- Review of organisation's processes and security controls in place for Data Protection.
  - Data Classification
  - Records Management
  - Information Protection
  - Data Loss Prevention

Key Deliverables

- Data Protection Gap Analysis findings
- Data Protection recommendations based on Gap Analysis findings

Assumptions

- Document type will be limited as mentioned in Scope Details.
- Review and validation of storage sites and databases where applicable will be limited to 1 of each.

Review Topic	Sessions	Review Checklist	Participants
Coverage of Organization's Processes and Security Controls	2	❖ Data Classification ❖ Records Management ❖ Information Protection ❖ Data Loss Prevention	IT Admin Team
Validation of Organization's Processes and Security Controls	2 - 3	❖ Data Classification ▪ Classification labels, criteria and approach ▪ Classification label policy configuration ❖ Records Management ▪ Record labels, criteria and approach ▪ Record retention and deletion configurations ❖ Information Protection ▪ User Rights Management ▪ Security controls for: ✓ Data at rest ✓ Data in transit ✓ Data in use ❖ Data Loss Prevention ▪ DLP channel coverage ▪ DLP policy coverage	IT Admin Team

IAM Process and Controls Assessment

Scope Details

- User Group – One Representative Department
- Application Coverage of M365 Suite:
  - Word, Excel, PowerPoint, Outlook, Teams, Power BI, OneDrive, OneNote, SharePoint.
- Review of coverage of organization's processes and security controls in place for IAM with reference to KPMG's process taxonomy (refer appendix).
  - Access Provisioning & Deprovisioning
  - User Access Reviews
- Testing of processes for sample user group.

Key Deliverables

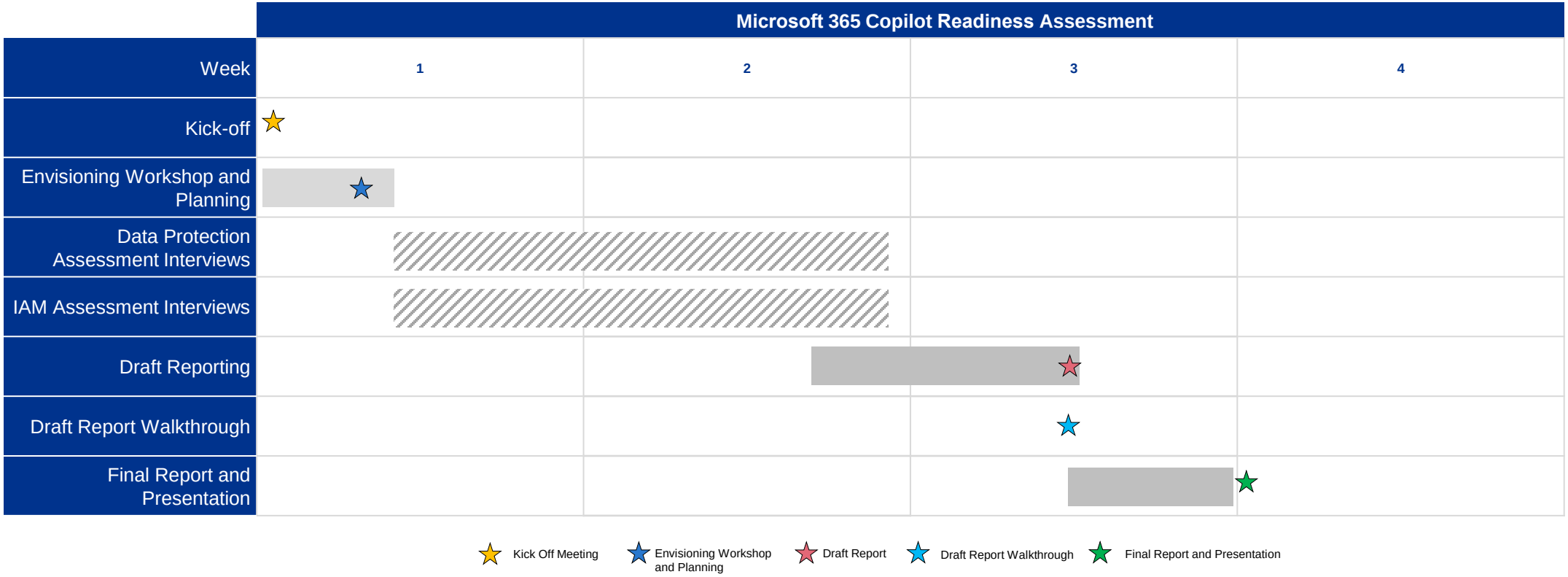
- IAM Gap Analysis report.
- IAM recommendations based on Gap Analysis report.

Assumptions

- Review of target operating model is considered to be out of scope
- The assessment is only considered to be for the sample user groups and the above mentioned application coverage
- It is assumed that Entra ID / Azure AD is integrated with On-Prem Active Directory
- Review of existing access management product is considered to be out of scope
- Review of access control matrix is considered to be out of scope

Review Topics	Sessions	Review Checklist	Participants
Coverage of Organization's Processes and Security Controls	2 - 3	❖ Access provisioning for new and existing users ❖ User access reviews ❖ Access deprovisioning	IT Admin Team
Validation of Organization's Processes and Security Controls	1 - 2	❖ Run a access review for the user group and the application scope through Microsoft Entra ID	IT Admin Team

Engagement Timeline



Appendix 1 – Identity Access Management Processes

SN	Process	Source for the review
1	HR Driven provisioning	Questionnaire
2	New user on-boarding	Questionnaire
3	User access matrix	Questionnaire
4	Existing user requesting additional access	Questionnaire
5	Existing user details update process	Questionnaire
6	User termination	Questionnaire
7	User access reviews flow	Questionnaire
8	User access reviews Schedule	Questionnaire
9	User access reviews reassignment flow	Questionnaire
10	Existing user access review with respect to access matrix	Reports from Entra ID
11	Existing user login activities	Reports from Access Management System

Appendix 2 – Data Protection Policies and Processes

SN	Category	Source for the review
1	Data Classification	Questionnaire
2	Data Access Control	Questionnaire
3	Encryption	Questionnaire
4	Data Masking/Anonymization	Questionnaire
5	Data Loss Prevention	Questionnaire
6	Data Retention and Disposal	Questionnaire