

Ogi Pro Consulting Services



Identity Management

2-Week Assessment



Keep your data secure and compliant, reduce demands on in-house IT and deliver a simplified experience for users with this identity management assessment for Microsoft 365.

Overview

More teams are working remotely and, in the cloud, so it's vital for companies to maintain secure user identities, ensuring only authorised individuals can access private data.

With Microsoft 365, this can be handled using Entra ID: an identity management and access solution that helps keep data secure and compliant. Setting up Entra ID correctly can take some fine tuning. We'll help ensure you have the right licenses and enable best practice security policies like Multi-Factor Authentication, Single Sign-On and password management are in place.

Through this engagement our friendly experts will integrate and configure Entra ID to provide professional and secure identity management for your organisation.



Key benefits



A simplified and frictionless experience for users that embeds baseline security principles into identity management with Entra ID



Authentication and single sign-on for Microsoft 365 and third-party platforms (like social media)



Reduced support requirements and reliable security for in-house service desks



Optimise use of Microsoft 365, maximising the value you get from your investment

This engagement includes:

Entra ID integration

Establishing policies for Multi-Factor Authentication (MFA), Single Sign-On (SSO) and Self-Service Password Reset (SSPR), including modern authentication policies.

Setting and enforcing password policies alongside passwordless sign-in and other enabling technologies (such as Windows Hello or biometric sign-in)

Complementary add-ons for this engagement include:

Securing Devices and Applications

Securing Content in SharePoint and OneDrive.

Scope

This engagement is focused on Identity Management in Microsoft 365. The intention is to keep the scale and complexity of the Engagement to a minimum to quickly provide the defined benefits to the customer and end-users. For larger, more complex organisations the engagement can be run multiple times with a new set of user stories/success criteria.

Examples of circumstances where this may be appropriate are:

- Complex organisations with many user-types
- Implementing advanced Identity Management Features in phases (e.g. MFA for all, followed by complex conditional access policies).
- Implementing core features first, and re-running as more advanced licensing becomes available, through e.g. move from Microsoft 365 E3 to E5.

Assumptions

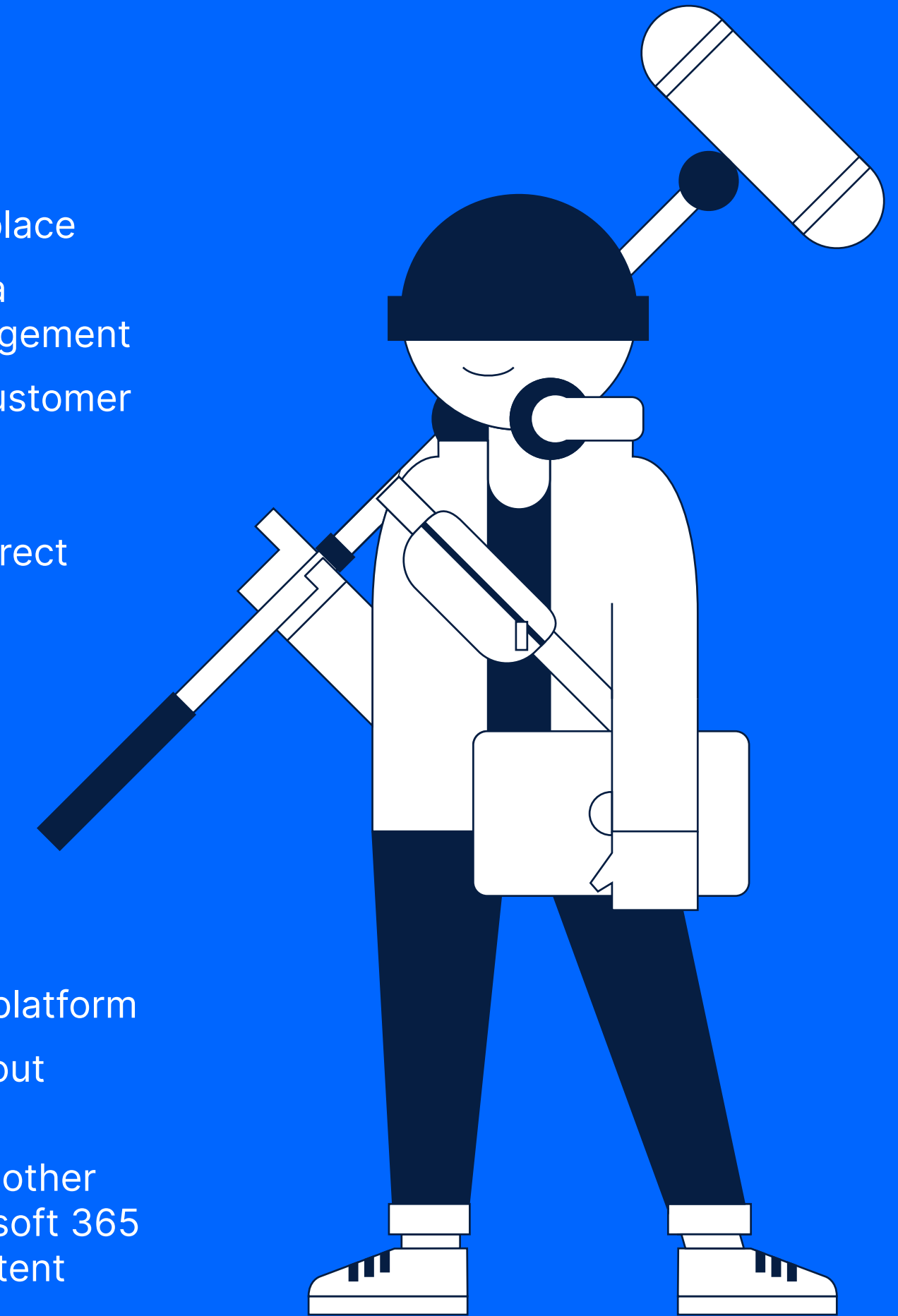
This Engagement is designed based on the following assumptions:

- The customer already has a Microsoft 365 Tenant in place
- Ogi will be provided with delegated admin access as a Microsoft Partner for at least the duration of the engagement
- For Hybrid Identity environments Ogi will work with Customer IT Teams to ensure prerequisites are in place
- Any additional licensing required to support the Engagement can be provided by Ogi as a Microsoft Direct Cloud Solutions Partner
- Workshops and non-disruptive implementation work will be carried out during standard business hours

Exclusions

- Upgrade of on-premise solution software/hardware if required as a prerequisite
- Migration of non-Microsoft users onto Microsoft 365 platform
- Migration of any other workflows to support the role-out of the Identity Management solution

Ogi are able to assist with many excluded items through other pre-defined engagements such as those covering Microsoft 365 Migration, Device and Application Management and Content Management.



Structure

All Ogi Cloud Engagements have a consistent structure designed to deliver customer-value against a set of agreed success criteria. These are measurable and unique to each customer, driven by their priorities, organisational culture, and mission. Our approach is based on Microsoft's Service Adoption Framework and consists of three main stages; Envision, Implement, and Enable.





Envision

Envisioning consists of determining with the customer the required scope of the engagement and establishing the necessary involvement from interested parties and stakeholders. Typically conducted through a workshop session but can also be an initial call/remote session.

It will cover:

- Exploring customer requirements/ drivers
- Explaining to customer processes and likely impacts – risks and benefits
- Review of existing environment
- Review of best practice recommendations and policy decisions
- Agreement as to proposed timeframe and strategy for user engagement

Key Outputs:

Implementation plan covering:

- Agreed Policies/Best Practice Changes to be made
- Impacted workflows and users
- Roll-out timetable
- End-User training requirements
- Identity Management Policy (Optional)

Requirement:

Typically half-day Senior Cloud engineer

Implement

This stage takes place over one-two weeks and includes the following key activities/deliverables:

Implement Office 365 baseline best-practice security measures

Review and update Active Directory/AAD integrations

Configure MFA and SSPR in Office 365

Deploy and configure Azure Active Directory Password Protection

Optional extension to include broader Identity Management Policy work to include non-365 systems can be discussed. This may involve a further consultancy work specifically tailored to customer needs.

Requirement

Half-day to 1-day Cloud Engineer

Additional time for dealing with third parties who don't have established DMARC policy/process.

Enable

User awareness training/materials

Enable Champions/Early Adopters

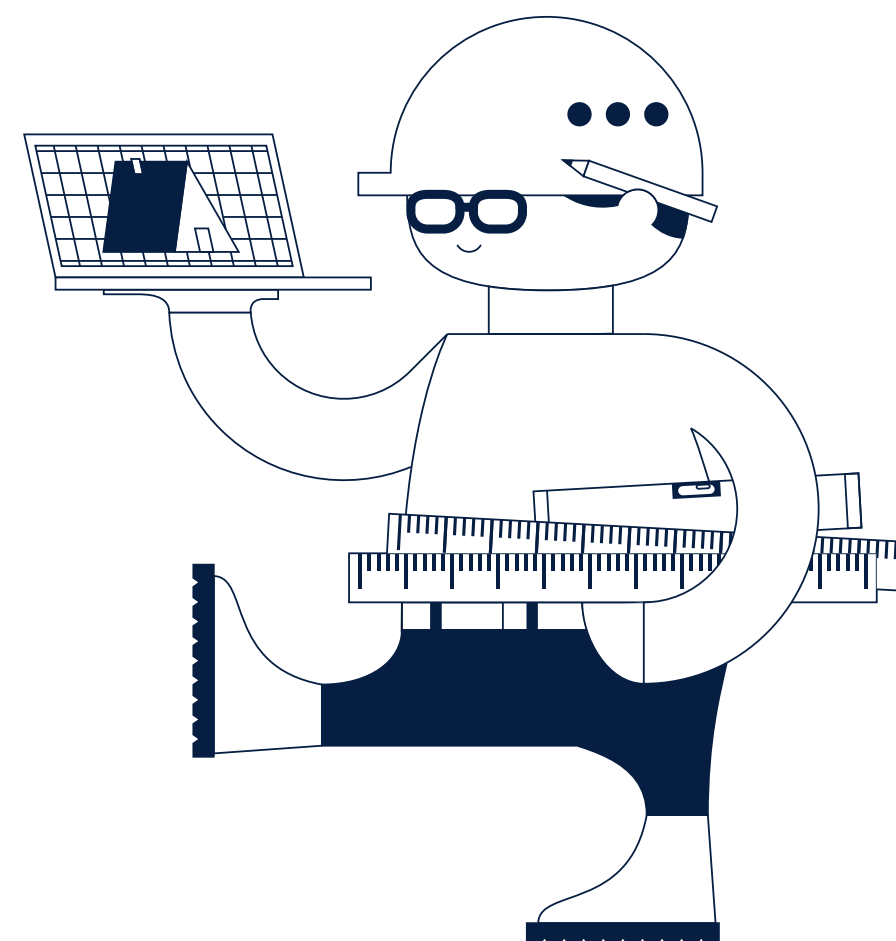
End-User Training (Optional)

Broad deployment to all users/follow up

Requirement

Half-day Cloud Engineer – Additional two hours for optional training (Half-day if remote)

Agenda timeframe: (accelerated - actual depends on customer involvement)



Timeframe Agenda

Week 1

Day 1 Envision session and produce outputs

Day 2 Produce and agree Implementation Plan

Day 3 Implement initial best-practice/policies
Implement Active Directory Connector/Password write back etc.

Days 4/5 Enable Early Adopters and test

Week 2

End User engagement and wider deployment



Let's hold a no obligation discovery call to see how we can help.

029 2002 0535

pro@ogi.wales



Crown
Commercial
Service
Supplier



Certificate No. 364832021



Certificate No. 345842020



Certificate No. 166022021

