

# 1. Microsoft Incentives - Proof of Engagement

## 1.1 FastTrack Overview

Microsoft provides the FastTrack service to help customers successfully deploy and drive user adoption of Microsoft 365 solutions. When customers purchase eligible Microsoft 365, Office 365, Windows 10, or EMS licenses, the FastTrack benefit is included at no additional cost for the life of their subscriptions. FastTrack helps your customers migrate data (500 or more seats), enable more effective teamwork, protect their organizations from cybersecurity threats, and keep devices and apps up to date.

FastTrack guidance covers three areas:

- Planning (setup, remediation, and configuration)
- Onboarding, with access to best practices
- Ensuring readiness with an adoption plan and training

All fields are required unless stated otherwise	
<b>Partner Name:</b>	Global Computing and Telecoms
<b>Customer Name:</b>	
<b>Customer Signature:</b>	
<b>Customer Signatory: Name (Printed):</b>	
<b>Customer Signatory: Role:</b>	
<b>Dates of Signature:</b>	
<b>*Optional: Tenant ID:</b>	
<b>*Optional: Domain:</b>	
<b>Tenant Name</b>	

<input checked="" type="checkbox"/> Exchange Online	<input checked="" type="checkbox"/> Intune
<input checked="" type="checkbox"/> Outlook Mobile	<input checked="" type="checkbox"/> Azure Active Directory Premium (AADP)
<input checked="" type="checkbox"/> SharePoint Online	<input checked="" type="checkbox"/> Azure Information Protection (AIP)
<input checked="" type="checkbox"/> Teams Calling	<input checked="" type="checkbox"/> Azure Advanced Threat Protection (AATP)
<input checked="" type="checkbox"/> Teams Meetings	<input checked="" type="checkbox"/> Microsoft Cloud App Security (MCAS)
<input checked="" type="checkbox"/> Teams Apps and platforms	<input checked="" type="checkbox"/> Microsoft Information Protection
<input checked="" type="checkbox"/> Teams Phone System	<input checked="" type="checkbox"/> Microsoft Information Protection
<input checked="" type="checkbox"/> ProPlus (Business applications)	<input checked="" type="checkbox"/> Microsoft Defender for Office 365
<input checked="" type="checkbox"/> Microsoft Edge	<input checked="" type="checkbox"/> Microsoft Defender for Identity
<input checked="" type="checkbox"/> Microsoft Defender for Endpoint	

<input type="checkbox"/> D365 Customer Engagement	<input type="checkbox"/> D365 For Retail
<input type="checkbox"/> D365 For Case Management	<input type="checkbox"/> D365 For Sales
<input type="checkbox"/> D365 For Customer Service	<input type="checkbox"/> D365 For Self-Serve
<input type="checkbox"/> D365 For Field Service	<input type="checkbox"/> D365 For Talent
<input type="checkbox"/> D365 For Marketing	<input type="checkbox"/> D365 For Team Members
<input type="checkbox"/> D365 For Operations/Unified Ops	<input type="checkbox"/> D365 Plan
<input type="checkbox"/> D365 For Project Service	<input type="checkbox"/> AX7
<input type="checkbox"/> D365 For Relationship Sales	<input type="checkbox"/> CRM Online
Other:	Other:

## 2. Project Implementation / Deployment Activities / Change Management

Please provide below as much detail as you can on at least one of the below areas:

### 2.1 Scope of work

Project Phase		
Envisioning	<b>Microsoft Azure Active Directory</b>	<ul style="list-style-type: none"> <li>• Environmental Assessment</li> <li>• Solution Alignment</li> </ul>
	<b>Microsoft Enterprise Mobility Suite (EMS)</b>	<ul style="list-style-type: none"> <li>• Environmental Assessment</li> <li>• Solution Alignment</li> </ul>
	<b>Windows 10 Enterprise</b>	<ul style="list-style-type: none"> <li>• Environmental Assessment</li> <li>• Solution Alignment</li> <li>• Solution Envisioning Workshop</li> </ul>
	<b>Microsoft Office 365 Pro Plus / Business applications</b>	<ul style="list-style-type: none"> <li>• Environmental Assessment</li> <li>• Solution Alignment</li> <li>• Solution Envisioning Workshop</li> </ul>
	<b>Microsoft Teams Meetings</b>	<ul style="list-style-type: none"> <li>• Environmental Assessment</li> <li>• Solution Alignment</li> <li>• Solution Envisioning Workshop</li> <li>• Participating in meetings using Teams- Meeting</li> </ul>
	<b>Microsoft Teams Calling</b>	<ul style="list-style-type: none"> <li>• Environmental Assessment</li> <li>• Solution Alignment</li> <li>• Solution Envisioning Workshop</li> <li>• Participating in meetings using Teams- Phone System</li> </ul>
	<b>Microsoft Teams App and Platforms</b>	<ul style="list-style-type: none"> <li>• Environmental Assessment</li> <li>• Solution Alignment</li> <li>• Solution Envisioning Workshop</li> <li>• Apps built on the Microsoft Teams platform</li> </ul>
	<b>Microsoft Exchange Online</b>	<ul style="list-style-type: none"> <li>• Environmental Assessment</li> <li>• Solution Alignment</li> <li>• Solution Envisioning Workshop</li> </ul>
	<b>Microsoft SharePoint Online</b>	<ul style="list-style-type: none"> <li>• Environmental Assessment</li> <li>• Solution Alignment</li> <li>• Solution Envisioning Workshop</li> </ul>
	<b>Microsoft Defender for Identity</b>	<ul style="list-style-type: none"> <li>• Environmental Assessment</li> <li>• Solution Alignment</li> <li>• Solution Envisioning Workshop</li> </ul>

	<b>Microsoft Defender for Office 365</b>	<ul style="list-style-type: none"> <li>• Environmental Assessment</li> <li>• Solution Alignment</li> <li>• Solution Envisioning Workshop</li> </ul>
	<b>Microsoft Defender for Endpoint</b>	<ul style="list-style-type: none"> <li>• Environmental Assessment</li> <li>• Solution Alignment</li> <li>• Solution Envisioning Workshop</li> </ul>
Plan	<b>Microsoft Azure Active Directory</b>	<ul style="list-style-type: none"> <li>• High Level Solution Design</li> </ul>
	<b>Microsoft Enterprise Mobility Suite (EMS)</b>	<ul style="list-style-type: none"> <li>• High level Solution Design</li> </ul>
	<b>Windows 10 Enterprise</b>	<ul style="list-style-type: none"> <li>• High level LAB Design</li> </ul>
	<b>Microsoft Office 365 Pro Plus &amp; Teams</b>	<ul style="list-style-type: none"> <li>• Configuration Guide</li> </ul>
	<b>Microsoft Exchange Online</b>	<ul style="list-style-type: none"> <li>• Configuration Guide</li> </ul>
	<b>Microsoft SharePoint Online</b>	<ul style="list-style-type: none"> <li>• Configuration Guide</li> </ul>
Build & Stabilize	<b>Microsoft Azure Active Directory</b>	<ul style="list-style-type: none"> <li>• Enable Azure Active Directory</li> <li>• Configure Azure AD Sync On-Premises</li> <li>• Configure UPN Suffix if required</li> </ul>
	<b>Microsoft Enterprise Mobility Suite (EMS)</b>	<ul style="list-style-type: none"> <li>• Assist the customer in the configuration of EMS capabilities including Microsoft Intune, Self-Service Password Reset (SSPR), MFA, single sign-on (SSO) and RMS.</li> <li>• Assist the customer in the enrollment of up to 10 identified mobile devices.</li> <li>• Assist the customer with Intune feature activation including: <ul style="list-style-type: none"> <li>– Application management policies (up to five applications)</li> <li>– Policy enforcement (up to 10 configuration profiles)</li> <li>– Device enrollment for Windows Phone, Android, and iOS devices.</li> <li>– Device configuration for Windows Phone, Android, and iOS devices.</li> </ul> </li> <li>• Assist the customer with configuration of up to five gallery applications including two integrated applications.</li> <li>• Assist the customer to activate Azure MFA on the Azure application portal for administrative users.</li> <li>• Assist the customer to activate SSPR.</li> <li>• Assist the customer to create two Azure RMS policy templates.</li> </ul>

		<ul style="list-style-type: none"> <li>•</li> </ul>
	<b>Windows 10 Enterprise</b>	<ul style="list-style-type: none"> <li>• Determine the suitability of the current operating system image to determine if an in-place upgrade may be used to deploy Windows 10.</li> <li>• Consider the use of the Windows 10 In-Place Upgrade for systems where no changes to the system firmware, disk layout, or where system configuration drift is within acceptable limits.</li> <li>• Systems that require system firmware or hardware changes will require the re-installation of Windows after the changes have been made.</li> <li>• Develop or upgrade infrastructure to support the deployment of a custom operating system image to support employees and systems in the following scenarios <ul style="list-style-type: none"> <li>○ New Devices</li> <li>○ Refresh of existing systems on the corporate network</li> <li>○ Refresh of existing systems used by remote workers</li> </ul> </li> <li>• Upgrade the Configuration Manager environment to support Windows 10 in-place, OSD and management.</li> <li>• Evaluate and update Microsoft Deployment Toolkit to the appropriate version with Windows 10 support.</li> <li>• (Non-Configuration Manager) Liaise with software vendor to update the incumbent deployment tooling to support the deployment of Windows 10.</li> </ul>
	<b>Microsoft Office 365 Pro Plus/ Business applications</b>	<ul style="list-style-type: none"> <li>• Configuration of XML.</li> <li>• Group Policy Object (GPO) configuration that utilizes Microsoft System Center Configuration Manager (SCCM) for deployment.</li> <li>• A review of updating options.</li> <li>• Office 365 ProPlus delivery methodology development.</li> <li>• Office 365 ProPlus update strategy development.</li> <li>• Legacy Microsoft Office replacement strategy development.</li> </ul>
	<b>Microsoft Teams (apps)</b>	<ul style="list-style-type: none"> <li>• Create Microsoft Teams Applications <ul style="list-style-type: none"> <li>○ 32 bit</li> <li>○ 64 bit</li> </ul> </li> <li>• Provide User Test Case Documents</li> </ul>






	<b>Exchange Online</b>	<ul style="list-style-type: none"> <li>• Configuring a Microsoft Exchange Server hybrid deployment.</li> <li>• Configuring email migration.</li> <li>• With email migration.</li> <li>• Configuring Exchange Online Unified Messaging (UM).</li> <li>• Help with mail-enabled application remediation.</li> <li>• Configuring public folder coexistence for Microsoft Exchange Server 2013, Microsoft Exchange Server 2010, or Microsoft Exchange Server 2007.</li> </ul>
	<b>Microsoft Defender Advanced Threat Protection</b>	<ul style="list-style-type: none"> <li>• Licensed users who classify(label or protection) content or consume classified content.</li> <li>• Threat Protection for 1<sup>st</sup> party app</li> <li>• Threat Protection for 3<sup>rd</sup> party app</li> </ul>
	<b>SharePoint Online</b>	<ul style="list-style-type: none"> <li>• Conduct one four-hour workshop with the customer to identify, and then assess, up to 20 site collections and 50 GB of data that are to be migrated into a SharePoint Online tenant.</li> <li>• Create site migration mapping documentation.</li> <li>• Build, configure, and prepare all required infrastructure for the migration environments: <ul style="list-style-type: none"> <li>○ Microsoft Azure Migration Tenant</li> <li>○ On-premises migration workstation installation</li> <li>○ Azure-based migration workstations</li> </ul> </li> <li>• Set up and configure the Migration Management Site: <ul style="list-style-type: none"> <li>○ Site Status Tracking.</li> <li>○ Reporting.</li> <li>○ Issues Management.</li> </ul> </li> <li>• Migrate up to 50 GB of content, as measured in the source.</li> <li>• Support customer validation of content for one day.</li> <li>• Present demonstration and migration results. <ul style="list-style-type: none"> <li>○ Present management stakeholder review on next steps</li> </ul> </li> </ul>

### 3. FastTrack Workloads Deployment activities

#### 3.1 Office 365 & Teams Deployment Activities

	Assess			Remediate	Enable	Migrate	
	Kick-off	Assessment workshops	Finalize deployment plan and remediation checklist	Baseline offer assumes three-week remediation efforts	Office 365 enablement	Pilot migration	Velocity migration
Key Activities	Facilitate a set of assessment workshops that are focused on each Office 365 service as defined in the Microsoft FastTrack service description.			Provide remote technical guidance and track Office 365 remediation activities.	Configure Office 365 services according to the Microsoft FastTrack Onboarding benefit description.	Validate that mailboxes are ready for velocity migration.	<ul style="list-style-type: none"> <li>Perform velocity mailbox migrations.</li> <li>Determine the success or failure of mailbox migrations.</li> </ul>
	Facilitate a set of assessment workshops that are focused on Office 365 onboarding service features to align the core Office 365 onboarding scope and its enhanced service features.			Provide additional project management and technical assistance to help make required configuration changes in the customer environment.	Help the customer with implement changes in the customer environment that help support migration to Office 365.	Help the customer define migration schedules and provide technical assistance that can help support mailbox migrations.	Help the customer define migration schedules and provide technical assistance that can help support mailbox migrations.
	Provide business and technical project resources who can participate in environment and change management assessment workshops and provide information to Microsoft teams that can lead to better alignment with overall Office 365 onboarding activities.			Promote remediation activities by making configuration changes that help move the customer environment to Office 365	Configure the customer environment to support migration to Office 365.	<ul style="list-style-type: none"> <li>Schedule pilot mailboxes for migration to Office 365.</li> <li>Address technical problems to promote a successful mailbox migration to Office 365.</li> </ul>	<ul style="list-style-type: none"> <li>Schedule mailboxes for migration to Office 365.</li> <li>Address technical issues to promote a successful mailbox migration to Office 365.</li> </ul>
Key Outcomes	Office 365 deployment plan and remediation checklist			<ul style="list-style-type: none"> <li>Configuration changes that were documented in the remediation checklist</li> </ul>	<ul style="list-style-type: none"> <li>Infrastructure configured for Office 365 Services consumption.</li> </ul>	Migration of validation mailboxes has been completed	Customer mailboxes have been migrated to the Exchange Online service.

#### 3.2 Microsoft SharePoint Online Deployment Activities

Assess 	Enable 	Migrate 	Close 	Next steps 
<ul style="list-style-type: none"> <li>Review inventory of Microsoft SharePoint 2007 or SharePoint 2010 site collections.</li> <li>Choose up to 20 site collections and up to 50 GB of content.</li> <li>Push the identified content databases into Azure.</li> </ul>	<ul style="list-style-type: none"> <li>Prepare a SharePoint on-premises instance.</li> <li>Ship migration data to the Microsoft Azure tenant.</li> <li>Set up and configure the migration management site.</li> <li>Activate the notification web part.</li> </ul>	<ul style="list-style-type: none"> <li>Migration of data from SharePoint 2007 or SharePoint 2010.</li> <li>Perform a single velocity migration event to migrate content into SharePoint Online.</li> <li>Support end-user testing.</li> </ul>	<ul style="list-style-type: none"> <li>Prepare the final content migration report.</li> <li>Deliver the closeout presentation to stakeholders.</li> </ul>	<ul style="list-style-type: none"> <li>Identify follow-up engagements to develop additional migration planning.</li> <li>Identify additional Microsoft Services offers that could accelerate time to value.</li> </ul>

1.

Two week duration

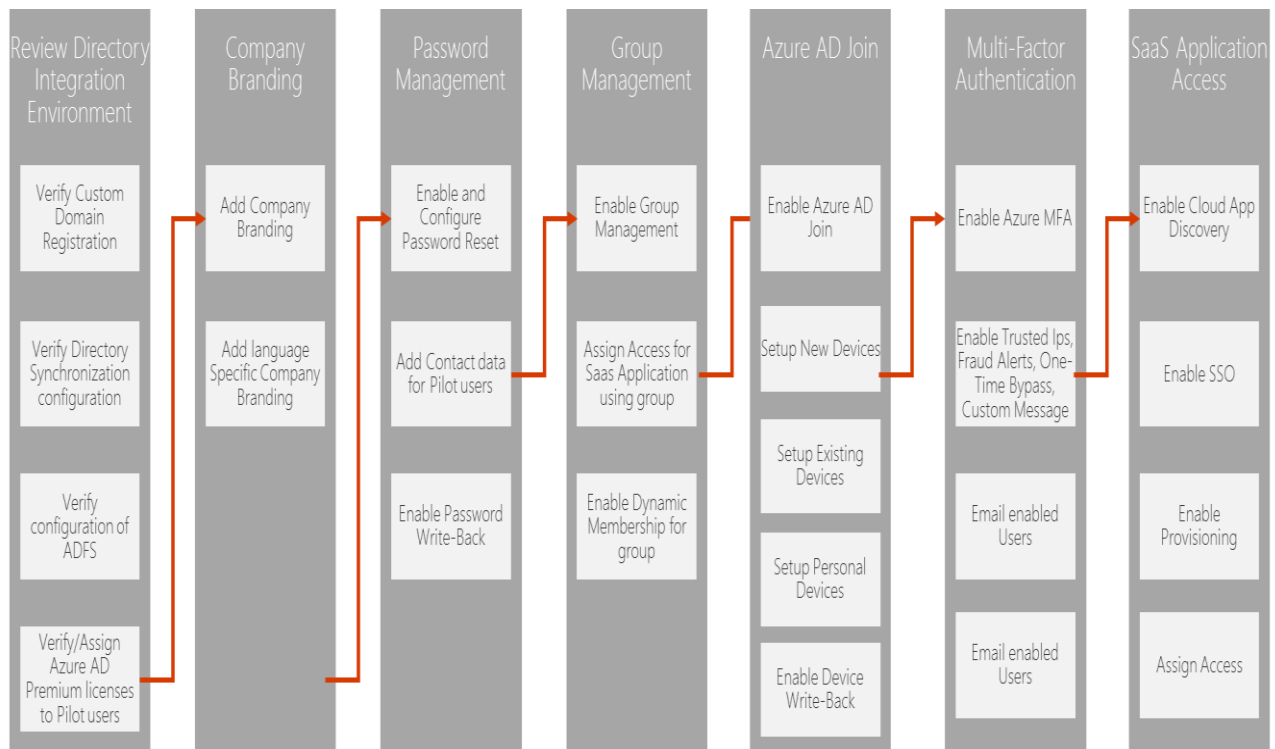
### 3.3 Microsoft Enterprise Mobility Service (EMS)

Assess 	Plan 	Enable 	Pilot 	Next Steps 
<ul style="list-style-type: none"> <li>Deliver kick-off meeting</li> <li>Deliver assessment and technical workshop(s)</li> <li>Develop remediation checklist</li> <li>Develop deployment requirements and plan</li> </ul>	<ul style="list-style-type: none"> <li>Plan Project activities</li> <li>Plan and implement policies</li> <li>Plan Solution Design, end-user communication/ marketing</li> <li>Definition of switch processes</li> </ul>	<ul style="list-style-type: none"> <li>Provide technical guidance for on-premises infrastructure</li> <li>Assistance with communications, training and change management</li> <li>Validate service enrolment</li> </ul>	<ul style="list-style-type: none"> <li>Target / Pilot environment installed</li> <li>De-provisioning from existing environment</li> <li>Provisioning of 150 Test devices in new environment</li> <li>5 Apps are successfully deployed</li> </ul>	<ul style="list-style-type: none"> <li>Enhanced features</li> </ul>
One week	Two weeks	Two weeks	Additional weeks	

### 3.4 Azure Active Directory Premium

This section details each of the features of the Azure Active Directory Premium Service component, including required decisions and configuration parameters.

The table below describes the design decisions for the Azure Active Directory Premium environment Implementation Activities and Tasks





## 3.5 Microsoft Intune

The purpose of this document is to provide operational specialists the steps required to implement the Network Device Enrollment Service (NDES) to support Microsoft Intune, the Mobile Device Management (MDM) and Mobile Application Management (MAM) component of Microsoft's Enterprise Mobility Suite. NDES enables the deployment of Certificate Profiles to Mobile devices using Simple Certificate Enrollment Protocol (SCEP) which allows for the deployment of Wi-Fi, VPN and email profiles on the devices.

### 3.5.1 The objective of this engagement is to:

- Integrate the Microsoft Office 365 FastTrack Onboarding Center deployment plan and remediation requirements into the customer's overall EMS deployment program.
- Provide the customer with onsite technical assistance and project management to complete the remediation and customer activities required for onboarding to EMS.
- Assist the customer with enrolling up to 150 users and devices in a production pilot of EMS prior to the full deployment. The pilot includes Microsoft Intune, Microsoft Azure Active Directory Premium and Azure Rights Management Services (RMS).
- Assist the customer in activating Multi-Factor Authentication (MFA) for administrative users.
- Assist the customer with building a user communication plan for EMS.
- Assist the customer to activate multi-forest directory synchronization to Azure Active Directory.
- Assist the customer in activating and configuring Active Directory Federation Services (AD FS) client access policies.
- Assist the customer in designing and configuring a Geo-Redundant AD FS configuration.
- Assist the customer in validating and gathering requirements for their Mobile Device Management (MDM) and Mobile Application Management (MAM) Solution.
- Assist the customer in mapping a uniform and distinctive policy planning process between the current MDM Solution and Microsoft Intune.
- Assist the customer in identifying core dependencies for the Solution.
- Assist the customer with the technical design of the Solution.
- Assist the customer with the test plan and performing tests.
- Assist the customer with the production pilot.

## 3.6 Teams Apps and platforms

### 3.6.1 Engagement Overview

- Microsoft Teams platform overview –Review Teams platform capabilities and new automation and integration scenarios.
- Scenario analysis –Identify and prioritize customer scenarios for Teams solutions.
- Solution design –Alignment on high-level solution architecture to meet scenario requirements.
- App activation and enablement –Review of various governance policies to enable apps in Teams.
- Provide Adoption Kit –End user training, workload introductions, and support resources.
- Success plan –Creation of a plan with a scope of work, identifying a pilot group of users and high-level timelines.

### 3.6.2 The objective of the engagement

- Microsoft Teams platform overview –Review Teams platform capabilities and new automation and integration scenarios.
- Scenario analysis –Identify and prioritize customer scenarios for Teams solutions.
- Solution design –Alignment on high-level solution architecture to meet scenario requirements.
- App activation and enablement –Review of various governance policies to enable apps in Teams.
- Provide Adoption Kit –End user training, workload introductions, and support resources.
- Success plan –Creation of a plan with a scope of work, identifying a pilot group of users and high-level timelines.

## 3.7 Teams Phone System Workshop

### 3.7.1 Engagement overview – high level

The scope of this engagement is to perform a detailed analysis of the customer's current environment, including user personas, devices and calling workloads. The objective is to jointly create a customized, prioritized, and actionable upgrade plan to move users to Microsoft Teams for Calling.

### 3.7.2 Engagement objectives

The objectives for the Teams Calling Workshop engagement are:

- Evaluation of your current telephony and PBX needs
- Environmental & workload analysis
- Demonstrate the end to end Teams Calling experience
- Direction on how to transform various user profiles into modern collaboration and communication environment
- Document the Journey from PBX to Teams for calling
- Customized report-out with actionable recommendations you can follow to enable, and adopt Teams for Calling

In this workshop the expectation is that you have covered the following topics:

- Microsoft teams calling experience
- Management scenarios for calling
- Use case and scenario discovery
- User, business and administrator roles in Teams Calling
- Environmental and site analysis

The following activities will be completed:

- Evolution of Voice
- Evolution of Voice management scenarios
- PBX to Teams Journey
- Workload analysis

## 3.8 Teams Meeting

### 3.8.1 Engagement overview – high level

The Meetings and Meeting Rooms Workshop includes three distinct phases:

1. Assess – Gather information on current environment and meeting practices
2. Art of the Possible – Showcase modern meeting experiences powered by Microsoft Teams
3. Build the Plan – Planning workshop for how to deploy and adopt Microsoft Teams meetings

### 3.8.2 Project Scope

1. Phase 1: Assess or pre-engagement
  - Identify key business decision maker stakeholders

- Gather information about customer environment
- Research customer challenges and opportunities
- Prepare for deep dive planning workshop
- 2. Phase 2: Art of the Possible, modern meeting immersive experience
  - Demonstrate how Microsoft Teams can solve your specific meetings challenges
  - Explore business cases in real-time and experience the future of meetings
- 3. Phase 3: Build the Plan
  - Discuss findings and recommendations
  - Receive a detailed actionable deployment and adoption framework that will help you transform meetings

### 3.8.3 Deliverables

<b>Deliverable</b>	<b>Description</b>
Assess or pre-engagement	Pre-engagement consultation to gather information on current environment and meetings practices
Art of the Possible	Immersion experience to showcase modern meeting experiences powered by Microsoft Teams
Build the Plan	Planning workshop to build the plan for how to deploy and adopt Microsoft Teams meetings
Report and recommendations PPT	Report showing recommendations

## 3.9 Azure Information Protection (AIP)

This section details the implementation of the Azure Rights Management Service developed for the customer environment and the steps to install, configure, and operate the required component that will deliver the AIP capability.

The following high-level activities are needed:

This section details each of the features of the Azure Rights Management Service component, including required decisions and configuration parameters.

Features	Description
<b>Azure RMS</b>	Core Azure RMS component
<b>Azure RMS Connector</b>	To support Cross premise Scenario for on premise Exchange/SharePoint/FileServers
<b>Azure RMS Delegated Administrators</b>	Groups and users delegated administrator privileges
<b>Azure RMS Super Users</b>	Super Users allowed to open all protected documents
<b>Tenant Key</b>	Private key used to sign all certificates and licenses
<b>Rights Policy Templates.</b>	Custom templates used to apply protection
<b>Logging Service</b>	Functionality to log all RMS activities
<b>Trusts</b>	Trusts with other organizations

### 3.10 Microsoft Defender Advanced Threat Protection

Microsoft Defender ATP is a comprehensive solution for preventing, protecting, detecting, and automating the investigation of and response to threats on endpoints. It's a core part of Microsoft Threat Protection, which combines and orchestrates the capabilities of Microsoft Defender ATP, Office 365 ATP, Azure ATP, and Microsoft Cloud App Security.

#### 3.10.1.1 Azure Advanced Threat Protection

Azure ATP is a cloud-based security solution that leverages your on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.

#### 3.10.1.2 Objectives

- To provide an understanding of the threats that ATA can provide detection services for.
- Assist with the creation of a response plan specific to the events that Microsoft Advanced Threat Analytics may identify.

- Assist with the design and deployment of Microsoft Advanced Threat Analytics to monitor for threats to Customer Name’s production Active Directory Domain Services (AD DS) environment.

### 3.10.1 Project Scope

The following table details the specific items supporting this scope that will be included.

Solution Component	Description or Considerations	Scope Assumptions
Educational workshops	<p>Microsoft will conduct three educational workshops that will be focused on the following topic areas (one workshop per topic area):</p> <ul style="list-style-type: none"> <li>• Understanding of the Cybersecurity Framework</li> <li>• Advanced Threat Analytics Overview</li> <li>• Deep dive into events that ATA monitors</li> </ul>	<ul style="list-style-type: none"> <li>• Personnel who would be responsible for making decisions if ATA detects a threat will attend these sessions.</li> <li>• Personnel who will be responsible for designing, deploying, and operating ATA will attend these sessions.</li> </ul>
ATA response planning workshops	<p>Partner will conduct four workshops, during which GCT personnel will help build a response plan that is specific to events that AATP might identify. The workshops will cover the following topic areas (one workshop per topic area):</p> <ul style="list-style-type: none"> <li>• Response team identification and responsibility definition</li> <li>• ATA event definition and classification</li> <li>• ATA event handling and response process definition</li> <li>• Organizational communication process definition</li> </ul>	<p>Personnel who are responsible for determining the following will attend the workshops:</p> <ul style="list-style-type: none"> <li>• Response team identification and responsibility definition</li> <li>• ATA event definition and classification</li> <li>• ATA event handling and response process definition</li> <li>• Organizational communication process definition</li> </ul>
ATA design workshops	<p>GCT will lead up to 1 design workshops that will be used to determine the specific ATA design that will be required to address the in-scope solution.</p>	<p>Required Customer Name personnel will attend these meetings. Decisions that will affect the final design will be made during the meetings.</p>
Production deployment of ATA	<p>GCT will help customer deploy "[Enter # of ATA Centers]" ATA Center and up to</p>	<p>GCT will help Customer Name deploy ATA into a production environment.</p>

	"[Enter # of ATA Gateways]" ATA Gateway listeners that will monitor the "[Enter AD DS Forest FQDN Here]" production AD DS forest.	
ATA tuning	Microsoft will assist Customer Name with reviewing of events that were identified by ATA after installation for up to "[Enter number of hours]" hours and will help address any false positives that are captured during this time.	Customer Name will assign operational staff that will work side by side with the Microsoft team to review any events that ATA captures and to determine, follow up on, and address any false positives as they occur. This assistance is limited to 40 hours over a one-week period.

### 3.11 Microsoft Edge

The purpose of this task is to provide guidance on the recommended practices for deploying the new Microsoft Edge in an enterprise environment using the public-facing Edge deployment plan documentation, and to collect/document details (using the wizard attached to this task) on:

- Customer's existing Internet browser type
- Deployment tools and configuration tools in use for their Windows PC
- Which Edge advanced features will be required, especially if IE Mode is needed and if an additional Site discovery (Enterprise Site List build) would be required

### 3.12 Microsoft Defender for Endpoint

Microsoft Defender for Endpoint is a platform designed to help enterprise networks to prevent, detect, investigate and respond to advanced threats on Endpoints.

#### 3.12.1 The engagement objectives:

- Deploy the Microsoft Defender to secure endpoints and configure endpoint protection and device restrictions profiles.
- Assess the operating system version and device management as well as the status of the client's Windows Defender AV services or other endpoint security software.
- Providing Cloud PC security baseline guidance specifically for: Attack surface reduction rules, Microsoft Defender Antivirus exclusion, Microsoft Defender SmartScreen.
- Assessing the status of the windows AV services or other endpoint security software.
- Assessing proxies and firewalls restricting network traffic.
- Explaining how to deploy a Microsoft Defender for Endpoint Detection and Response (EDR) agent profile using one of the supported management methods.

- Deploy guidance, configuration assistance and education on : Threat and vulnerability management; Attack surface reduction; Next-generation protection; EDR; Automated investigation and remediation; secure score for devices; Microsoft Defender SmartScreen configuration using Microsoft Endpoint Manager; and Device discovery.
- Reviewing simulations and tutorials (like practice scenarios, fake malware and automated investigation).
- Integrating Microsoft Defender for Office 365 with Microsoft Defender for Endpoint.
- Conduct walkthroughs of the Microsoft Defender Security Portal.

### 3.12.2 The following activities will be completed:

- Threat and vulnerability management.
- Attack surface reduction
- Next generation protection
- EDR (Endpoint Detection and Response)
- Automated investigation and remediation.

## 3.13 Microsoft Defender for Identity

Microsoft Defender for Identity is a cloud-based security solution that leverages your on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.

### 3.13.1 The engagement objectives:

- Create the client's instance of Defender for Identity
- Connecting Defender for Identity to Active Directory
- Deploying the sensor to capture and parse network traffic and windows events directly from the client's domain controllers including downloading the sensor package; configuring the sensor on the client's domain controller silently (in the background); deploying the sensor to the client's multi-forest environment; and configuring the Windows Event Collector.
- Configuring the portal, including: integrating Defender for Identity with Microsoft Cloud App Security; configuring entity tags; tagging sensitive accounts; receiving email notifications for health issues and security alerts; configuring alert exclusions.
- Facilitating the migration from Advanced Threat Analytics (ATA) to Defender for Identity.
- Providing deployment guidance, configuration assistance and education on: understanding the identity Security Posture Assessment report; understanding the User Investigation Priority Score and User Investigation ranking report; understanding the inactive user report; and explanation on a compromised account.



## 3.14 Microsoft Defender for Office 365

The Microsoft Defender for Office 365 safeguards the organization against malicious threats posed by email messages, links (URLs), and collaboration tools.

### 3.14.1 The Project scope

- Threat protection policies which are defined to set the level of protection for the organization.
- Viewing real time reports to monitor Defender for Office 365 performance in the organization
- Threat investigation and response capabilities
- Automated investigation and response capabilities.

### 3.14.2 The engagement objectives:

- Provide guidance for enabling safe links, Safe Attachments, and anti-phishing.
- Provide guidance for configuring automation, and response.
- Provide guidance on using Attack Simulator.
- Provide guidance on reporting and threat analytics.
- Providing guidance for understanding incident correlation in the Microsoft 365 Defender portal.

## 4. Change management activities.

The following phases will be followed to drive change and increase adoption of the Microsoft Cloud Services

### 1. Start Phase

- a. Plan initial adoption
- b. Validate adoption prerequisites
- c. Assemble the team
- d. Assess your organization's readiness for change

### 2. Experiment Phase

- a. Create champions program
- b. Complete governance quick start
- c. Define use cases
- d. Finalize early adopters program
- e. Setup feedback channels
- f. Bring support staff on board

### 3. Scale Phase

- a. Define outcomes and success measures.
- b. Select service strategy.
- c. Engage stakeholders.
- d. Design and launch an awareness campaign.
- e. Design and launch a communication campaign
- f. Design and launch a training program.
- g. Understand reporting tools.
- h. Prepare for ongoing business engagement.
- i. Prepare for ongoing service health & adoption reviews.