# 

Statement of Work

Azure Active Directory Implementation Services

Prepared for

Prepared by

Date: 20 Feb 2020

Version: 1.0

Table of contents

[Introduction 1](#_Toc33095730)

[1. Project objectives and scope 1](#_Toc33095731)

[1.1. Objectives 1](#_Toc33095732)

[1.2. Areas in scope 2](#_Toc33095733)

[1.3. Areas out of scope 8](#_Toc33095734)

[2. Project approach, timeline, and deliverable acceptance 10](#_Toc33095735)

[2.1. Approach 10](#_Toc33095736)

[2.2. Timeline 16](#_Toc33095737)

[2.3. Deliverable acceptance process 16](#_Toc33095738)

[2.4. Project governance 17](#_Toc33095739)

[2.5. Project completion 18](#_Toc33095740)

[3. Project organization 18](#_Toc33095741)

[3.1. Project roles and responsibilities 18](#_Toc33095742)

[4. Customer responsibilities and project assumptions 20](#_Toc33095743)

[4.1. Customer responsibilities 20](#_Toc33095744)

[4.2. Project assumptions 21](#_Toc33095745)

This Statement of Work (SOW) and any exhibits, appendices, schedules, and attachments to it are made pursuant to Work Order **7-TWNTOSPDU** and describes the work to be performed (Services) by Microsoft (“us,” “we”) for (“Customer,” “you,” “your”) relating to the implementation of Azure Active Directory (project).

This SOW and the associated Work Order expire 30 days after their publication date, unless signed by both parties or formally extended in writing by Microsoft.

Introduction

Singapore’s Ministry of Education () has taken on the initiative to revisit their Identity Management Services provided to Singapore’s students, Singapore’s school staff and the HQ Staff. As part of this revisit, the has taken on to implement a solution concept with a new on-premises Identity Management System. Directory Services part of this system synchronizes the identity objects related to students, school staff and HQ staff into Microsoft Azure Active Directory Services.

Within the solution the Microsoft Azure Active Directory Services is envisioned to service the Office 365 tenant dedicated to students and school staff as well as the authentication and authorization source for around hundred and forty (140) student and school staff related applications used by students, school staff and HQ staff totaling up to around five hundred and fifty thousand (550.000) users.

Azure Information Protection (AIP) will be used to protect sensitive information for those users. This solution provides data protection capabilities that can help customers classify, label, and protect sensitive information. The goal is to implement the core information protection capabilities of Microsoft Azure Information Protection.

, as the implementor of the earlier mentioned Identity Management System for their end Customer the Singapore’s Ministry of Education, has engaged Microsoft Services through this Statement of Work to assist them with the planning of the service configuration, usage and operations aspects of the Microsoft Azure Active Directory Services in earlier mentioned context.

# Project objectives and scope

## Objectives

The objective of this project is to integrate the on-premises Active Directory Domain Services (AD DS) environment with Azure Active Directory.

The purpose of this SOW is to provide you with the scope, activities, and timeline necessary to complete these activities, where this project:

* Establishes integration between your on-premises AD DS environments and Azure Active Directory to support onboarding to Microsoft Office 365 or other online services. Azure Active Directory Connect will be installed and configured for synchronization, and authentication will be established using password hash synchronization, pass-through authentication, or federated authentication using Active Directory Federation Services (AD FS) or a third-party identity provider.
* Enables and configures Azure Active Directory self-service password management, self-service group management (SSGM), privileged identity management (PIM), and group-based licensing assignment.
* Enables and configures Azure Multi-Factor Authentication (MFA) and configure Azure Active Directory conditional access policies for a tenant, applying controls to Azure Active Directory–integrated applications including Office 365. Educate on the policy options available and taken through a policy design exercise, after which those policies will be applied to the tenant.
* Enables and configures Azure Active Directory Password Protection for blocking weak passwords in Windows Active Directory
* Enables and configures Azure Active Directory Access Reviews to efficiently manage groups memberships, access to enterprise applications and roles assignments.
* Implement core Azure Information Protection (AIP) capabilities that can help users to manually protect their data.

## Areas in scope

### General project scope

Microsoft will provide Services in support of the following scope.

| Area | Description | Assumptions |
| --- | --- | --- |
| Azure Active Directory integration | Integrate 1 Azure Active Directory tenant with up to one AD DS forest (or forests) for synchronization and authentication. Microsoft will deliver the following to achieve this:  Installation and configuration of Azure Active Directory Connect synchronization to Customer specifications on up to 2 servers (1 primary and 1 staging), limited to options that are configurable through the Azure Active Directory Connect configuration wizard  Configuration of Azure Active Directory authentication using password synchronization, pass-through authentication, or federated authentication  Implementation of the Azure Active Directory seamless single sign-on (SSO) feature optionally if the Customer is not using federated authentication  Installation of the Azure Active Directory Connect Health Agent and demonstrate it to the Customer if the Customer is licensed for Azure Active Directory Premium  Implementation of Azure Active Directory business-to-business (B2B) with basic configuration and demonstrate it to the Customer  If it’s decided that AD FS will be used for authentication, installation and configuration of AD FS and Web Application Proxy (WAP) roles will be performed on up to 8 servers in no more than 2 Customer datacenters, configured for a new AD FS farm using Windows Internal Database (WID) |  |
| Azure Active Directory Identity Management | Implement and configure Azure Active Directory identity management capabilities in one **(1)** Azure Active Directory tenant. Microsoft will deliver the following to achieve this:  Implementation and configuration of Azure Active Directory self-service password reset to Customer specifications  Implementation and configuration of Azure Active Directory self-service group management to support management of cloud-based security groups  Configuration of Azure Active Directory group-based licensing to assign licenses to users based on Customer-defined licensing profiles  Implementation of Azure Active Directory Privileged Identity Management with basic configuration and demonstrate it to the Customer |  |
| Azure Active Directory MFA and Conditional Access | Configure Azure Multi-Factor Authentication (MFA) and Azure Active Directory conditional access in one **(1)** Customer tenant to help secure Azure Active Directory–integrated applications and services, including Office 365. Microsoft will deliver the following to achieve this:  Configuration of Azure MFA to Customer specifications  Design and implementation of Azure Active Directory conditional access policies in the tenant  If the Customer is using AD FS for federated authentication to Azure Active Directory, AD FS issuance authorization rules will be configured to implement controls for legacy authentication.  Implementation and configuration of Azure Active Directory Identity Protection to Customer specifications and demonstrate it to the Customer if the Customer is licensed for Azure Active Directory Premium P2. | Only applications that are integrated with Azure Active Directory will be subjected to MFA or conditional access policy.  If Office 365 will be protected by the solution, the Customer has deployed an Office client that supports modern authentication (Microsoft Office 2013, Microsoft Office 2016, or Office 365).  If access is to be restricted to managed or compliant devices, Microsoft Intune will be used for mobile device management and hybrid Azure Active Directory join will be used for domain-joined computers. Implementation of these services is scoped separately. |
| Azure AD Password Protection and Identity Governance | Configure Azure AD Password Protection for one (1) Windows Server Active Directory forest   * Deploy Azure AD Password protection services proxy services on one (1) member server. * Deploy Azure AD Password protection DC agent service on one (1) domain controller and enable the service in Audit mode.   Configure Azure AD Access Reviews for up to two (2) groups with basic configuration and demonstrate to customer. | Customer is responsible for reviewing the band passwords during the audit mode and determine when they are ready to enforce Azure AD Protection.  Customer is responsible for deploying Azure AD Password DC agent service on all remaining domain controllers. |
| AIP workshop | Microsoft will conduct an AIP education workshop that will help you understand the features and capabilities of the AIP service. | Refer to “training” section |
| Enable Azure Information Protection services | Microsoft will work with you to implement core AIP capabilities in your Azure tenant. This includes verification that you have onboarded your users, assigned appropriate licenses, and received access to both the AIP configuration portal and the Microsoft Azure Rights Management Services (RMS) templates portal. | has an Azure subscription that is associated with the Azure Active Directory directories that the users are in.  has purchased the appropriate Enterprise Mobility and Security or AIP licenses.  All users who will use AIP capabilities have been added to, or synchronized in, ’s Azure Active Directory tenant. |
| Deploying AIP client components | Microsoft will work with you to deploy the AIP client to your domain-joined desktop computers, making use of your existing software deployment approach. | has an existing software deployment tool that can deploy EXE-based software.  Clients that need the AIP client are available in the software deployment tool. |
| Integration with Microsoft Exchange server | Microsoft will deploy a highly available instance of the AIP connector on ’s network and integrate it with the existing Microsoft Exchange Server implementation. | has installed Microsoft Exchange Server 2010, Microsoft Exchange Server 2013, or Microsoft Exchange Server 2016 with the updates needed to support AIP.  https://docs.microsoft.com/en-us/information-protection/get-started/requirements-servers |
| Integration with Microsoft Exchange online | Microsoft will integrate ’s Exchange Online implementation with AIP. |  |

### Software products and technologies

The products and technology that are listed in the following table are required for the project. The Customer is responsible for obtaining all identified licenses and products.

| Product and technology item | Version | Ready by |
| --- | --- | --- |
| Windows Server Active Directory Domain Services | 2008–2016 | Start of the project |
| Azure Active Directory | Basic or Premium | Start of the project |
| Azure Active Directory Premium (Required for self-service password and group management; group-based license assignment can be implemented with Azure Active Directory Basic) P2 is required for Azure Active Directory Identity Protection. | P1 or P2 | Start of the Enable phase |
| Modern Office client | 2013, 2016, or 365 | Start of the Enable phase |
| AIP license | https://azure.microsoft.com/en-us/pricing/details/information-protection/ | Customer |

### Data migration

Data migration is not in scope for this SOW.

### System integration

The following system integration is in scope for the project.

| Integration | Description of scope | Responsibility | | Ready by |
| --- | --- | --- | --- | --- |
| Azure Active Directory | AD DS will be integrated with Azure Active Directory. | Microsoft with Customer support | End of the project | |
| Exchange server | Exchange server will be configured to use information protection templates for the manual protection of email to the following servers:  **In scope:** One Exchange Server 2010, Exchange Server 2013, or Exchange Server 2016, with the updates that will be needed to integrate Exchange Server with AIP through the AIP connector. | Microsoft | Customer | |
| Exchange server | One Exchange Server will be configured with DLP policies to the following servers:  **In scope:** Exchange Server 2010, Exchange Server 2013, or Exchange Server 2016 with the updates that will be needed to use transport rules to apply DLP policies. | Microsoft | Customer | |
| Exchange online | Exchange Online will be configured to use information protection templates for the manual protection of emails.  **In scope:** Configuration of Exchange Online that will help it integrate with Azure Rights Management. | Microsoft | Customer | |
|  | Exchange Online will be configured with DLP policies.  **In scope:** Configuration of Exchange Online that will help DLP policies be applied. | Microsoft | Customer | |

### Environments

The following environments will be required to deliver the project.

| Environment | Location | Responsibility | Ready by |
| --- | --- | --- | --- |
| Development | Customer facility | Customer | Start of Remediate phase |
| Test | Customer facility | Customer | Start of Remediate phase |
| Production | Customer/Azure | Customer | Start of Remediate phase |

### Testing and defect remediation

#### Testing

The following testing is included in the scope of the project. If additional time is needed for Microsoft testing support, then it can be requested through the Change management process described in this SOW.

| Test type (environment) | Description | Responsibility | | |
| --- | --- | --- | --- | --- |
| Has responsibility  for testing? | Provides data or test cases | Provides guidance and support |
| Validation testing (production) | Test cases will be run in the production environment to validate that the implemented solution is functioning as designed. | Microsoft | Microsoft | Customer |

#### Defect remediation

If defects are identified during testing, the priority of the item will be jointly agreed upon by the Customer and Microsoft. Defect prioritization is defined in the following table.

| Priority | Description | Remediation in scope? |
| --- | --- | --- |
| P1 | **Blocking defect**  Development, testing, or production launch cannot proceed until this type of defect is corrected. A defect of this type blocks further progress in this area. The solution cannot ship, and the project team cannot achieve the next milestone until such a defect is corrected. | Yes |
| P2 | **Significant defect** This type of defect must be fixed prior to moving to production. Such a defect, however, will not affect test plan implementation. | Yes |
| P3 | **Important defect** It is important to correct this type of defect. However, it is possible to move forward into production through the use of a workaround. | No; the problem will be logged. Remediation will be performed through an agreed-upon change request only. |
| P4 | **Enhancements and low priority defects** P4 defects consist of feature enhancement and cosmetic defects. These include design requests that vary from original concepts. | No; the problem will be logged. Remediation will be performed through an agreed-upon change request only. |

## Areas out of scope

Any area not explicitly included in the Areas in scope section is out of scope for Microsoft during this project. Areas out of scope for this project are listed in the following table.

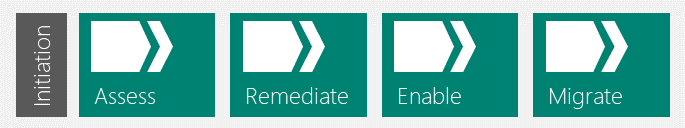
| Area | Description |
| --- | --- |
| Product licenses and subscriptions | Product licenses (Microsoft or non-Microsoft) and cloud service subscriptions are not included. |
| Encryption keys | Bring Your Own Key (BYOK): With BYOK, customers can upload their own generated private key into Microsoft Hardware Security Modules hosted in Azure Key Vault. The implementation of BYOK keys is out of scope for this project.  Hold Your Own Key (HYOK): With HYOK, the Customer can have a hybrid Active Directory RMS and AIP deployment with on-premises keys that are used for some of the classification policies. The implementation of HYOK is out of scope for this project. |
| AD FS | Customization of AD FS sign-in pages is out of scope.  AD FS integration with applications or services beyond Azure Active Directory is out of scope. |
| Azure Active Directory Application Integration | Integrate on-premises or Azure Active Directory gallery applications with Azure Active Directory for authentication |
| Azure Active Directory identity management | Changes to individual group objects to accommodate self-service management in Azure Active Directory, including conversion of synchronized groups to cloud-based groups, is out of scope. |
| Azure MFA server or third-party MFA providers | Deployment of the on-premises Azure MFA server is outside the scope of this project, as is integration with a third-party multi-factor authentication provider. |
| Azure Active Directory Password Protection | Deploying Azure AD Password DC agent service on all remaining domain controllers except the domain controllers in scope  Enforcement of Azure AD Password Protection in Windows Active Directory Forest. |
| Product licenses and subscriptions | Product licenses (Microsoft or non-Microsoft) and cloud service subscriptions are not included. |
| Hardware | Microsoft will not provide hardware for this project. |
| Integration with third-party software | Microsoft will not be responsible for integration with third-party software. |
| Data migration | Data migration activities are not in scope for this project. |
| Product bugs  and upgrades | Product upgrades, bugs, and design change requests for Microsoft products are not in scope for this project. |
| Source code review | The Customer will not provide Microsoft with access to non-Microsoft source code or source code information. For any non-Microsoft code, Microsoft Services will be limited to the analysis of binary data, such as a process dump or network monitor trace. |
| Process reengineering | Designing functional business components of the solution is not included. |
| Organizational change management | Designing—or redesigning—the Customer’s functional organization is not included. |

# Project approach, timeline, and deliverable acceptance

## Approach

The project will be structured following the Microsoft Online Services Lifecycle methodology across three of the possible four distinct phases: Assess, Remediate, Enable, and Migrate (Migrate is not included in this SOW). Each phase has distinct activities and deliverables that are described in the following sections.

If a deliverable requires formal review and acceptance (a process described in the Deliverable acceptance process section), this is indicated in the following sections.



### Engagement initiation

Before beginning the project, the following prerequisites must be completed.

| Category | Description | |
| --- | --- | --- |
| **Microsoft activities** The activities to be performed by Microsoft | Conduct a preinitiation call to initiate team formation and communicate expectations.  Document the project launch prerequisites using input from this SOW.  Track the status of launch prerequisites and adjust the engagement initiation phase start date accordingly.  Conduct a detailed walk-through of the SOW with the Customer to agree on an initial project schedule and approach. |
| **Customer activities** The activities to be performed by the Customer | Attend and participate in the preinitiation call.  Assign project initiation and launch prerequisite responsibilities to accountable Customer leadership and establish target completion dates.  Complete the project initiation and launch prerequisites.  Staff the project with the required Customer resources in the time frames that were agreed upon in the preinitiation call. |

### Assess

During the Assess phase, Microsoft will conduct a series of workshops to gather design requirements. Microsoft and the Customer will review the results of the planning workshops and jointly determine requirements necessary to support the deployments.

|  | | |
| --- | --- | --- |
| Category | Description | |
| **Microsoft activities** The activities to be performed by Microsoft | * Conduct an assessment and planning workshop to gather requirements, information about the current environment, and Customer design decisions. * Assist the Customer with the implementation of the Office 365 IdFix directory synchronization error remediation tool to identify conflicts and formatting errors in AD DS that need to be remediated prior to directory synchronization. * Produce a preparation checklist that details the tasks that must be completed to facilitate implementation of the integration solution, including the resources that must be procured. * Conduct an assessment and planning workshop to gather requirements and information about the current environment, provide education related to Azure MFA and Azure Active Directory conditional access capabilities, and facilitate Customer design decisions. * Design Azure Active Directory conditional access policies based on Customer requirements. * AIP workshop: This workshop covers core AIP capabilities for 4 hours. * Produce a design and plan document and review with customer. |
| **Customer activities** The activities to be performed by the Customer | * Participate in the assessment and planning workshop, communicate requirements, provide current environmental information, and make design decisions * Run the Office 365 IdFix tool in each in-scope AD DS forest and provide the results to Microsoft for evaluation. The tool requires read-only permissions in AD DS. |
| **Key assumptions** | None |

#### Deliverables

| Name | Description | Acceptance required? | Responsibility |
| --- | --- | --- | --- |
| Preparation checklist | A Microsoft Excel spreadsheet that documents the tasks that must be completed by the Customer and the resources that must be procured to facilitate the completion of in-scope work. | Yes | Microsoft |
| Design and plan | A Word document that captures design decisions made during the workshop, documents the design for the solution, and details the high-level plan for the completion of in-scope work. | Yes | Microsoft |
| AIP workshop slide deck | This workshop describes core AIP capabilities. | No | Microsoft |

### Remediate

During the Remediate phase, the Customer uses the remediation and deployment plan to prepare the environment for onboarding to Azure Active Directory, with assistance from Microsoft. This preparation includes completion of prerequisites, procurement, and provisioning of required hardware or virtual machines, cleanup of AD DS content, and the deployment of Azure Active Directory Connect. These preparations are based on decisions made during the Assess phase of the project.

|  | |
| --- | --- |
| Category | Description |
| **Microsoft activities** The activities to be performed by Microsoft | * Provide general guidance and answer questions during Customer-led completion of identified preparation tasks. * Provide input to end-user communications related to the solution. * Validate license assignment: Assignment of AIP licenses to the appropriate users. Microsoft will work with to validate that the required licenses are assigned to the appropriate users. If they are not, Microsoft will assist in the remediation. |
| **Customer activities** The activities to be performed by the Customer | * Procure the resources required for the project and complete all identified preparation tasks, including IdFix error remediation in the on-premises AD DS forest and user principal name changes, if necessary. * Complete all identified preparation tasks to facilitating implementation of the solution. * Work with Microsoft to assign AIP licenses to the appropriate users. * Prepare user communications. |
| **Key assumptions** | Items in the preparation checklist can be remediated within 1 week.  has purchased the appropriate licenses for the needed AIP capabilities.  All AIP users have been onboarded to the production Azure Active Directory tenant. |

#### Deliverables

| Name | Description | Acceptance required? | Responsibility |
| --- | --- | --- | --- |
| Preparation checklist completed | An Excel spreadsheet that documents the tasks that must be completed by the Customer and the resources that must be procured to facilitate the completion of in-scope work. | Yes | Customer |

### Enable

During the Enable phase, Azure Active Directory Connect components will be installed in the production environment and components will be tested to validate expected functionality. After validation, Microsoft will perform a final demonstration of functionality. An engagement closeout meeting completes the project.

|  | | |
| --- | --- | --- |
| Category | Description | |
| **Microsoft activities** The activities to be performed by Microsoft | Produce test cases that will be used to validate the implemented solution functions as designed.  Install and configure Azure Active Directory Connect, including Azure Active Directory authentication agents if the Customer selects pass-through authentication.  Complete the initial synchronization with Azure Active Directory and implement ongoing regular synchronization.  Configure the Azure Active Directory seamless SSO feature if the Customer selects it and is not using federated authentication.  If AD FS is chosen for authentication, install AD FS and WAP and configure the farm.  If AD FS is chosen for authentication, provide AD FS product knowledge during the Customer-led configuration of load balancers and other networking equipment.  Configure authentication of Customer domains in Azure Active Directory.  Configure and demonstrate Azure Active Directory Connect Health if the Customer is licensed for Azure Active Directory Premium.  Configure and demonstrate Azure Active Directory B2B.  Produce test cases that will be used to validate the implemented solution functions as designed.  Complete validation testing for the solution.  Produce a delivery summary document.  Configure Azure Active Directory self-service password reset.  Configure Azure Active Directory self-service group management.  Configure Azure Active Directory group-based licensing.  Configure and demonstrate Azure Active Directory Privileged Identity Management (PIM).  Configure Azure MFA.  Implement the Azure Active Directory conditional access policies that were initially scoped for test user accounts.  Implement and configure Azure Active Directory Identity Protection.  Implement and configure Azure Active Directory Password Protection in Audit mode.  Implement and Configure Azure Active Directory Access Review.  Complete validation testing of the solution.  Apply the MFA and conditional access solution to privileged users, this can optionally be performed through a phased rollout. Microsoft will disengage after one **(1)** week of the phased rollout, after which the Customer will be responsible for completion.  Demonstrate Azure Active Directory Identity Protection for the Customer.  Microsoft will implement AIP capabilities in ’s production Azure Active Directory tenant.  Microsoft will deploy 2 AIP connector servers in a high availability configuration.  Microsoft will configure Exchange to make use of Azure RMS templates for manual protection of emails. |
| **Customer activities** The activities to be performed by the Customer | Assist Microsoft, as necessary, during production implementation tasks.  If the Customer selects a third-party federated identity provider, provide subject matter expertise for that identity provider and implement the configuration required to use federated authentication with Azure Active Directory. Engage the product vendor, as necessary.  If AD FS is chosen for authentication, configure load balancers and other networking equipment to establish high-availability for AD FS on the private and perimeter network and publish AD FS to the Internet.  If AD FS is chosen for authentication, customize AD FS sign-in pages, as desired, to apply organizational branding.  Manage all user communication related to the rollout of the MFA, AIP, and conditional access solution.  Provide the access or personnel needed to configure the Exchange server environment for rights management.  Provide the access or personnel needed to configure the SharePoint server environment for rights management.  Provide the access or personnel needed to configure the Exchange Online service for rights management.  If deploying the solution to users through a phased rollout more than 1 week in duration, complete the rollout to users after Microsoft disengages.  Participate in a demonstration of Azure Active Directory Identity Protection.  Participate in solution validation testing.  Take ownership of the solution used for ongoing management and support. |
| **Key assumptions** |  |

#### Deliverables

| Name | Description | Acceptance required? | Responsibility |
| --- | --- | --- | --- |
| Test cases | An Excel spreadsheet that documents the test cases that will be conducted to validate that the implemented solution functions as designed. | Yes | Microsoft |
| Delivery summary | A Word document that summarizes the work completed, provides relevant maintenance guidance, and documents recommended next steps. | No | Microsoft |
| AIP connector server architecture diagram | This Microsoft Visio diagram is used to define the architecture that is used when the AIP connector is being deployed on premises. | Yes | Microsoft |

### Migrate

This SOW does not include a Migrate phase.

## Timeline

During project planning, a detailed timeline will be developed. All dates and durations are relative to the project start date and are estimates only.

## Deliverable acceptance process

During the project, Microsoft will submit certain deliverables (listed in the Approach section as deliverables with “Acceptance required?” equal to “Yes”) for the Customer’s review and approval.

Within **three (3)** business days of the date of submittal, the Customer is required to:

* **Accept the deliverable** by signing, dating, and returning a service deliverable acceptance form, which can be sent by email, or by using (or partially using) the deliverable

Or

* **Reject the deliverable** by notifying Microsoft in writing; the Customer must include a complete list of reasons for rejection.

Deliverables shall be deemed accepted unless the written rejection notification is received by Microsoft in the timeframe specified.

If a rejection notification is received, Microsoft will correct problems with a deliverable that are in scope for the project (and documented in this SOW), after which the deliverable is deemed accepted.

Problems that are outside the scope of this SOW, and feedback provided after a deliverable has been accepted will be addressed as a change request, managed as described in the Change management process section.

## Project governance

The governance structure and processes the team will adhere to for the project are described in the following sections:

### Project communication

The following will be used to communicate during the project:

* **Communication plan**: this document will describe the frequency, audience, and content of communication with the team and stakeholders. It will be developed by Microsoft and the Customer as part of project planning.
* **Status reports**: the Microsoft team will prepare and issue regular status reports to project stakeholders per the frequency defined in the communication plan.
* **Status meetings**: the Microsoft team will schedule regular status meetings to review the overall project status, the acceptance of deliverables, and review open problems and risks.

### Risk and issue management

The following general procedure will be used to manage active project issues and risks during the project:

* **Identify**: identify and document project issues (current problems) and risks (potential problems that could affect the project).
* **Analyze and prioritize**: assess the potential impact and determine the highest priority risks and problems that will be actively managed.
* **Plan and schedule**: determine the strategy for managing priority risks and issues and identify a resource who can take responsibility for mitigation and remediation.
* **Track and report**: monitor and report the status of risks and problems.
* **Escalate**: escalate to project sponsors the high impact problems and risks that the team is unable to resolve.
* **Control**: review the effectiveness of risk and issue management actions.

Active issues and risks will be regularly monitored during the project.

### Change management process

During the project, either party is able to request modifications to the Services described in this SOW. These changes only take effect when the proposed change is agreed upon by both parties. The change management process steps are:

* **The change is documented**: all change requests will be documented by Microsoft in a Microsoft change request form and submitted to the Customer. The change request form includes:
  + A description of the change.
  + The estimated effect of implementing the change.
* **The change is submitted**: the change request form will be provided to the Customer.
* **The change is accepted or rejected**: the Customer has **three (3)** business days to confirm the following to Microsoft:
  + Acceptance—the Customer must sign and return change request form.
  + Rejection—if the Customer does not want to proceed with the change or does not provide an approval within three business days, no changes will be performed.

### Executive steering committee

The executive steering committee provides overall senior management oversight and strategic direction for the project. The executive steering committee for the project will meet per the frequency defined in the communication plan and will include the roles listed in the following table. The responsibilities for the committee include:

* Making decisions about project strategic direction.
* Serving as a final arbiter of project issues.
* Approving significant change requests.

| Role | Organization | |
| --- | --- | --- |
| Project sponsor | End Customer |
| Project sponsor | Customer |
| Delivery manager | Microsoft |

### Escalation path

The Microsoft project manager will work closely with the Customer project manager, sponsor, and other designees to manage project issues, risks, and change requests as described previously. The Customer will provide reasonable access to the sponsor or sponsors in order to expedite resolution. The standard escalation path for review, approval, or dispute resolution is as follows:

* Project team member (Microsoft or the Customer)
* Project manager (Microsoft and the Customer)
* Microsoft delivery manager
* Microsoft and the Customer project sponsor
* Executive steering committee

## Project completion

The project will be considered complete when at least one of the following conditions is met:

* All Microsoft deliverables that require acceptance have been delivered and accepted (or deemed accepted).
* The Work Order has been terminated.

# Project organization

## Project roles and responsibilities

The key project roles and the responsibilities are as follows.

#### Customer

| Role | Responsibilities |
| --- | --- |
| Project sponsor | * Provide the estimated project commitment: 2–4 hours a week * Make key project decisions. * Serve as a point of escalation to support clearing project roadblocks. |
| Project manager | Provide the estimated project commitment: 20 hours a week  Serve as primary point of contact for the Microsoft team.  Manage the overall project.  Deliver the project on schedule.  Take responsibility for Customer resource allocation, risk management, and project priorities.  Communicate with executive stakeholders. |
| Active Directory lead and identity lead (or leads) | Take responsibility for Azure Active Directory and an integrated on-premises AD DS forest (or forests).  Take responsibility for the Azure Active Directory identity management solution going forward. |

|  |  |
| --- | --- |
| Identity lead (or leads) | * Provide requirements for the MFA and conditional access solution and make design decisions. * Take responsibility for Azure Active Directory. * Take responsibility for the MFA and conditional access solution going forward. |
| Security lead (or leads) | * Provide security requirements for the solution. * Optionally, participate in solution validation testing. |
| User communication lead (or leads) | Take responsibility for user communications related to the MFA and conditional access solution. |

|  |  |
| --- | --- |
| Technical team lead | Provide the estimated project commitment: full time  Serve as primary technical point of contact.  Take ownership of technical architecture and code deliverables. |

#### Microsoft

| Role | Responsibilities | |
| --- | --- | --- |
| Delivery manager | Manage and coordinate the overall Microsoft project.  Serve as a single point of contact for escalations, billing issues, personnel matters, and contract extensions. |
| Microsoft project manager | Manage and coordinate Microsoft project delivery.  Take responsibility for issue and risk management, change management, project priorities, status communications, and status meetings.  Coordinate Microsoft and Microsoft subcontractor resources but not Customer resources. |
| Microsoft lead architect | Design the overall solution.  Provide guidance based on Microsoft-recommended practices. |
| Microsoft consultant | Lead workshop and produces document deliverables.  Provide technical support during Customer-led completion of preparation tasks.  Complete all in-scope implementation work. |

# Customer responsibilities and project assumptions

## Customer responsibilities

In addition to Customer activities defined in the Approach section, the Customer is also required to:

* Provide information:
  + This includes accurate, timely (within three business days or as mutually agreed upon), and complete information.
* Provide access to people and resources.
  + This includes access to knowledgeable Customer personnel, including business user representatives, and access to funding if additional budget is needed to deliver project scope.
* Provide access to systems.
  + This includes access to all necessary Customer work locations, networks, systems, and applications (remote and onsite).
* Provide a work environment.
  + This consists of suitable work spaces, including desks, chairs, and Internet access.
* Manage non-Microsoft resources.
  + The Customer will assume responsibility for the management of all Customer personnel and vendors who are not managed by Microsoft.
* Manage external dependencies.
  + The Customer will facilitate any interactions with related projects or programs in order to manage external project dependencies.
* Manage the End Customer ()
  + With regards to the End-Customer () stakeholders and their dependencies.
  + With regards to End-Customer’s () participation during workshops and collect their input and/or feedback if required in a timely manner inline with timelines as outlined in this Statement of Work.
* Provide transparency and inclusiveness
  + On governance level to the Microsoft Team’s governance component with regards to steering community, project status and project management with the end Customer towards matters that would be directly or indirectly related to or influence this project at all times.

## Project assumptions

The project scope, Services, fees, timeline, and our detailed solution are based on the information provided by the Customer to date. During the project, the information and assumptions in this SOW will be validated, and if a material difference is present, this could result in Microsoft initiating a change request to cover additional work or extend the project duration. In addition, the following assumptions have been made:

* Work day:
  + The standard work day for the Microsoft project team is between 8 AM and 5 PM, Monday through Friday.
* Standard holidays:
  + Observance of consultants’ country-of-residence holidays is assumed and has been factored into the project timeline.
* Remote working:
  + The Microsoft project team may perform Services remotely.
  + If the Microsoft project team is required to be present at the Customer location on a weekly basis, resources will typically be on site for three nights and four days, arriving on a Monday and leaving on a Thursday.
* Language:
  + All project communications and documentation will be in English. Local language support and translations will be provided by the Customer.
* Staffing:
  + If necessary, Microsoft will make staffing changes. These can include, but are not limited to, the number of resources, individuals, and project roles.
* Informal knowledge transfer:
  + Customer staff members who work alongside Microsoft staff will be provided with information knowledge transfer throughout the project. No formal training materials will be developed or delivered as part of this informal knowledge transfer.