# **Azure AD Design and Operations Advisory**

Statement of Work

Prepared for

Prepared by

Date: April 17, 2020

Version: 1.1

# Table of contents

[Introduction 1](#_bookmark0)

1. [Project objectives and scope 1](#_bookmark1)
   1. [Areas in scope 1](#_bookmark2)
   2. [Areas not in scope 5](#_bookmark3)
2. [Project approach, timeline, and acceptance 7](#_bookmark4)
   1. [Approach 7](#_bookmark5)
   2. [Timeline 7](#_bookmark6)
   3. [Project governance 7](#_bookmark7)
   4. [Project completion 8](#_bookmark9)
3. [Project Organization 9](#_bookmark10)
   1. [Project roles and responsibilities 9](#_bookmark11)
4. [Customer responsibilities and project assumptions 10](#_bookmark12)
   1. [Customer responsibilities 10](#_bookmark13)
   2. [Project assumptions 11](#_bookmark14)

This Statement of Work (SOW) and any exhibits, appendices, schedules, and attachments to it are made pursuant to Work Order 6CHE203-283284-338044 and describes the work to be performed (Services) by Microsoft (“us,” “we”) for (“”, “Customer,” “you,” “your”) relating to **Azure AD Design and Operations Advisory** (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**

relies on Microsoft Office 365 collaboration platform as well Azure AD as its cloud authentication platform for several years. With some design specificities blocking from migrating to the latest version of Azure AD Connect to take advantage of many new technical capabilities related to security, identity and authentication, Customer has requested advisory services from Microsoft Consulting Services in order to mitigate current limitations, get recommendations on recommended design practices and receive assistance in migrating the solution to a newer version of Azure AD Connect.

In this project, Microsoft will assist with reviewing and reconfiguring existing hybrid identity infrastructure based on Azure Active Directory Connect (Azure AD Connect), designing and assisting in implementation of selected Azure AD capabilities.

# **Project objectives and scope**

## **Areas in scope**

### **General project scope**

Microsoft will provide Services in support of the following scope.

### **Project management and governance**

|  |  |  |
| --- | --- | --- |
| **Area** | **Description** | **Assumptions** |
| Project management and governance | Microsoft will support the Customer with project management and governance on the Customer’s transformation to Microsoft 365 through the following activities.   * Act as single point of contact for all Microsoft-related activities in the context of this project. * Establish the program governance and own the communication plan. * Monitor the consistency of design decisions across workstreams and teams. * Facilitate the collaboration of the different Microsoft structures with the Customer’s stakeholders involved in the project. |  |

|  |  |  |
| --- | --- | --- |
| **Area** | **Description** | **Assumptions** |
|  | * Perform weekly and/or monthly reporting of progress. * Wherever possible project delivery resources will receive recommendations from Azure AD Product Group. |  |

* + - 1. **Azure Active Directory**

|  |  |
| --- | --- |
| **Workstream** | **Description** |
| Azure Active Directory | * Review and analyze the existing integration between your on-premises AD DS environments and Azure Active Directory to support onboarding to Microsoft 365. * Assist in troubleshooting current error messages and investigate blockers for migrating current Azure AD Connect to the newer version * Review current customization rules and join rules, their numbering, precedence and dependencies and provide with recommendations on improvements * Support with advisory and hands-on practices to deploy stand-by Azure AD Connect solution and to migrate the above rules and configuration * Support in testing and validating new solution |

* + - 1. **Review of AD Design Patterns**

|  |  |
| --- | --- |
| **Workstream** | **Description** |
| Active Directory | * Advisory and assessment of capability of Functional Root Level Upgrade in a Legacy Domain Environment (2003 to 2012 or later) |

* + 1. **Software products and technologies**

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

|  |  |  |
| --- | --- | --- |
| **Product and technology item** | **Version** | **Ready by** |
| **The following software is required for Azure Active Directory implementation:** | | |
| Active Directory Domain Services | 2008–2019 | Start of the project |

|  |  |  |
| --- | --- | --- |
| **Product and technology item** | **Version** | **Ready by** |
| Azure Active Directory Premium (if required for self-service password and group management; the group-based license assignment can be implemented with Azure Active Directory Basic.) P2 is required for Azure Active Directory Identity Protection, which is out of scope for phase 1 of the project. | P1 | Build phase |
| Modern Office client | 2013, 2016, or 365 | Start of the Build phase |

### **System integration**

The following system integration is in scope for the project. Given the amount of customizations Microsoft cannot commit to being responsible for the final integration. However, every effort will be made to succeed.

|  |  |  |  |
| --- | --- | --- | --- |
| **Integration** | **Description of scope** | **Responsibility** | **Ready by** |
| Azure Active Directory | On-premises Active Directory Domain Services will be integrated with Azure Active Directory. | Customer with Microsoft support | End of the project |

### **Environments**

The following environments will be required to deliver the project.

|  |  |  |  |
| --- | --- | --- | --- |
| **Environment** | **Location** | **Responsibility** | **Ready by** |
| Production | Customer/Azure | Customer | Project start |

### **Testing and defect remediation**

#### Testing

The following testing is included in the scope of the project. If the Customer has responsibility for testing, the Microsoft effort to support that activity is identified. If additional time is needed for Microsoft testing support, then it can be requested through the [Change management process](#_bookmark8) described in this SOW.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Test type (environment)** | **Description** | **Responsibility** | | |
| Has responsibility for testing? | Provides data or test cases | Provides guidance and support |
| System testing (development) | * System testing focuses on determining whether functionality meets design. During the Plan phase a high-level test plan will be created to guide testing activities. This test plan is a Microsoft | Microsoft | Customer | Customer |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Test type (environment)** | **Description** | **Responsibility** | | |
| Has responsibility for testing? | Provides data or test cases | Provides guidance and support |
|  | Excel workbook listing up to 5 test cases, expected results, and observed results. Testing is focused on Customer- specific scenarios as opposed to generic testing of Azure fundamentals.   * The Microsoft effort to support this testing is limited to the Build and Stabilize phases. |  |  |  |

#### Defect remediation

If defects are identified during testing, the priority of the item will be jointly agreed upon by the Customer and Microsoft. The Microsoft team will attempt to fix all in-scope P1 and P2 defects. If this troubleshooting does not result in root cause identification and resolution within five business days, then additional time can be requested through the [Change management process](#_bookmark8) described in this SOW. 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 not in scope**

Any area not explicitly included in the [Areas in scope](#_bookmark2) section is not in scope for Microsoft during this project. Areas not in 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. |
| 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. |
| Customer change management | Designing—or redesigning—the Customer’s functional Customer is not included. |
| Networking | Configuration of physical network devices, such as routers and firewalls, and virtual network appliances deployed on Azure is not in scope. |
| Certification and accreditation | Customer regulatory compliance certification and accreditation activities outside of general support for existing Customer processes are not in scope. |
| Workloads | Workload application compatibility, custom application remediation, configuration, or integration of workloads, whether Microsoft or third-party, is not in scope. |
| PAW - Physical server setup, management, and maintenance | The following is not in scope:   * Physical server setup, installation, and networking interfaces or evaluation of new hardware or software * Ongoing production operational support |
| PAW - Networking configuration and hardware token usage and management | Internet Protocol Security, smart cards, and FIDO2 devices are out of scope. |

|  |  |
| --- | --- |
| **Area** | **Description** |
| PAW as a virtual machine | Deploying PAWs or productivity workstations as virtual machines is not in scope. |
| PAW - Discovery | Discovery and categorization of administrative tasks and applications are not in scope. |
| PAW - Virtual private network (VPN) integration | Integration of the Customer’s VPN solution is out of scope. |
| AD FS | Configuring ADFS and ADFS integration is out of scope. |
| Azure Active Directory integration | The following is not in scope:   * Enabling Hybrid Azure AD join for Windows down-level devices |
| 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, are not in scope. * Implementation of Entitlement management and Access Reviews |
| Azure AD Password Protection | * Implementation of password protection for Windows Server Active Directory |
| 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. |
| Authentication types for applications published through Azure Active Directory App Proxy | * Web applications that use form-based or [header-based](https://docs.microsoft.com/en-us/azure/active-directory/application-proxy-ping-access) access (Refer to third party product PingAccess) are out of scope. * Web APIs that you want to expose to rich applications on different devices are out of scope. * Applications hosted behind a [Remote Desktop Gateway](https://docs.microsoft.com/en-us/azure/active-directory/application-proxy-publish-remote-desktop) are out of scope. * Rich client apps that are integrated with the Active Directory Authentication Library are out of scope. |
| Azure platform design and implementation | * Design and implement Azure as a platform for cloud-based applications and services. * Develop an infrastructure-as-code solution to implement the design using DevOps practices, and Azure DevOps tooling. |
| Azure operations | * Explain how operations are different in the cloud. * Prepare for required and recommended Azure operations practices. * Develop an operations recommendations summary to identify Azure operational maturity gaps. |

|  |  |
| --- | --- |
| **Area** | **Description** |
| Azure platform management | * Establish basic monitoring and management functionality using Azure Monitor, Alerts, and Log Analytics. |

# **Project approach, timeline, and acceptance**

## **Approach**

The project will be structured and managed by the Customer team with Microsoft Project Management and Governance team supporting project phase orchestration.

## **Timeline**

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

Azure AD Connect Analysis 15 days

Azure AD Connect Implementation Phase 15 days

Buffer time

ion, testing,

(documentat

lab environments, AoB) 15 days

\*Note that for these components, the number of days in this table represents effort in days based on the hours assigned to relevant tasks. Actual calendar duration can be longer in days based on time allocated to the Customer for remediation activities.

## **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:

* **Status reports**: the Microsoft team will prepare and issue regular status reports to project stakeholders on a weekly or fortnightly basis.
* **Status meetings**: Microsoft will hold regular status meetings to review the overall project status, the confirmation of outcomes, and open problems and risks, based on the project status report. The status meeting will occur within the week following the distribution of the status report.

### **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 problems and risks will be regularly monitored during the project.

### **Change management process**

During the project, either party can request, in writing, additions, deletions, or modifications to the

services described in this SOW (“change”). Approved changes will be managed through amendments and could lead to additional costs and schedule impacts. We shall have no obligation to commence work in connection with any change until the details of the change are agreed upon in an amendment signed by the authorized signatories from both parties.

Within three (3) consecutive business days of receipt of the proposed amendment, you must either indicate acceptance of the proposed change by signing the amendment or advise us not to perform the change. If you advise us not to perform the change, we will proceed with the original agreed upon services only. In the absence of your acceptance or rejection within the previously noted time frame, we will not perform the proposed change.

### **Escalation path**

The Microsoft project manager will work closely with the Customer project manager, sponsor, and other designees to manage project problems, 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

## **Project completion**

Microsoft will provide Services defined in this SOW to the extent of the fees available and the term specified in the Work Order. If additional Services are required, the [Change management process](#_bookmark8) will be followed and the contract modified. The project will be considered complete when at least one of the following conditions has been met:

* Fees have been met.
* SOW is terminated pursuant the conditions of the agreement.

# **Project Organization**

## **Project roles and responsibilities**

The key project roles and the responsibilities are as follows.

**Customer**

|  |  |
| --- | --- |
| **Role** | **Responsibilities** |
| Project sponsor | * Make key project decisions. * Serve as a point of escalation to support clearing project roadblocks. |
| Project manager | * 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. |
| Technical team lead | * Serve as primary technical point of contact. * Take ownership of technical architecture and code deliverables. |
| 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. * 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. |
| Active Directory resource | * Implement the changes to Active Directory required to support authentication use cases, if needed. |
| Networking resource | * Provision the network for the Azure Active Directory App Proxy. |

**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 consultants | * 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](#_bookmark5) 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 personnel, including business user representatives, and access to funding if additional budget is needed to deliver project scope.
  + This includes the identification of key personnel (stakeholders, decision makers, architects, and subject matter specialists) to participate in the workshops, design sessions, and testing activities described in the Approach section.
  + This includes allocating enough qualified staff (to run the workstreams in parallel).
* Confirm key personnel availability and coordinate personnel participation.
  + Key personnel will attend workshops and design sessions to provide requirements and participate in the discussions and decision making.
  + Key personnel identified to participate must be empowered to make decisions on behalf of the Customer and to engage and coordinate with other teams.
  + Key personnel will be able to make and approve binding design decisions in three days.
  + Key personnel required for the project will complete all identified preparation tasks to facilitate implementation of the solution
* Provide access to systems.
  + This includes access to all necessary Customer work locations, networks, systems, and applications (remote and onsite).
  + The Customer is responsible for configuring and controlling all Azure subscriptions and consumption.
* Provide a work environment.
  + This consists of suitable workspaces, 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.

## **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:

* Workday:
  + The standard workday for the Microsoft project team is between 8 AM and 5 PM, Monday through Friday.
  + When travel to a Customer location is required, the arrival time, especially on Mondays, might vary depending on the travel time. This also applies for departure time on Fridays.
  + Services not provided during regular business hours (8 AM to 5 PM, Monday through Friday) are subject to an extra charge detailed in the Enterprise Services Work Order.
  + Work outside of regular business hours will be mutually agreed upon with a two-week notice period.
* 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.
  + Microsoft resources will be mobilized up to four weeks from the date of the Work Order signature.
  + If work is interrupted, the activities may be resumed once requested and agreed to by Microsoft. In this case Microsoft may require up to six weeks to mobilize the resources and have the complete project team in place. In this situation Microsoft cannot guarantee that the team members will be the same team members who worked previously in the project.
* 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.
* Other assumptions:
  + All work is to be contiguously scheduled. Any breaks in the engagement calendar must be scheduled four (4) weeks in advance or will be billed without interruption.
  + Customer Lab and / or development facility is available.
  + Any delay on delivering customer required items could impact the delivery schedule.