# 

Statement of Work

Design and Implementation for Active Directory (DIAD)

Prepared for

Prepared by

Date: 22 June 2020

Version: 1.4

Table of contents

[Introduction 1](#_Toc39485650)

[1. Project objectives and scope 1](#_Toc39485651)

[1.1. Objectives 1](#_Toc39485652)

[1.2. Areas in scope 1](#_Toc39485653)

[1.3. Areas out of scope 6](#_Toc39485654)

[2. Project approach, timeline, and deliverable acceptance 7](#_Toc39485655)

[2.1. Approach 7](#_Toc39485656)

[2.2. Timeline 11](#_Toc39485657)

[2.3. Deliverable acceptance process 11](#_Toc39485658)

[2.4. Project governance 12](#_Toc39485659)

[2.5. Project completion 13](#_Toc39485660)

[3. Project organization 13](#_Toc39485661)

[3.1. Project roles and responsibilities 13](#_Toc39485662)

[4. Customer responsibilities and project assumptions 14](#_Toc39485663)

[4.1. Customer responsibilities 14](#_Toc39485664)

[4.2. Project assumptions 15](#_Toc39485665)

This Statement of Work (SOW) and any exhibits, appendices, schedules, and attachments to it are made pursuant to Work Order OF03205-276039-328531 and describes the work to be performed (Services) by Microsoft (“us,” “we”) for (“Customer,” “you,” “your”) relating to Security Modernization (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

# Project objectives and scope

## Objectives

The objective of this project is to deploy a new Active Directory Domain Services (AD DS) environment for . This new AD DS environment will serve as a production directory service that provides authentication and authorization services across a variety of ’s resources. This objective will be met by using the following principles:

* Designed by Microsoft and using the latest Microsoft-recommended practices
* Built by employing the latest security recommendations

## Areas in scope

### General project scope

Microsoft will provide Services in support of the following scope.

| Area | Description | Assumptions |
| --- | --- | --- |
| Design Workshops | Microsoft will lead up to six (6) design workshops to determine specific configuration elements for the AD DS deployment. | All required personnel will attend these meetings.  Decisions will be made during the meetings so the final design can be completed. |
| Domain controllerdeployment (on-premises) | Microsoft will assist with the deployment of up to three (3) AD DS domain controllers within the production network environment for the new forest. | Physical hardware or virtual machines are available on theproduction network and have been built per the specifications that are outlined in the design document for this project. |
| Domain Name Service (DNS) | Microsoft will assist with the configuration of a single Active Directory integrated DNS forward lookup zone to serve as the primary namespace for this AD DS deployment. | It is assumed that will provide an Internet-resolvable DNS namespace that is a subzone of their current DNS namespace to serve as the AD DS DNS namespace. |
| Site structure | Microsoft will assist with the configuration of Active Directory Sites and Services to model the ’s IP subnets as it relates to their network infrastructure. | It is assumed that has a complete listing of all IP subnets that will participate within this new AD DS environment and this list will be given to Microsoft to configure AD DS. |
| Secure Domain Group Policy object (GPO) | A GPO will be deployed that will replace the Default Domain Policy using Microsoft recommended security baselines. | will provide input into the Account Policies portion of this GPO. |
| Secure Domain Controller GPO | A GPO will be deployed that will replace the Default Domain Controllers Policy using Microsoft recommended security baselines. | The settings that are applied within this GPO will remain unchanged. |
| Organizational unit (OU) configuration | A predetermined OU structure will be applied to this configuration which is based upon the tier model for Active Directory Domain Services administration. | The recommended OU structure that is provided as a part of this deployment will remain unchanged. |
| Administrative delegations | An administrative OU model will be deployed following the recommended model for isolating resources per security tiers. This design provides recommendations for Tier 0 (AD service, Services administrators and Domain Controllers) and isolation of this tier with Tier 1 (servers) and Tier 2 (workstations). The detailed delegation model for Tier 1 and Tier 2 is out of scope and should be provided by a following project. | The “Admin” OU model and corresponding delegations as a part of this deployment will remain unchanged. |

### Software products and technologies

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

This project will rely upon functionality that is provided as a part of either the Datacenter or Standard edition of Windows Server 2019. Between those two options, the edition that will be used is solely up to and the requirements of their AD DS deployment. The following table provides additional detail about the required software for this project.

The standard domain controller installation that will be provided includes the following software prerequisites.

**Important note:** unless otherwise agreed to in the work order, temporarily appoints Microsoft to act as its agent for the limited purpose of accepting and agreeing to the user terms of any click-through license agreement that accompanies the software (Microsoft or non-Microsoft) that is listed in this SOW or the work order and is included within the test and development environments. can read these terms by clicking the About box in the toolbar ribbon for the specific product at www.microsoft.com or by requesting a copy from the Microsoft Delivery Manager.

Unless otherwise agreed to in writing in the work order, temporarily entitles Microsoft to act as its agent for the download of the required software. With this authority, Microsoft can apply the known-good media process to download and validate the required software and can compile the software into a specific disk image structure that can be used to build an MDT server or provide a known good build ISO.

| Product and technology item | Version | Ready by |
| --- | --- | --- |
| Windows Server 2019 | Datacenter or Standard | Prior to Enable phase |

The following software packages will be required for the solution and are available as Internet downloads at no cost. Microsoft will provide a text file with packages, versions, and their respective download locations. A script will be provided to help download the required files.

| Name | Provided Through |
| --- | --- |
| Microsoft BgInfo (from the Sysinternals Suite) | Scripted download |
| Microsoft Assessment and Deployment Kit | Scripted download |
| Windows Management Framework | Scripted download |
| Microsoft Report Viewer | Scripted download |
| Microsoft Deployment Toolkit | Scripted download |
| Microsoft .NET Framework | Scripted download |
| Microsoft Attack Surface Analyzer | Scripted download |
| Microsoft Network Monitor | Scripted download |
| Remote Server Administration Tools for Windows | Scripted download |
| Microsoft Local Administrator Password Solution | Scripted download |
| TCPView for Windows (from the Sysinternals Suite) | Scripted download |
| Microsoft Process Explorer (from the Sysinternals Suite) | Scripted download |
| Microsoft Process Monitor (from the Sysinternals Suite) | Scripted download |
| Microsoft PsTools (from the Sysinternals Suite) | Scripted download |
| Microsoft security baseline templates | Scripted download |
| Administrative templates for Windows 10 | Scripted download |

**Note:** The use of Windows Defender is recommended as the antivirus solution for the new AD DS environment. might choose to use their own antivirus software. However, because domain controllers are managed as Tier 0 resources, and the existing antivirus infrastructure also manages other tiers (1 and 2), a new Tier 0–specific antivirus infrastructure would need to be deployed to adequately support the new, in-scope AD DS environment. This new antivirus infrastructure would need to be governed as a Tier 0 resource and managed accordingly, possibly adding overhead.

### Environments

The following environments will be required to deliver the project.

| Environment | Location | Responsibility | Ready by |
| --- | --- | --- | --- |
| Development/Test | Dedicated Secure Room | Customer | Prior to Enable phase |
| Production | Secure Datacenter | Customer | Prior to Enable phase |

### 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 described in this SOW.

| Test type (environment) | Description | Responsibility | | |
| --- | --- | --- | --- | --- |
| Has responsibility  for testing? | Provides data or test cases | Provides guidance and support |
| System and Functional testing (Enable) | System and Functional testing focuses on determining whether functionality meets design. Test cases for this deployment have been prewritten for the specific solution and are based on the design presented in the Systems Design document.  This duration of the activity is **time boxed at three (3)** **days**. | Microsoft | Customer | Microsoft |

#### 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; up to eight (8) hours of P1 defect remediation is in scope. |
| 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. | No; the problem will be logged. Remediation will be performed through an agreed-upon change request only. |
| 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.

**Note:** This project uses a preconfigured AD DS deployment that follows recommended practices. Any changes to the default configuration, aside from those listed as in-scope, are considered out of scope for this project.

| Area | Description | |
| --- | --- | --- |
| Additional AD DS delegations or DS Access Control Lists | This project provides a default AD DS administrative delegation model for managing Tier 0 resources. Placeholder roles are provided for Tier 1 and Tier 2. The detailed delegation model for Tier 1 and Tier 2 is out of scope. Changes or additions to this default model are considered out of scope for this project. |
| Additional AD DS domain controller installation or configuration | This project has been scoped for the deployment of up to three (3) AD DS domain controllers. The deployment of domain controllers beyond this number is considered out of scope for this project. |
| Additional Group Policy Design, Configuration or Implementation | This project will provide two new GPO’s which will override the existing Default Domain and Default Domain Controllers GPO objects which will be based on SCM templates. Additional GPOs for managing general workstations, servers (computer), or user-related objects are out of scope for this project. |
| Additional Testing, including UAT and application testing | This project will perform system testing to validate that the new AD DS environment has been built per the specifications that are listed in the design document for this project. Any additional testing is considered out of scope for this project.  Furthermore, system testing activities have been time-boxed to four days. Testing processes extending beyond this timeframe are considered out of scope for this project. |
| Cloud Services Planning | Planning for cloud services such as Microsoft Azure Networking, Azure Storage, or Azure Active Directory. |
| Data migration | Data migration activities, including the migration of Active Directory objects into this new environment, are not in scope for this project. |
| 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. |
| Directory Migration or Consolidation | Migration, consolidation, or rationalization of AD DS objects, including users, groups, workstations, servers, applications, logon scripts, or group policies. |
| Organizational change management | Designing—or redesigning—the Customer’s functional organization is not included. |
| Process reengineering | Designing functional business components of the solution is not included. |
| Product bugs  and upgrades | Product upgrades, bugs, and design change requests for Microsoft products are not in scope for this project. |
| Product licenses and subscriptions | Product licenses (Microsoft or non-Microsoft) and cloud service subscriptions are not included. |
| Role Definition | Custom definition of roles and the creation of new accounts or roles (such as groups) are out of 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. |
| System integration | System integration and interfaces are not in scope for this project. |

# Project approach, timeline, and deliverable acceptance

## Approach

Microsoft follows a structured approach for the deployment of AD DS environments. This approach is as follows:

* **Assess:** during the Assess phase, Microsoft works with you to begin the project and complete design and planning workshops. The result is an updated AD DS design which will be built and deployed into your production environment during the Enable phase.
* **Enable:** during the Enable phase, Microsoft works with you to prepare, deploy and validate the new AD DS environment into your production network environment.

This section will provide additional detail regarding key activities, work products (Microsoft and ), and assumptions for each phase of this project.

### Assess Phase

The Assess phase begins with the project initiation (kickoff) and ends with the completion of an AD DS design, which will be configured and deployed in the Enable phase.

| Category | Description | |
| --- | --- | --- |
| **Microsoft activities** The activities to be performed by Microsoft | Conduct Kick-off and Scope Validation meeting  Conduct AD DS Design Workshops  Create Solution Design Document and Review with  Create Draft Test Plan Document and Review with |
| **Customer activities** The activities to be performed by | * Work with Microsoft to identify the Project team members * Participate in Kick-off and Scope Validation meeting * Participate in Design Workshops * Facilitate any necessary communication or information in preparation for requests that might result from discussions during the design workshops and information gathering exercises * Make decisions when architectural options are presented * Participate in the review and approval process of the Solution Design Document. * Participate in the review and approval process of the Test Plan Document |
| **Key assumptions** | * SMEs will be available for Design Workshops. * All required personnel will attend design workshops to determine specific configuration elements for the AD DS deployment. Decisions will be made during the workshops so that the final design can be completed. * has a complete listing of all IP subnets that will participate within this new AD DS environment. * will provide an Internet-resolvable DNS namespace that is a subzone of their current DNS namespace to serve as the AD DS DNS namespace. * Physical hardware or virtual machines are available on the production network of and have been built per the specifications that are outlined in the design document for this project. |

#### Workshops

| Workshop | Topics Covered | Maximum Hours per Session | Maximum Number of Sessions |
| --- | --- | --- | --- |
| Kick-off and Scope Validation Workshop | * Initiate the project * Validate scope * Assign appropriate project team members | 4 | 1 |
| Review ’s proposed AD design | * Review of ’s proposed Active Directory design to more thoroughly understand their requirements | 4 | Up to 2 |
| Forest/Domain Name and DNS Design Workshop | * Forest Name * Domain Name * DNS Namespace | 2 | 1 |
| Site Design and Domain Controller Physical/Logical HW Design Workshop | * Site Design * Domain Controller Design * DC Naming | 2 | 1 |
| GPO Design Workshop | * Solution Group Policy * Account Policy Settings | 2 | 1 |
| Administrative Model Workshop | * Solution Administrative Model * Delegations * Role Members | 2 | 1 |

#### Deliverables

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Description | Acceptance required? | Responsibility |
| Solution Design Document | Word document detailing the AD DS design, including any specific configuration details as determined during the design workshops | Y | Microsoft |
| Draft Test Plan Document | Word document detailing the test cases which will satisfy the validation of the deployed environment | N | Microsoft |
| Communications Plan | Plan for communicating with stakeholder groups during the project | N | Customer |
| Project Plan | Schedule for domain controller build and testing activities | N | Customer |

### Enable Phase

During the Enable phase, the AD DS design is installed onto a production network and validated (tested) to make sure that the design meets the specifications in the solution design document. After it is validated, the AD DS deployment is deemed production-ready, and an engagement closeout meeting completes the project.

| Category | Description |
| --- | --- |
| **Microsoft activities** The activities to be performed by Microsoft | * Validate environmental prerequisites * Validate software hash against ’s media * Prepare and update hydration scripts for environment * Create the implementation guide document and review with * Deploy AD DS domain controllers * Complete System Testing * Remediate or mitigate P1 defects within System Testing timebox. * Review and update Test Plan document with testing results and feedback. * Deliver final test plan document and review with |
| **Customer activities** The activities to be performed by the Customer | * Prepare all environment prerequisites including software, hardware, or virtual machines for the deployment of AD DS as illustrated in the solution design document * Provide appropriate personnel to assist in the system testing process * Provide appropriate personnel to assist in mitigating any P1 defects * Fix or mitigate all P2, P3, or P4 defects * Participate in the review and approval process of the test plan document * Attend and participate in the project closeout meeting |
| **Key assumptions** | * All required personnel will work with Microsoft during the system testing processes. * Physical hardware or virtual machines are available on the ’s production network and have been built per the specifications that are outlined in the design document for this project. * will provide change management approvals for the AD DS installations |

#### Deliverables

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Description | Acceptance required? | Responsibility |
| Implementation Guide Document | A Word document that provides step-by-step instructions for installing Active Directory domain controllers | Y | Microsoft |
| Final Test Plan Document | Expanding upon the draft version that was completed during the Assess phase, a Word document that includes all test cases and test results | Y | Microsoft |

## Timeline

During project planning of the project, a detailed project 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 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 problems 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 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 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.

### 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

## 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 will be followed and the contract modified. The project will be considered complete when at least one of the following conditions has been met:

* All fees available have been utilized for Services delivered and expenses incurred.
* The term of the project has expired.
* All Microsoft activities and in-scope items have been completed.
* 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 | * 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. |
| Lead business analyst | * Serve as primary functional point of contact for the team that is responsible for functional business analysis. |

#### Microsoft

| Role | Responsibilities | |
| --- | --- | --- |
| Microsoft project manager | * Manage and coordinate Microsoft project delivery. * Serve as a single point of contact for escalations, billing problems, personnel matters, and contract extensions. * 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 architect | * Provide guidance based on Microsoft-recommended practices. * Identify and manage technical risks. * Quality review of deliverables. |
| Microsoft consultant | * Provide technical design leadership. * Deliver workshops and sessions. * Responsible for development and delivery of technical deliverables. |

# 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.

## 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 Mondays and leaving on a Thursday.
* Language:
  + All project communications and documentation will be in US 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.