# 

Statement of Work

Active Directory Hardening and Privileged Access Workstation

Prepared for

Prepared by

Date: 22 June 2020

Version: 1.1

Table of contents

[Introduction 1](#_Toc4434549)

[1. Project objectives and scope 2](#_Toc4434550)

[1.1. Objectives 3](#_Toc4434551)

[1.2. Areas in scope 3](#_Toc4434552)

[1.3. Areas out of scope 14](#_Toc4434553)

[2. Project approach, timeline, and deliverable acceptance 17](#_Toc4434554)

[2.1. Approach 17](#_Toc4434555)

[2.2. Timeline 27](#_Toc4434556)

[2.3. Deliverable acceptance process 28](#_Toc4434557)

[2.4. Project governance 28](#_Toc4434558)

[2.5. Project completion 30](#_Toc4434559)

[3. Project organization 31](#_Toc4434560)

[3.1. Project roles and responsibilities 31](#_Toc4434561)

[4. Customer responsibilities and project assumptions 33](#_Toc4434562)

[4.1. Customer responsibilities 33](#_Toc4434563)

[4.2. Project assumptions 34](#_Toc4434564)

This Statement of Work (SOW) and any exhibits, appendices, schedules, and attachments to it are made pursuant to Work Order [insert Work Order number] and describes the work to be performed (Services) by Microsoft (“us,” “we”) for c (“Customer,” “you,” “your”) relating to Active Directory Hardening (ADH) and Privileged Access Workstation (PAW) (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

CUSTOMER NAME REMOVED, like many organizations in both the commercial and government sectors, faces an increasingly challenging cyberthreat environment. Attackers have become sophisticated in both attack methodologies and in navigating business and social structures to obtain the information which they are seeking. These modern cyberattackers are adept at rapidly gaining administrative access to computing environments. These attacks are difficult to identify, and they often result in remote malicious actors gaining unfettered access to most or all of an organization’s electronic documents, including emails, reports, presentations, Customer data, and other intellectual property. These attackers sometimes also target an organization as a relay point to attack customers, suppliers, employees, or trusted business partners of that organization.

Protecting against these attacks is a key priority for CUSTOMER NAME REMOVED.

The Microsoft Services Privileged Access Workstation (PAW) offer addresses the need for highly secured workstations for the administration of identity systems, application servers, cloud services, private cloud fabric, and sensitive business functions. A PAW is a hardened and locked-down workstation which is designed to help safeguard sensitive accounts and their tasks.

Using PAW is a first step toward improving security posture. PAWs can help protect privileged accounts and help reduce the risk of credential theft, lateral movement, and elevation of privileges.

The implementation of PAW should be performed together with other mitigations, such as limiting the number of highly privileged administrative accounts in on-premises IT systems and cloud services, and overall service hardening, which can help a company defend against credential theft attacks.

The purpose of this SOW is to provide CUSTOMER NAME REMOVED with a proposal for Microsoft’s Active Directory Hardening (ADH) and PAW offerings for the **ONO Active Directory** environment from Microsoft Services.

The project explained within this SOW utilizes Microsoft’s unique expertise in Active Directory and cybersecurity, and includes training workshops, discovery and analysis activities, and collaborative assistance to prioritize and strengthen CUSTOMER NAME REMOVED’s **ONO** Active Directory administrative environment.

This SOW details the services Microsoft will provide CUSTOMER NAME REMOVED in meeting the objectives for CUSTOMER NAME REMOVED’s **ONO** Active Directory Hardening and PAW initiatives.

# Project objectives and scope

The scope of this project is to assist CUSTOMER NAME REMOVED with discovering existing privileged access within their production **ONO** Active Directory Domain Services (AD DS) environment which will be documented within an exposure report document. This information will provide context for establishing a transition plan so CUSTOMER NAME REMOVED may transition into Microsoft’s recommended model for administering Active Directory. This is referred to as “Microsoft’s Reference Architecture for Active Directory Administration”.

Microsoft’s Reference Architecture for Active Directory Administration focuses on a tiered model for Active Directory administration. The tiered model for Active Directory administration is as follows:

* Tier 0 – In an enterprise environment, Tier 0 includes all administrators in control of the Active Directory forest, domains, and domain controllers and systems which operate or manage Tier 0 resources (i.e. monitoring, A/V, etc.) In this project, we will focus on the administrative user objects contained within the following Active Directory groups which have the most control over Tier 0 resources; Enterprise Admins, Domain Admins, Schema Admin, BUILTIN\Administrators, Account Operators, Backup Operators, Print Operators, Server Operators, Group Policy Creators Owners, and Cryptographic Operators.
* Tier 1 – In an enterprise environment, Tier 1 includes all administrators who are in control of multiple server operating systems, enterprise application administrators, and administrators of cloud services. These are not in scope for this project.
* Tier 2 – In an enterprise environment, Tier 2 includes administrative roles that have administrative rights to provide user, computer, and device support. These are not in scope for this project.

Given Tier 0 focuses on credentials that when compromised may provide an attacker highly privileged access to any resource secured by Active Directory, our focus will be to assist CUSTOMER NAME REMOVED with moving into the recommended model for Active Directory Administration.

In addition, the engagement is also to implement PAWs with applications for the following administrative tasks, which are based on Microsoft-recommended practices, architectures, accumulated field experience, and Customer requirements:

* Active Directory Domain Services (AD DS) management

PAW leverages the newest and most advanced security features in Windows 10 Enterprise, including:

* Unified Extensible Firmware Interface (EFI) Secure Boot
* Windows BitLocker Drive Encryption
* Windows Defender Antivirus
* Windows Defender Credential Guard
* Windows Defender Exploit Guard
* Windows Defender Firewall
* Microsoft AppLocker application whitelisting
* Integration with Azure Log Analytics

The default PAW image includes a number of common administrative tools, including:

* Microsoft Remote Server Administration Tools (RSAT)
* Windows PowerShell
* Microsoft Azure PowerShell module for ARM (AzureRM)

In addition, CUSTOMER NAME REMOVED wants Microsoft to review the **ONO** Active Directory environment from Security perspective and provide the recommendations for the transition to recommended security practices by Microsoft. As a timeboxed efforts, Microsoft will analyze and understand the current **ONO**’s Active Directory environment and will highlight the impact that would result in implementing the Active Directory Hardening policies in ONO Active Directory environment.

## Objectives

The objective of this project is to help CUSTOMER NAME REMOVED improve the security posture of their production **ONO** Active Directory Forest administrative environment by:

* Providing training workshops to share Microsoft recommended practices for administering high-value Active Directory assets.
* Discover, analyze and share CUSTOMER NAME REMOVED’s existing security exposure for high-value Active Directory assets in **ONO** environment.
* Facilitate, plan and prepare CUSTOMER NAME REMOVED for deploying a recommended Active Directory administration model in **ONO** environment.
* Assist CUSTOMER NAME REMOVED with reducing the number of highly privileged Active Directory administrative accounts by implementing, and moving into, a recommended Active Directory administration model in **ONO** environment.
* Assist CUSTOMER NAME REMOVED with deploying Privileged Access Workstation for Active Directory access and management in **ONO** environment.
* Assist CUSTOMER NAME REMOVED by highlighting the impact that would arise due to applying Active Directory hardening policies in **ONO** Active Directory environment.

## Areas in scope

### General project scope

To deliver the Active Directory Hardening solution for CUSTOMER NAME REMOVED, Microsoft will provide the following services:

### Active Directory Hardening

| Area | Description | Assumptions |
| --- | --- | --- |
| Tier 0 exposure analysis | Discover and analyze Tier 0 privileged credentials within 1 production AD DS domain  Discover and analyze privileged credential exposure on member servers located within the in-scope AD DS domain. Specifically:   * + Service accounts running with elevated privileges   + Elevated privileges within the local administrator group | CUSTOMER NAME REMOVED completes all appropriate change management processes to deploy the data collection component of the analysis tools.  CUSTOMER NAME REMOVED deploys the data collection component of the analysis tools to all appropriate systems (Domain Controllers and Servers) within their environment required to meet the scope of this engagement. |
| Tier 0 transition planning workshops | Conduct 11 transition planning workshops focused on:   * + Group Policy Settings Review and Planning (Default domain and Default domain controllers GPO’s); up to 2 hours   + Transitioning Enterprise Admins, Domain Admins, Schema Admins and Administrators to recommended AD DS admin model groups; up to 8 hours   + Transitioning Group Policy Creator Owners group to recommended AD DS admin model groups; up to 2 hours   + Transitioning Server Operators to recommended AD DS admin model groups; up to 2 hours   + Transitioning Account Operators to recommended AD DS admin model groups; up to 1 hour   + Transitioning Backup Operators to recommended AD DS admin model groups; up to 1 hour   + Transitioning Cryptographic Operators to recommended AD DS admin model groups; up to 1 hour   + Transitioning Virtualization Admins to recommended AD DS admin model groups; up to 1 hour   + Splitting accounts that currently have privileges to multiple tiers; up to 4 hours   + Plan for implementing a group of critical machines that will be used by Tier 0 users; up to 2 hours   + Plan for blocking Tier 0 users from navigating to the internet (Proxy block); up to 2 hours | The Tier 0 Transition Plan document contains the results of the Tier 0 Transition Planning workshops. This document will be used to move users into their new Active Directory administrative group once the recommended Tier 0 configuration is deployed. |
| Implement recommended and preconfigured AD DS administrative model | Deploy recommended AD DS administration model to 1 production AD DS domain including:   * + Organization unit (OU) structure including a new, “Computer Quarantine” OU.   + Group policy objects (GPO’s) with baseline security recommendations   + Administrative groups and associated AD DS delegations   Link and enable new default domain, default domain controllers and computer quarantine GPO’s  Transition and validate AD DS user objects out of default administrative groups into appropriate new tiered model group – up to 30 hours.  Provide post deployment operational assistance for up to 16 hours. | Microsoft will support CUSTOMER NAME REMOVED during the process of implementing the recommended and preconfigured AD DS administrative model into the production AD DS environment |

### Privileged Access Workstation

| Area | Description | Assumptions |
| --- | --- | --- |
| PAW kickoff and solution workshop | Microsoft will lead a one (1) day workshop during which the team kicks off the project, documents specific customer environment information and agree on the major design decisions with the Customer. | The vision and scope of the project will be documented as part of the architecture and design document. |
| PAW reference architecture | Microsoft will use the PAW reference architecture. | PAW reference architecture can be deployed in the Customer environment as is, without modification. |
| PAW administrative workstation image | Configure a single workstation image for one (1) hardware model or type  One administrative workstation image for Windows 10 Enterprise will be prepared with the Microsoft Deployment Toolkit (MDT).  This image is designed for one (1) specific administrative application.  This is time-boxed to three (3) days. |  |
| Administrative workstation deployment | Deploy up to five (5) PAWs. | The Customer will have the workstation hardware ready before the start of the project. |
| AD DS | Microsoft will help the Customer deploy organizational units (OUs) and group policy objects (GPOs) and grant permissions for the PAW images in production AD DS (one (1) domain) based on the predefined Microsoft PAW reference architecture. | PAW reference architecture can be deployed in the Customer environment as-is, without modification. |
| Monitoring | PAW integration with Azure Log Analytics. | The Customer has Azure subscription and the Log Analytics workspace ready before the project starts. |
| System testing assistance | PAW solution item testing assistance rendered to Customer (applies to items within the nonproduction build environment)  System testing focuses on the functionality meeting the design.  This is time-boxed to two (2) days. | Testing assistance is constrained to the time allocated during this project. |
| Operational guidance | A document containing recommended operational guidance and practices which can be used to maintain the security infrastructure and systems within the PAW. This document will include practices and procedures which define service ownership functions and roles. |  |
| One deployment | PAWs will be deployed in a physically secure room and connected to the simulated production AD DS.  After testing is complete, the solution will be disconnected from the simulated AD DS, moved to the datacenter, and connected to the production AD DS. | The physically secure room that contains the server hardware will be ready before the project starts. |

| Area | Description | Assumptions |
| --- | --- | --- |
| Deployment assistance – additional workstations | Microsoft will help customer deploy up to five (5) additional PAWs.  The activity is time-boxed to two (2) days. | All PAWs will be of the same hardware model/type. |
| Deployment assistance – additional hardware image | Microsoft will create one (1) additional hardware image to support deployment of PAW to one (1) additional hardware model or type.  The activity is time-boxed to three (3) days. | Hardware and hardware drivers will be available before the work starts. |
| Deployment assistance – additional application | Microsoft will help the Customer add one (1) additional application or system to be managed by PAWs. The following activities are in scope:  Management tools for one (1) additional application or system will be added to the MDT and deployed to PAWs  Appropriate AD DS security groups are updated to support management of this additional application/system  AppLocker rules are updated to include new management tools  The activity is time-boxed to two (2) days. | The Customer will provide management tools required to manage application/system before the work starts.  No network changes need to be made to manage this application/system from a PAW. |
| Deployment assistance – additional Active Directory Domain Services Domain | Microsoft will assist the Customer with the modification of one (1) additional AD DS domain | The additional domain which is selected is in the same AD DS forest as the original domain in the core component. |

### Time-boxed efforts

| Area | Description | Assumptions |
| --- | --- | --- |
| Kickoff and workshops | Analyze and understand the current **ONO**’s production Active Directory environment and highlight the impact that would result in implementing the Active Directory Hardening policies that environment. | The applications and services currently hosted in **ONO**’s production Active Directory environment are documented for Authentication and Security perspective.  Details about the applications and services will be available and provided during the workshops and information gathering sessions. |

### Software products and technologies

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

**Important note:** unless otherwise agreed to in the Work Order, the Customer 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 which accompanies the software (Microsoft or non-Microsoft) which is listed in this SOW or the Work Order and is included within the test and development environments. The Customer can read these terms by clicking the **About** box in the toolbar ribbon for the specific product at [www.microsoft.com](http://www.microsoft.com) or by requesting a copy from the Microsoft Project Manager.

Unless otherwise agreed to in writing in the Work Order, the Customer 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 which can be used to build an MDT server or provide a known good build ISO image.

| Product and technology item | Version | Ready by |
| --- | --- | --- |
| Windows Server | 2016 or newer | Start of the project |
| Windows | 10 Enterprise x64 | Start of the project |

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.

| Product and technology item | Ready by |
| --- | --- |
| Microsoft BGInfo (from the Sysinternals Suite) | Scripted download |
| Microsoft Assessment and Deployment Kit (ADK) | Scripted download |
| Windows Management Framework | Scripted download |
| Microsoft Report Viewer | Scripted download |
| Microsoft Deployment Toolkit (MDT) | Scripted download |
| Microsoft .NET Framework | Scripted download |
| Microsoft Message Analyzer | Scripted download |
| RSAT for Windows | Scripted download |
| Microsoft LAPS | 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 |
| Administrative templates for Windows 10 | Scripted download |
| Gemalto smart card MiniDriver | Scripted download |
| Microsoft RDC Manager (RDCMan) | Scripted download |
| Microsoft SQL Server Tools | Scripted download |

### System integration

The following system integration is in scope for the project.

| Integration | Description of scope | Responsibility | | Ready by |
| --- | --- | --- | --- | --- |
| Simulated AD DS | The PAW deployment will be tested in the simulated production AD DS. A virtual machine with a domain controller is sufficient. | Customer | Start of the project | |
| Production AD DS (**ONO**) | AD DS membership - the PAWs will be joined to the production domain.  AD DS configuration - OUs, GPOs, and delegated permissions will be added to the production AD DS service. | Customer | Start of the project | |

### Environments

The following environments will be required to deliver the project. For the following environments, Customer will be responsible for allocating and setting up the base hardware, network hardware, and network connectivity, and will provide the required software.

### Active Directory Hardening

| Environment | Location | Responsibility | Ready by |
| --- | --- | --- | --- |
| Production Active Directory Forest (**ONO**) | Customer | Customer | Start of engagement |
| Production Active Directory Domain (**ONO**) | Customer | Customer | Start of engagement |

### Privileged Access Workstation

| Environment | Location | Responsibility | Ready by |
| --- | --- | --- | --- |
| Build | Dedicated secure room | Customer | Before the Build phase of this project |
| Production | Secure datacenter | Customer | Before the Deploy phase of this project |
| Log Analytics Workspace | Azure subscription | Customer | Before the Build phase of this project |

### 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.

### Active Directory Hardening

| Test type (environment) | Description | Responsibility | | |
| --- | --- | --- | --- | --- |
| Has responsibility  for testing? | Provides data or test cases | Provides guidance and support |
| System testing | System Testing focuses on system functionality meeting the design. Test cases are based upon the Test Plan document and include functionality tests of the new Tier 0 administrative model and the validation of the pre-configured permissions against the new structure. The Microsoft effort to support this testing is limited to 4 hours. | Customer | Customer | Microsoft |

### Privilege Access Workstation

| Test type (environment) | Description | Responsibility | | |
| --- | --- | --- | --- | --- |
| Has responsibility  for testing? | Provides data or test cases | Provides guidance and support |
| System testing (build) | System testing focuses on the functionality meeting the design. The testing duration is time-boxed to two (2) days. Test cases are based on the test guide. | Microsoft | Customer | Microsoft |
| Customer acceptance testing (production) | This consists of testing administrator functionality of key real-world scenarios. Test cases are based on the operations guide. Testing duration is time-boxed to one (1) day. | Customer | 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 for ADH? | Remediation in scope for PAW? |
| --- | --- | --- | --- |
| 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 4 hours | 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. | No; the problem will be logged. Remediation will be performed through an agreed-upon change request only. | 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. | 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. | No; the problem will be logged. Remediation will be performed through an agreed-upon change request only. |

**Note:** Product bug fixes and design change requests are not in scope. Product-related issues must be addressed separately through Premier support.

### Training

The following training will be delivered during the project.

| Type | Description (including location) | Quantity and duration |
| --- | --- | --- |
| Instructor-led | **Description:** Microsoft secure modern enterprise foundations  **Location:** Delivered on site at Customer facility in [enter customer location]  **Materials:** PowerPoint presentation  **Project phase:** Envision | **Number of sessions:** 1 **Duration:** 1 hour  **Number of participants:** up to 30 |
| Instructor-led | **Description:** Understanding credential theft  **Location:** Delivered on site at Customer facility in [enter customer location]  **Materials:** PowerPoint presentation  **Project phase:** Envision | **Number of sessions:** 1  **Duration:** 2 hours  **Number of participants:** up to 30 |
| Instructor-led | **Description:** Overview of Microsoft’s Tiered Administration Model  **Location:** Delivered on site at Customer facility in [enter customer location]  **Materials:** PowerPoint presentation  **Project phase:** Envision | **Number of sessions:** 1 **Duration:** 3 hours  **Number of participants:** up to 30 |
| Instructor-led | **Description:** Overview of the Tier 0 Configuration Model – Administration and Delegation Model Overview  **Location:** Delivered on site at Customer facility in [enter customer location]  **Materials:** PowerPoint presentation  **Project phase:** Envision | **Number of sessions:** 1 **Duration:** 4 hours  **Number of participants:** up to 30 |
| Instructor-led | **Description:** Overview of the Design and Implement Active Directory Configuration Model – Secure Group Policies Overview  **Location:** Delivered on site at Customer facility in [enter customer location]  **Materials:** PowerPoint presentation  **Project phase:** Envision | **Number of sessions:** 1 **Duration:** 2 hours  **Number of participants:** up to 30 |
| Instructor-led | **Description:** Active Directory Hardening Discovery Tools Overview Workshop  **Location:** Delivered on site at Customer facility in [enter customer location]  **Materials:** PowerPoint presentation  **Project phase:** Envision | **Number of sessions:** 1 **Duration:** 2 hours  **Number of participants:** up to 30 |

In addition, Informal knowledge transfer will be provided throughout the project. Informal knowledge transfer is defined as information shared when Customer staff members work side by side with Microsoft staff. This could include whiteboard discussions, email threads, conference calls, and facilitated meetings regarding technical topics. Transfer activities are secondary to completing deliverables and maintaining the project schedule. No deliverables or meeting summaries will be provided for the following sessions or activities.

## 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 tables.

### Active Directory Hardening

| 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. |
| Organizational change management | Designing—or redesigning—the Customer’s functional organization is not included. |
| Physical server setup, management, and maintenance | Physical server setup, installation, and networking interfaces or evaluation of new hardware or software.  Ongoing production operational support. |
| Role definition | Custom definition of roles and the creation of new accounts or roles (such as groups). This project will utilize a predetermined administrative model as provided by recommended AD DS administration model. |
| Operations | Operational assessments, improvement plans, or designs for new operational processes or procedures beyond the documented guidance as delivered within the operations guide. |
| Current production environment | Any changes to the current environment that are not related to the defined scope of this project. |
| Test Environment | Building of a test environment.  Duplication of customer’s existing Windows corporate domain environment within a test lab or the creation of test domains to simulate production domains. |
| Support | Post-deployment support. Additional support can be purchased separately. |

### Privileged Access Workstation

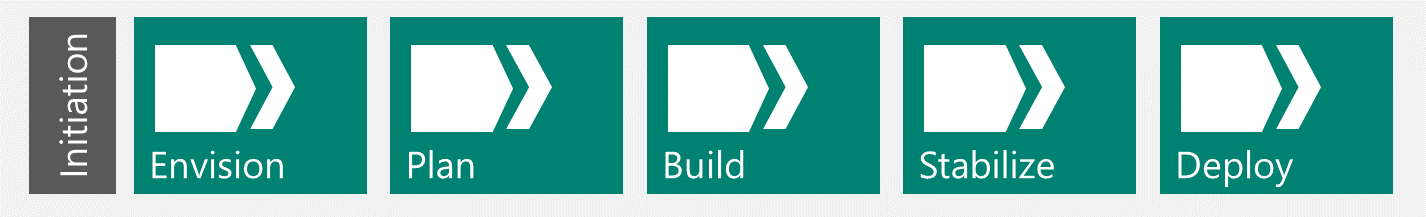
| Area | Description | |
| --- | --- | --- |
| Physical server setup, management, and maintenance | Physical server setup, installation, and networking interfaces or evaluation of new hardware or software.  Ongoing production operational support. |
| PAW enterprise functions | Windows 10 Enterprise functionalities such as Internet Protocol Security (IPsec), smart card logon, Windows Defender Device Guard, and Windows Defender Application Guard. |
| PAW as a virtual machine | Deploying one (1) or multiple PAWs and productivity workstation as virtual machines (unless added as an option to this engagement). | |
| Discovery | Discovery and categorization of administrative tasks and applications. |
| Role definition | Custom definition of roles and the creation of new accounts or roles (such as groups). |
| Log Analytics (OMS) configuration | Configuration of Log Analytics dashboards, reports, or related items beyond onboarding the PAWs. |
| Operations | Operational assessments, improvement plans, or designs for new operational processes or procedures beyond the documented guidance as delivered within the operations guide. |
| Current production environment | Changes to the current environment to resolve issues which are not related to the defined scope of this project. |
| Monitoring services | Setup or configuration of monitoring, auditing, or alerting services to monitor the health of the environment beyond any items which are explicitly included in the scope. |
| Migration or consolidation | Migration, consolidation, or rationalization of AD DS objects, including users, groups, workstations, servers, applications, or group policies—this includes logon scripts and data migration. |
| Lab or test environment | Building of a lab environment.  Deploying of PAWs and deployment environment in the lab environment  Running of test cases. |
| Support | Post-deployment support. Additional support can be purchased separately. |
| General production domain hardening | Securing of AD DS components other than privileged user accounts. (General hardening of servers such as domain controllers is out of scope.) |
| Remote access for PAWs | Integration of the Customer’s virtual private network (VPN) solution. |

# Project approach, timeline, and deliverable acceptance

## Approach

The project will be structured following the Microsoft solution delivery methodology across five distinct phases; Envision, Plan, Build, Stabilize, and Deploy. 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.  Discuss change management for ADH tool deployment  Discuss change management for transitioning users into new groups  Schedule of kick-off and training workshops  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 prerequisites 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. |

### Envision

### Active Directory Hardening

During the Envision phase, the team will identify and define the requirements for the overall solution, gain an understanding of the environment, design a high-level solution strategy that meets the requirements of the solution, define the roles and responsibilities of the project team, and create a Vision and Scope Document identifying what will be accomplished.

Additionally, Microsoft will provide CUSTOMER NAME REMOVED with a series of training workshops to help prepare CUSTOMER NAME REMOVED for reviewing the Tier 0 Exposure report, planning administrative user transitions and completing Tier 0 administrative user object movement into the recommended Tier 0 configuration model.

|  | | |
| --- | --- | --- |
| Category | Description | |
| **Microsoft activities** The activities to be performed by Microsoft | Conduct project kick-off meeting  Lead 1 requirements gathering workshops lasting no more than 1 hour in total  Develop vision and scope document  Conduct training as defined in the Training section of this SOW |
| **Customer activities** The activities to be performed by the Customer | Participate in project kick-off meeting and workshops  Participate in requirement gathering workshops  Provide requested information and documentation  Review, accept and approve the vision and scope document  Identify appropriate personnel to attend training workshops  Attend training workshops |

#### Deliverables

| Name | Description | Acceptance required? | Responsibility |
| --- | --- | --- | --- |
| Vision/Scope document | The Vision Scope documents the agreement on the desired solution and overall project direction between the team and the customer. | Yes | Microsoft |

### Privileged Access Workstation

During the Envision phase, the team (Microsoft and the Customer) will reach agreement on a shared vision for the project and the specific scope which will be required to make that vision a reality.

The team will kick the project off by coordinating a series of envisioning working sessions with key stakeholders to verify requirements and gather data about the existing environment. Microsoft will then create a project vision and scope section in the architecture and design document which will serve as the project’s charter, align expectations among the project team and stakeholders, and document the requirements.

|  | | |
| --- | --- | --- |
| Category | Description | |
| **Microsoft activities** The activities to be performed by Microsoft | Conduct the kickoff meeting  The design sessions will cover conceptual PAW reference architecture.  Agree on the vision and scope and document them in the Technical Guide deliverable.  Create a project plan with key milestones. This is a preliminary, high-level project plan with key milestones. |
| **Customer activities** The activities to be performed by the Customer | Gather information which might be requested during the Envision phase workshop.  Review the vision and scope document deliverable and participate in its approval process.  Make decisions when architectural options are presented.  Engage operations and service owners to help raise awareness about systems to be implemented. |
| **Key assumptions** | Customer service owners and architects have been identified and will attend and participate in the PAW envisioning workshop. |

#### Deliverables

| Name | Description | Responsibility |
| --- | --- | --- |
| Draft project plan | A preliminary version of the project plan with key milestones. | Microsoft |

### Plan

### Active Directory Hardening

During the Plan phase, Microsoft will work with CUSTOMER NAME REMOVED to use the analysis tools to begin gathering information about Tier 0 resources. Using this information, Microsoft will lead and conduct sessions to review data that has been collected with CUSTOMER NAME REMOVED and will produce a Tier 0 Exposure Report highlighting areas CUSTOMER NAME REMOVED should consider further investigating.

The activities within this phase are to prepare CUSTOMER NAME REMOVED for the deployment of the new Tier 0 administration model and the transition of existing administrative accounts into this model.

|  | |
| --- | --- |
| Category | Description |
| **Microsoft activities** The activities to be performed by Microsoft | Assist with ADH tools deployment; up to 12 hours  Assist with the remediation of data collection issues; up to 4 hours  Process collected data  Perform Tier 0 analysis and information preparation  Create the Tier 0 exposure report  Conduct Tier 0 exposure review meeting with Customer  Conduct Tier 0 transition planning workshops with Customer  Document Tier 0 Transition Plan  Conduct Tier 0 Transition Plan review meeting with Customer |
| **Customer activities** The activities to be performed by the Customer | Provide requested information and documentation  Participate in Tier 0 transition planning workshops  Review, acceptance and approval of the Tier 0 Exposure Report  Review, acceptance and approval of the Tier 0 Transition Plan document |

#### Deliverables

| Name | Description | Acceptance required? | Responsibility |
| --- | --- | --- | --- |
| Tier 0 Exposure Report | A set of files containing information collected using the ADH tools during the discovery and analysis phase. | Yes | Microsoft |
| Tier 0 Transition Plan | Microsoft Word document describing the results of the Tier 0 Transition Planning workshops. This document will be used to move users into their new Active Directory administrative group once the recommended Tier 0 configuration is deployed. | Yes | Microsoft |

### Privileged Access Workstation

During the Plan phase, Microsoft will work with the customer to develop and meet the technical and functional requirements in the logical and physical designs, and to define and describe the environment end state. Microsoft will record the PAW design in the technical guide document. The project plan will be updated to reflect the detailed timeline for the Build, Stabilize, and Deploy phases.

|  | |
| --- | --- |
| Category | Description |
| **Microsoft activities** The activities to be performed by Microsoft | * Update the technical guide document with Customer environment information. * Review the technical guide with the Customer. * Review the project plan with the Customer |
| **Customer activities** The activities to be performed by the Customer | Gather the information requested during the planning design sessions.  Review the technical guide document and participate in its approval  Customer subject matter experts (SMEs) will participate in the design sessions and make decisions when architectural options are presented. |
| **Key assumptions** | PAW reference architecture can be deployed in the customer environment as-is, without modification. |

#### Deliverables

| Name | Description | Responsibility |
| --- | --- | --- |
| Technical guide | A document with PAW reference architecture including description of the solution and its components, logical solution, and its physical implementation. | Microsoft |
| Final project plan | Final version of the project plan with key milestones. | Microsoft |

### Build

### Active Directory Hardening

The Build phase focuses on the deployment of the recommended Active Directory administration model into CUSTOMER NAME REMOVED’s production Active Directory using automation scripts provided by Microsoft. This includes the deployment of:

* Group Policy Objects – the deployment of the new group policy objects does not include linking them to an organizational unit (OU). This process will occur during the deploy phase.
* Tier 0 Organizational Units (OU’s) – these will be newly created OU’s that will be placed into CUSTOMER NAME REMOVED’s production Active Directory environment. Movement of objects into the new OU structure will occur during the Deploy phase.
* Tier 0 Administrative Groups – the deployment of the recommended Tier 0 administrative groups. The movement of users into these groups will follow information documented in the Tier 0 Transition Plan and will occur during the deploy phase.
* Tier 0 Administrative Delegations – using the new Tier 0 Administrative groups and OU’s, delegations will be completed applying recommended permissions to both the Tier 0 administrative groups and the appropriate Tier 0 OU.

While this configuration will be deployed during this phase, activation of the configuration does not occur until the Deploy phase after CUSTOMER NAME REMOVED’s with the assistance of Microsoft, tests and validates the configuration during the Stabilize phase.

|  | | |
| --- | --- | --- |
| Category | Description | |
| **Microsoft activities** The activities to be performed by Microsoft | Microsoft will assist Customer with implementing the recommended AD DS administration model into production AD DS domain |
| **Customer activities** The activities to be performed by the Customer | Implement the recommended AD DS administration model into the production AD DS environment |

### Privilege Access Workstation

During the Build phase, the team builds the PAW solution components in a physically secure room. The goal of this phase is to help the team connect the PAW deployment to the simulated production Active Directory environment.

|  | | |
| --- | --- | --- |
| Category | Description | |
| **Microsoft activities** The activities to be performed by Microsoft | * Build the MDT server used to deploy PAWs. * Deploy one (1) PAW image on up to five (5) production workstations which are attached to a simulated production AD DS. * Update test guide document. * Review test guide document with the Customer. * Update implementation guide document. * Review implementation guide document with the Customer. |
| **Customer activities** The activities to be performed by the Customer | Participate in Build phase activities.  Participate in review activities. |
| **Key assumptions** | Customer SMEs will participate in the development sessions.  The Costumer will provide appropriate secure room facilities, including hardware and software.  The Customer will provide Customer-specific test cases. |

#### Deliverables

| Name | Description | Responsibility |
| --- | --- | --- |
| Implementation guide document | A document with configuration information and step-by-step instructions used to build the end state described in the architecture and design document | Microsoft |
| Test guide | A document with test cases that documents testing procedures. | Microsoft |

### Stabilize

### Active Directory Hardening

During the Stabilize phase, testing of the recommended Tier 0 configuration will be completed. The intention of this phase is to test, and validate, the recommended Tier 0 configuration functions as designed and that test users, who have been granted access in the new Tier 0 configuration, have appropriate permissions as designed.

|  | | |
| --- | --- | --- |
| Category | Description | |
| **Microsoft activities** The activities to be performed by Microsoft | Assist with System testing  Update test plan with testing results  Lead a meeting to review test results with Customer |
| **Customer activities** The activities to be performed by the Customer | Perform System testing  Attend the test results review meeting   * Review, acceptance and approval of the test plan document |

#### Deliverables

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Description | Acceptance required? | Responsibility |
| Test Plan | A Microsoft Word document that includes test results and notes about implementing the defined test cases in the document. | Yes | Microsoft |

### Privileged Access Workstation

During the Stabilize phase, the combined Microsoft and Customer team will implement the test guide in the physically secure room, document the results for the test cases, and validate the Build process. Microsoft will record the recommended operational practices and procedures in the operations guide.

The Stabilize phase is complete when the solution has been verified through the implementation of the test guide by the Customer.

|  | | |
| --- | --- | --- |
| Category | Description | |
| **Microsoft activities** The activities to be performed by Microsoft | * Conduct functional testing using the test cases from the test guide. This activity is time-boxed to two (2) days.   Update the operations guide document.  Review the operations guide with the Customer. |
| **Customer activities** The activities to be performed by the Customer | Engage designated test users.  Perform system testing based on the test guide.  Review the implementation guide and participate in its approval.  Review the operations guide and participate in its approval. |
| **Key assumptions** | Customer SMEs and test users are ready to participate in the testing activities.  A post-deployment support process will be established by the Customer prior to commencement of the Deploy phase. |

#### Deliverables

| Name | Description | Responsibility |
| --- | --- | --- |
| Operations guide document | A document with operational guidance for the systems and components which are described in the architecture and design document. | Microsoft |

### Deploy

### Active Directory Hardening

The Deploy phase consists of transitioning existing privileged accounts to the new Tier 0 configuration.

The transition of existing resources to the new Tier 0 configuration consists of the following:

* Enablement and linking of Group Policy Objects to the domain and domain controllers OU’s
* Moving users out of the default AD DS administrative groups into the appropriate group within the new recommended AD DS administrative model following the Tier 0 Transition Plan document.

|  | | |
| --- | --- | --- |
| Category | Description | |
| **Microsoft activities** The activities to be performed by Microsoft | Microsoft will assist with the following activities:   * Link and enable new default domain, default domain controllers and computer quarantine GPO’s * Transition and validate AD DS user objects out of default administrative groups into appropriate new tiered model group. * Provide operational assistance as defined by the scope of this project * Conduct project closeout |
| **Customer activities** The activities to be performed by the Customer | * Link and enable new default domain, default domain controllers and computer quarantine GPO’s * Transition and validate AD DS user objects out of default administrative groups into appropriate new tiered model group. * Participate in project closeout |

### Privileged Access Workstation

The Deploy phase begins with the implementation of the PAW solution for production use. The PAW deployment in the physically secure room will be disconnected from the simulated production Active Directory environment, and the PAWs will be moved to the datacenter and connected to the real production Active Directory environment.

The Customer will, based on the operations guide, validate the solution functionality in the production environment. Customer will have one (1) day to validate the functionality of the new administrative workstations within its organization.

After the validation tests are completed, the production rollout begins. First, customer administrators will use the solution to perform their daily work. During the rollout, these administrators will report problems which must be addressed and will work with Microsoft to troubleshoot and resolve these problems.

|  | | |
| --- | --- | --- |
| Category | Description | |
| **Microsoft activities** The activities to be performed by Microsoft | * Connect PAW to the production environment   + During PAW production implementation, Microsoft will assist as needed as the Customer puts the implementation guide into effect.   + Microsoft support activities are limited to the first five (5) PAWs in the Customer production forest. * Handover and close out the project. |
| **Customer activities** The activities to be performed by the Customer | Deploy the solution to production.  Provide direction to Microsoft resources during this project phase  Run Customer acceptance tests  Provide feedback on production use  Provide sign-off for project results. |
| **Key assumptions** | * The Customer will take responsibility for its change control processes (e.g. submitting all necessary change requests) * Affected organizations will identify the resources and groups which will be required for the Deploy phase. * The deployment process for one (1) production domain and up to five (5) PAWs will help the Customer continue and finalize integration of additional PAWs, if necessary. |

#### Deliverables

|  |  |  |
| --- | --- | --- |
| Name | Description | Responsibility |
| Up to five (5) production PAWs deployed | Up to five (5) production PAWs have been successfully deployed and tested. | 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.

### Active Directory Hardening

### Privileged Access Workstation

It is estimated that this engagement will be performed in approximately three (3) weeks and will include the phases and milestones noted.

### Time-boxed Efforts for Environment Analysis and Recommendations

This part of the engagement is time-boxed for the efforts will include the phases and milestones noted.

## 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.
* **Review and acceptance** of the solution or custom source code is based on completion and acceptance of UAT as described in the Testing and defect remediation section.

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 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 | 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

Microsoft will provide services defined in this SOW to the extent of the fees available and the period of performance 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 | * Part-time, 2–4 hours a week * Make key project decisions. * Serve as a point of escalation to support clearing project roadblocks. |
| Project manager | Full time  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 Technical lead | Full time throughout project  Serve as primary technical point of contact.  Take ownership of technical architecture and code deliverables. |
| AD DS SMEs | Full Time  Primary functional point of contact for the team who is responsible for administration of Active Directory and infrastructure  Is responsible for running data collection utilities and making changes to Active Directory  Attends and provides input into the Analysis phase workshops |
| Test Lead | Full time during Stabilize phase  Part time during Deploy phase  Responsible for test plans and guides and coordinating testing resources for acceptance tests |
| Technical Team Lead | Expected allocation of 16-40 hours a week. Available for and responsive to *ad hoc* technical, operational, or process questions.  Serve as primary technical point of contact.  Take ownership of technical architecture and code deliverables. |
| Technical architect | Expected allocation of 4-12 hours a week. Available for and responsive to *ad hoc* technical, operational, or process questions. Full-time availability with expected allocation of 4–12 hours a week.  Responsible for quality assurance (QA) and escalation of technical decisions and issues. |
| Test and QA lead | Expected allocation of 4-12 hours a week. Available for and responsive to *ad hoc* technical, operational, or process questions.  Take responsibility for test plans and guides and coordinating the acceptance testing of resources. |
| Security SMEs | Expected allocation of 4-12 hours a week. Available for and responsive to *ad hoc* technical, operational, or process questions.  Provides technical representation for cybersecurity as it relates to the security architecture to be implemented. |
| Other SMEs | Expected allocation of 4-12 hours a week. Available for and responsive to *ad hoc* technical, operational, or process questions.  Provide technical representation related to systems and services, including network, DNS, PKI, and smart card integration. |

#### Microsoft

| Role | Responsibilities | |
| --- | --- | --- |
| Microsoft delivery manager | * Part time * 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 | Part time  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 Consultant | * Full time * Deliver workshops and sessions * Responsible for development of technical deliverables |
| Microsoft Architect | Part time  Provide technical design leadership and oversight  Provide guidance based on Microsoft-recommended practices. |

# 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.
* Provide a meeting room to facilitate training and planning workshops.
  + This consists of a suitable room which is equipped with a projector that accommodates participants for both training and planning workshop sessions.
  + A dedicated physically secure room with desks, chairs, and network access which the project team can use for the duration of the project (should be ready before the project kick off):
    - A secure storage location for documentation and DVDs which will be used on the project (this place would preferably be in the secure room)
    - At least one (1) DVD-writing device (external or built-in) in the project room
    - A stack of 20 writable single-layer DVDs
    - Paper shredder, ideally also capable of shredding DVD media
    - A separate dedicated Internet connection for the secure room with at least 16 megabits a second downstream which can be used for the known-good media build process
    - A centralized project repository for project information and documentation
* Provide the following:
  + At least one physical server used for the build and production environment capable of running virtual machines on Hyper-V.
  + Simulated production AD DS. One virtual machine with domain controller function is suitable.
  + Five (5) unused and unopened laptops or desktops which will be used as production PAWs
  + Test data and personnel which will be needed to conduct solution system testing, including interfaces.
  + Test data and personnel which will be needed to conduct customer acceptance testing of the solution, including interfaces.
  + Log Analytics Contributor rights (Azure RBAC) on a Log Analytics workspace in one of the customer’s Azure subscriptions for the user who will add the monitoring solutions to the Azure Log Analytics workspace. The Log Analytics workspace stores the log data, which are used to monitor PAWs.
  + Log Analytics Reader rights (Azure RBAC) on a Log Analytics workspace in one of the customer’s Azure subscriptions for the users who need to view and search Azure Log Analytics monitoring data.
* 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.
* Other general responsibilities.
  + Customer will follow all appropriate change management processes and obtain approval in time for the deployment of the solution per this projects schedule
  + CUSTOMER NAME REMOVED is responsible to deploy the data collection component of the analysis tools to all appropriate systems (Domain Controllers and Servers) within their environment required to meet the scope of this engagement.
  + CUSTOMER NAME REMOVED is responsible for moving the users from their current group memberships into the destination group as defined by the Transition Plan workshop and documented within the Transition Plan document.

## 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 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.
* Technical Assumptions:
  + Managed Servers are Active Directory domain joined.
  + Only Windows Server operating systems in main or extended lifecycle support are in scope (Windows Server 2008 and above). Windows Server operating systems or versions under custom agreements will not be supported. Only systems with a supported version of the .NET framework installed are in scope.
  + Microsoft assumes that all machines have the default admin shares turned on.
  + Data collection is limited to systems that can be reached by collection tools. Network segmentation may result in suboptimal coverage of data collection.
* Documentation:
  + All document deliverables will be on Microsoft standard templates.