Statement of Work

Privileged Access Workstation

Prepared for

County of Dekalb

Prepared by

Microsoft Consulting Services

Date: March 25, 2021

Version: *1.1*

Table of contents

This Statement of Work ("SOW") and any exhibits, appendices, schedules, and attachments to it are made pursuant to Letter Agreement DORV212-333967-407188 (hereinafter referred to as "Work Order"), and describes the work to be performed ("Services") by Microsoft Corporation ("Microsoft," "us," "we," or "our") for County of Dekalb ("County of DeKalb," "Customer," "you," or "your") relating to your Privileged Access Workstation Project ("project").

This SOW and the associated Work Order expire thirty (30) days after their publication date (date Microsoft submits to Customer) unless signed by both parties or formally extended in writing by Microsoft.

Introduction

County of Dekalb, 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 that they are seeking. These modern cyber attackers 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.

The Microsoft Consulting 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 that is designed to help safeguard sensitive accounts and their tasks.

Using PAW is a first step toward improving security posture. PAW 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.

County of Dekalb has requested Microsoft assistance with the implementation of PAW; that assistance will be delivered through Microsoft Consulting Services.

1. Project objectives and scope

1.1. Objectives

The objective of this project is to modernize County of Dekalb 's security infrastructure as it relates to secure privileged access for on premises and cloud environments. The project will achieve this through the implementation of Microsoft-recommended controls focused on securing the Azure Active Directory (Azure AD) and Active Directory Domain Services (AD DS) accounts used for administration.

The project consists of the following areas:

Area	Objectives
PAW for cloud services management	• Design and implement a PAW for the secure management of Microsoft Azure and Office 365 services by privileged user roles. This PAW is used by Azure AD accounts with 'Tier 0' equivalent privilege, such as Global Administrators, Security Admin and Conditional Access Admin. • PAW will itself be configured and managed through cloud services to minimize security dependencies on the Customer's on-premises environment. • Implement Microsoft Defender for Endpoint for PAW devices. • Implement On-Premises Administration Reach-Back to securely reach back and administer On-Premises workloads • Implement an automated operating system (OS) deployment server based on the Microsoft Deployment Toolkit (MDT).

1.2. Areas in scope

This section outlines the work and activities required to accomplish the objectives set forth in this SOW.

1.2.1. General project scope

Microsoft will provide Services in support of the following scope.

1.2.1.1. PAW for cloud services management

Area	Description	Assumptions
PAW for cloud services management	• Deploy up to ten (10) PAW for cloud services management (PAW-CSM) devices on one (1) PAW-CSM hardware models including one (1) workload for one (1) PAW-CSM use cases. • Configure Microsoft Intune compliance policies for PAW devices. • Configure Microsoft Intune configuration policies to harden PAW devices. • Configure Azure Multi Factor Authentication ("MFA"), self-service password reset, and Azure AD Conditional Access policies to support PAW scenarios. • Configure Azure Active Directory Identity Protection to allow Conditional Access to use Identity Protection Sign-in Risk as part of Conditional Access policy rules. This provides a baseline configuration that helps protect the following privileged roles:	• Administrative and support applications include PowerShell modules for: Azure compute, Azure AD, MS Online, and Azure AD Privileged Identity Management. • The implementation and configuration of Azure Active Directory roles or Azure roles are limited to fit to the default duration of engagement.

Area	Description	Assumptions
	○ Global Administrator ○ Conditional Access Administrator ○ Intune Service Administrator ○ Privileged Role Administrator ○ Security Administrator - Configure Windows Update for Business policies. - Configure Intune [time-boxed to sixteen (16) hours of effort] to deliver identified administrative and support applications for PAW devices. - Configure the Windows Analytics workspace to be able to access device health, update readiness, and upgrade readiness dashboards. - Microsoft will assist the Customer with the configuration and deployment of a remote access solution to enable PAW-CSM devices to securely connect to and administer on-premises workloads leveraging Azure Bastion.	- Azure Bastion is available in Customer Azure region - Customer has secure deployment of the Azure environment, which includes at least one vNet with connectivity to their on-premises environment and can deploy virtual machines into this vNet
Microsoft Defender for Endpoint	- Lead one (1) workshop up to eight (8) hours with the objective to validate Microsoft Defender for Endpoint design decisions. - Enable Microsoft Defender for Endpoint on up to ten (10) supported Windows 10 PAW devices. - Lead 1 workshop of up to eight (8) hours with the objective to transfer knowledge about the operations of Microsoft Defender for Endpoint.	- The Customer will make it possible for endpoints to communicate directly with the Microsoft Defender for Endpoint service endpoint. - Windows devices will run in a version or build that supports Microsoft Defender for Endpoint.
Clean Source Deployment Process	Implement an automated operating system deployment server, based on MDT technology.	- Network Infrastructure is available. - A secure room is available.

1.2.2. Software products and technologies

The products and technology listed in the following table are required for project execution. The party responsible for obtaining the items is indicated.

Product and technology item	Version	Ready by
Microsoft 365 Or	E5, M365 E5, M365 E5 Security,	Build Phase

Product and technology item	Version	Ready by
Microsoft Enterprise Mobility and Security ("EMS") Microsoft Defender for Endpoint	Microsoft Defender for Endpoint SKUs	
Windows 10	1809 or higher	Start of the Remediate Phase
Azure subscription (or subscriptions)		Start of Enable phase
Windows Server (Refer to Section **Error! Reference source not found.**, **Error! Reference source not found.**)	2019	Start of the project

1.2.3. Environments

The following environments will be required to deliver the project.

Environment	Location	Responsibility	Ready by
Production	• Azure tenant and subscription for Azure services • Customer facility used for device deployment	Customer	Start of the project
Secure Room	Customer facility	Customer	Start of the project

1.2.4. Testing and defect remediation

Testing

The following testing is included in the scope of the project.

Test type (environment)	Description	Responsibility			
		Test execution	Provides data	Provides test cases	Provides guidance and support
PAW for cloud services management					
System testing (PAW in Production)	Test cases will be executed in the production environment to validate that the implemented solution is functioning as designed. This activity is time-boxed to eight (8) hours.	Microsoft	Microsoft	Microsoft	Customer
Validation testing	Test cases will be executed in the production environment to	Microsoft	Microsoft	Microsoft	Customer

Test type (environment)	Description	Responsibility			
		Test execution	Provides data	Provides test cases	Provides guidance and support
(Microsoft Defender for Endpoint in Production)	validate that the implemented solution is functioning as designed.				
System testing ("MDT")	System Testing will be based on test cases.	Microsoft	Microsoft	Microsoft	Customer

Defect remediation

If defects are identified during testing, the priority of the defect will be jointly agreed upon by the Customer and Microsoft based on the definitions below. Defects in each severity level will be remediated in priority order, where possible. Defects with the same severity may receive a higher priority and will be fixed first.

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

Priority	Description	Remediation in scope?
		change request only.

1.3. Areas out of scope

Any area not explicitly included in the Areas in Scope section will be considered out of scope for Microsoft during this project. Specific areas that are out of scope for this project, include the following.

Area	Description
Physical server setup, management, and maintenance	The following are out of scope: • Physical server setup, installation, and networking interfaces or evaluation of new hardware or software • Ongoing production operational support
Networking configuration and hardware token usage or management	Usage or management of Internet Protocol Security ("IPsec"), smart cards, or FIDO2 devices is out of scope.
PAW as a virtual machine	Deploying PAWs or productivity workstations as virtual machines is out of scope.
Discovery	Discovery or categorization of administrative tasks and applications is out of scope.
Admin Azure Active Directory tenant	Implementation of an Admin Azure Active Directory tenant to support credential isolation and management of the production hybrid identity forest
VPN integration	Integration of the Customer's VPN solution is out of scope.
Azure AD identity management	Changes to individual group objects to accommodate self-service management in Azure AD, including conversion of synchronized groups to cloud-based groups, is out of scope.
Azure MFA server and third-party providers	Deployment of the on-premises Azure MFA Server is outside the scope of this project, as is integration with a third-party multi-factor authentication provider.
Configuration and enablement of conditional access	• Design and implementation of conditional access through Active Directory Federation Services is out of scope. • Design and implementation of conditional access for Microsoft Exchange on premises is out of scope.

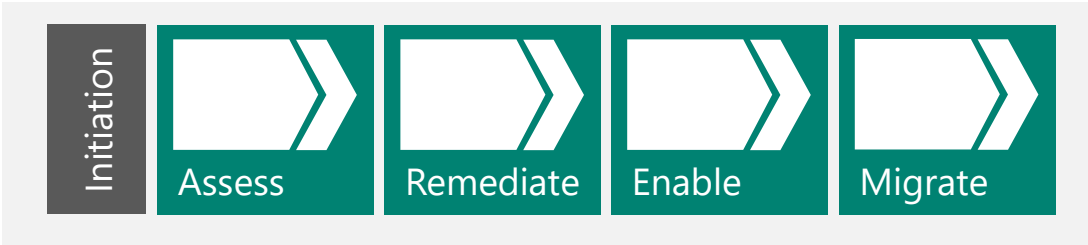| Area	Description
	• Design and implementation of conditional access for standard user (non-privileged roles) scenarios is out of scope.
Configuration and enablement of mobile device management foundation	• Design and implementation of Configuration Manager infrastructure is out of scope. • Configuring infrastructure components for email, Wi-Fi, and VPN are out of scope. • Integration with any on-premises service, solution, or product other than those specified in this document as in scope (such as Network Device Enrollment Services or Configuration Manager) is out of scope. • Migrating from third-party mobile device management is out of scope. • Management of computers with the Intune agent is out of scope. • Configuring Samsung Knox or kiosk mode is out of scope. • Assistance with the rollout of unsupported device platforms is out of scope. • Assistance with the enrollment in an environment that has not been implemented by Microsoft Consulting Services is out of scope. • Deployment of settings and configurations that are not supported by Intune or the device's operating system platform is out of scope. • Design and implementation of Intune polices for any scenarios other than PAW is out of scope.
Product licenses and subscriptions	Product licenses (Microsoft or non-Microsoft) and cloud service subscriptions are not included.
Break/fix support	Microsoft will not provide break/fix support for AD DS, Azure, Azure Active Directory, Office 365, Windows 10, applications, or systems used during this engagement.
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.
System integration	System integration and interfaces are not in scope for this project.
Training	Training outside of what is identified in the workshops listed in the Areas in scope section is out of scope.
Microsoft Defender for Endpoint	• Security Information and Event Management ("SIEM") integration. • Response and remediation of any threats that Microsoft Defender for Endpoint might detect in the duration of the engagement. • Assistance in engaging with a Microsoft Threat Expert through the Microsoft Defender Security Center portal.

Area	Description
	• Implement any remediation activities or security recommendations suggested by the Threat & Vulnerability Management dashboard. • The implementation of Attack Surface Reduction rules and policies. • Enablement of Microsoft Defender for Endpoint on Linux endpoints. • Enablement of Microsoft Defender for Endpoint on MacOS endpoints. • Enablement of Microsoft Defender for Endpoint on Windows 7, Windows 8.1 Windows Server 2012R2, and 2008R2 SP1 endpoints.
Use of Clean Source deployment process	• Usage and extension of the solution after engagement closure is at the Customer's own discretion. • Evaluation of the image for regulatory compliance is out of scope. • Recommended practices that address compliance requirements are out of scope. • Identification of silent installation commands or creation of unattended installation scripts for application installers is out of scope. • Running of scripts that automate image-setting customization and configuration is out of scope. • Unsupported processes that are used to remove inbox applications are out of scope.

2. Project approach, estimated timeline, and deliverable acceptance

2.1. Approach

The project will be structured following the Microsoft Online Services Lifecycle ("OSL") methodology across four distinct phases: Assess, Remediate, Enable, and Migrate. 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.

2.1.1. Engagement initiation

Before beginning the project and dispatching resources, the following prerequisites must be completed, remotely where applicable.

Category	Description
Microsoft activities The activities to be performed by Microsoft	• Conduct an initiation call to commence team formation and communicate expectations. • Document the project launch prerequisites using input from this SOW. • Track the status of 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 initiation call. • Assign responsibilities for project initiation and launch prerequisites to accountable customer resources 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 initiation call.

2.1.2. Assess

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

Category	Description
Microsoft activities The activities to be performed by Microsoft	**PAW for CSM activities** • Conduct a solution overview and planning workshop to inform the customer how the PAW for CSM solution is architected and capture any environment specific design decisions where appropriate. • Produce a preparation checklist which details the tasks that must be completed to allow for implementation of the integration solution, including the resources that must be procured. • Produce a design and plan document that reflects the PAW implementation.

Category	Description

	• Produce a draft of the PAW implementation guide document.
	• Conduct a solution overview and planning workshop to tell the Customer how the Reach-Back add-on was designed and capture appropriate environment-specific design decisions.
	• Update the preparation checklist, which details the tasks that must be completed to facilitate the implementation of the Reach-Back Add-On, including the resources that must be procured.
	• Add the Reach-Back Add-On–specific details to the design and plan document.
	• Add the Reach-Back Add-On–specific details to the draft version of the PAW implementation guide document.
	
	Microsoft Defender for Endpoint activities
	
	• Conduct one (1) design workshop to:
	  o Provide a brief overview of Microsoft Defender for Endpoint specific to features and capabilities related to this project.
	  o Gather Customer requirements for Microsoft Defender for Endpoint.
	  o Capture related design decisions for the Customer's use of Microsoft Defender for Endpoint.
	  o Define a plan for configuring and testing Microsoft Defender for Endpoint in the customer's environment.
	• Draft the Microsoft Defender for Endpoint Design and Plan Document. Review the document with Customer and update it.
	• Draft the preparation checklist. Review the checklist with the Customer and finalize it.
	• Draft the test cases spreadsheet. Review the test cases with Customer and finalize them.
	
	Clean Source Deployment Process activities
	
	• Assess readiness for secure room and MDT Server setup.
	• Produce a preparation checklist.
	• Produce a Design and Plan Document.

Customer activities The activities to be performed by the Customer	• Provide access to key personnel, service-level agreements, the current environment, and documentation.

Category	Description
	• Participate in Assess Phase activities, including workshops; communicate requirements; provide current environmental information; and make design decisions.
	Microsoft Defender for Endpoint activities
	• Provide access to key personnel, service-level agreements, current environment, and documentation. • Make decisions when options are presented. • Plan and identify target users or devices for enabling Microsoft Defender for Endpoint.
Key assumptions	*Microsoft Defender for Endpoint activities*
	• The Customer will coordinate appropriate resources for the design and plan workshop and will schedule meeting rooms to accommodate the size of the group. • Customer will participate in the review and approval of the Design and Plan Document and the Preparation Checklist.
	Clean Source deployment process activities
	• A secure room is available for Clean Source deployment.

Deliverables

PAW for CSM

Name	Description	Acceptance required?	Responsibility
Preparation Checklist	A Microsoft Excel spreadsheet that documents the tasks that must be completed by the Customer and the resources that must be procured to facilitate the completion of in-scope work	No	Microsoft
Design and Plan Document	A Microsoft Word document that captures design decisions made during the workshop, documents the design of the solution, and details the high-	Yes	Microsoft

Name	Description	Acceptance required?	Responsibility
	level plan for the completion of in-scope work		
Draft Implementation Guide	A Word document that summarizes how the solution is implemented	No	Microsoft

Microsoft Defender for Endpoint

Name	Description	Acceptance required?	Responsibility
Preparation Checklist	An Excel spreadsheet that documents the tasks that must be completed by the Customer and the resources that must be procured to facilitate the completion of in-scope work	No	Microsoft
Design and Plan Document	A Word document that captures design decisions made during the workshop, documents the design of the solution, and details the high-level plan for the completion of in-scope work	Yes	Microsoft
Draft Test Cases	An Excel document that summarizes validation test done to confirm expected functionality	No	Microsoft

Clean Source deployment process

Name	Description	Acceptance required?	Responsibility
Preparation Checklist	An Excel spreadsheet that documents the tasks that must be completed by the Customer and the resources that must be procured to facilitate the completion of in-scope work	No	Microsoft
Design and Plan Document	A Word document that captures design decisions made during the workshop, documents the design of the solution, and details the high-level plan for the completion of in-scope work	Yes	Microsoft

2.1.3. Remediate

During the Remediate Phase, the Customer will use the remediation and deployment plan to prepare the environment for PAW deployment.

Category	Description
Microsoft activities The activities to be performed by Microsoft	**PAW for CSM activities** • Provide general guidance and answer questions for up to **eight (8) hours** during Customer-led completion of identified preparation tasks. • Finalize the PAW Implementation Guide Document • Provide general guidance and answer questions during Customer-led completion of identified preparation tasks. **Microsoft Defender for Endpoint activities** • Assist with the remediation activities that have been identified after the workshop (limited to **sixteen (16) hours**). **Clean Source deployment process activities** • Provide general guidance and answer for up to **eight (8) hours** during Customer-led completion of identified preparation tasks.
Customer activities The activities to be performed by the Customer	• Produce all resources required for the project and complete all identified preparation tasks. • Assist Microsoft, as necessary, during production implementation tasks. • Participate in solution validation testing, as necessary. • Take ownership of the solution for ongoing management and support. • **Microsoft Defender for Endpoint activities** • Assign operational staff that will work side by side with the Microsoft team to identify, review, follow up on, and address or remediate performance or detection problems as they occur. • Prepare required production infrastructure and subscriptions.
Key assumptions	• The Customer is responsible for all remediation activities and will perform them with Microsoft assistance. Microsoft is not responsible for any remediation activities.

Category	Description
	• The Customer will communicate the actions taken and the results of those actions to Microsoft for inclusion in the updated preparation checklist and design and plan.

Deliverables

PAW for CSM

Name	Description	Acceptance required?	Responsibility
Implementation Guide	A Word document that summarizes how the solution was implemented	Yes	Microsoft

Microsoft Defender for Endpoint

Name	Description	Acceptance required?	Responsibility
Final Test Cases	An Excel document that summarizes the validation test done to confirm expected functionality	No	Microsoft

2.1.4. Enable

During the Enable Phase, PAW will be implemented and tested to validate expected functionality. After validation, Microsoft will perform a final demonstration of functionality. An engagement closeout meeting completes the project.

Category	Description
Microsoft activities The activities to be performed by Microsoft	**PAW for CSM activities** • Produce test cases that will be used to validate that the solution functions as designed. • Implementation activities necessary to deliver PAW for CSM devices: o Azure AD configuration o Intune configuration • Conduct validation testing.

Category	Description
	• Resolve defects.
	• Produce the Operations Guide.
	• Produce a Delivery Summary Document.
	• Add Reach-Back add-on–specific test cases that will be used to validate the solution functions as designed.
	• Complete the implementation activities necessary to deliver the Reach-Back add-on.
	• Conduct validation testing.
	• Resolve defects.
	• Add Reach-Back Add-On–specific details to the operations guide.
	• Add Reach-Back Add-On–specific details to the design and plan document.
	• Add Reach-Back Add-On–specific details to the delivery summary document.
	Microsoft Defender for Endpoint activities
	• Assist with the implementation of Microsoft Defender for Endpoint configuration capabilities based on workshop design decisions.
	• Assist with Microsoft Defender for Endpoint configuration on up to ten (10) devices.
	• Assist with solution validation through the test cases.
	• Provide time-boxed support for the following activities (limited to **4 hours**):
	o Provide the Customer with guidance on triaging and remediating identified problems.
	• Conduct one (1) operations workshop.
	• Finalize the Microsoft Defender for Endpoint Design and Plan Document.
	• Finalize the Delivery Summary Document.
	Clean Source deployment process activities
	• Implement MDT Server for bare-metal device deployment.
	• Perform tests as stated in Test Cases Document.
	• Produce the Delivery Summary Document.

Category	Description
Customer activities The activities to be performed by the Customer	• Assist Microsoft, as necessary, during production implementation tasks. • Participate in solution validation testing. • Take ownership of the solution for ongoing management and support. **PAW for CSM activities** • Manage user communication related to the rollout of the MFA and conditional access solution. **Microsoft Defender for Endpoint activities** • Identify target users for Microsoft Defender for Endpoint configuration • Assist in validating the functionality. • Support pilot users in their enrollment into Microsoft Defender for Endpoint. • Implement Microsoft Defender for Endpoint on the selected endpoints together with Microsoft Consultants. • Participate in the Operations Workshops for skills and knowledge transfer to the Customer's Operations Team.
Key assumptions	*Microsoft Defender for Endpoint* • The Customer will have obtained the required host systems (physical or virtual) that will be used for production implementation and they will be available by the start of this phase so that validation activities can be performed. • Microsoft Defender for Endpoint will be deployed on a production network. It will monitor production endpoints. • When Microsoft Defender for Endpoint is first installed, it might find problems or compromises in the environment. The Customer will provide personnel who can help determine whether the recorded event is a benign positive or the indication of an actual attack. If it is a benign positive, Customer will work with Microsoft to make configuration adjustments designed to address the benign positive event. • Test cases other than those that have been listed as in scope will be completed by the Customer and will not affect the completion of this project.

Category	Description
	• Required configuration changes will be made within the time frame that has been identified for tuning assistance.

Deliverables

PAW for CSM

Name	Description	Acceptance required?	Responsibility
Test Cases	An Excel spreadsheet that documents the test cases that will be run to validate that the implemented solution functions as designed	Yes	Microsoft
Operations Guide	A Word document containing recommended operational guidance and practices that can be used to maintain the security infrastructure and systems within the PAW	Yes	Microsoft
Delivery Summary Document	A Word document that summarizes the work completed, provides any relevant maintenance guidance, and documents any recommended next steps	No	Microsoft

Microsoft Defender for Endpoint

Name	Description	Acceptance required?	Responsibility
Delivery Summary	A Word document that summarizes the work completed, provides any relevant maintenance guidance, and documents any recommended next steps	No	Microsoft

Clean Source deployment process

Name	Description	Acceptance required?	Responsibility
Test Cases	An Excel spreadsheet that documents the test cases that will be run to validate that the implemented solution functions as designed	Yes	Microsoft
Delivery Summary	A Word document that summarizes the work completed, provides any relevant maintenance guidance, and documents any recommended next steps	No	Microsoft

2.1.5. Migrate

This SOW does not include a Migrate Phase.

2.2. Estimated Timeline

2.2.1. PAW for cloud services management

Component	Assess	Remediate	Enable	Total (in working days)
Microsoft Defender for Endpoint	4 days	2 days	4 days	10 days
Clean Source Deployment Process	0.5 day	0.25 day	4.25 days	5 days
PAW for CSM Baseline	3 days	3.5 days	7.5 days	14 days
PAW for CSM On-premises administration Reach-Back—using the Azure Bastion	2 days	0.5 day	2.5 days	5 days

2.2.2. Total durations

Assess
9.5 days

Remediate
6.25 days

Enable
18.25 days

These durations reflect working days.

2.3. Deliverable acceptance process

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

Within three (3) business days after 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 deliverable(s) 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 issues provided after a deliverable has been accepted will be addressed as a change request and managed as described in the Change management process section.

2.4. Project governance

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

2.4.1. 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, per the frequency defined in the communication plan, to review the overall project status, the acceptance of deliverables, and review open issues and risks.

2.4.2. 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 and risks (potential issues that could affect the project).
- **Analyze and prioritize**: assess the potential impact and determine the highest priority risks and issues 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 issues.
- **Escalate**: escalate to project sponsors the high impact issues 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.

2.4.3. Change management process

During the project, either party can 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 including impact on the project scope, schedule, and fees.
- **The change is submitted**: the change request form will be provided to the Customer.
- **The change is accepted or rejected**: The Customer has three (3) business days to confirm the following to Microsoft:
  - Acceptance—the Customer must sign and return change request form.
  - Rejection—if the Customer does not want to proceed with the change or does not provide an approval within three (3) business days, no changes will be performed.

2.4.4. 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's strategic direction.
- Serving as a final arbiter of project issues.
- Approving significant change requests.

Role	Organization
Project Sponsor	Customer
Delivery Manager	Microsoft

2.4.5. Escalation path

The Microsoft Project Manager will work closely with the Customer's 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 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's Project Sponsor
- Executive Steering Committee

2.5. 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 (1) 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.

3. Project organization

3.1. Project roles and responsibilities

The key project and leadership roles and the responsibilities are as follows.

Customer

Role	Responsibilities
Project Sponsor	- Provide the estimated project commitment: **Two (2) – four (4)** hours a week. - Make key project decisions. - Serve as a point of escalation to support clearing project roadblocks.
Project Manager	- Provide the estimated project commitment: **Twenty (20)** hours a week. - Serve as primary point of contact for the Microsoft team. - Manage the overall project. - Deliver the project on schedule.

Role	Responsibilities
	• Take responsibility for Customer resource allocation, risk management, and project priorities. • Communicate with executive stakeholders.
Technical Team Lead	• Expected allocation of **Sixteen (16) – forty (40)** hours a week. • Be available for, and responsive to, 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 **Four (4) – Twelve (12**) hours a week. • Be available for, and responsive to, technical, operational, or process questions. Full-time availability with expected the allocation of **Four (4) – Twelve (12)** hours a week. • Take responsibility for quality assurance ("QA") and escalation of technical decisions and problems.
Test and QA Lead	• Expected allocation of **Four (4) – Twelve (12)** hours a week. • Be available for, and responsive to, technical, operational, or process questions. • Take responsibility for test plans and guides and coordinating the acceptance testing of resources.

SMEs	• Expected allocation of **Eight (8) – Twenty-four (24)** hours a week**.**
	• Be available for, and responsive to, technical, operational, or process questions.
	• Provide technical representation related to systems, Services, architecture, and operation and process, including:
	
	   o Azure AD, Intune, cloud security architecture, network and DNS, and Microsoft Defender for Endpoint.
	   o On-premises security architecture.
	   o Network, DNS, public key infrastructure, and smart card integration.
	   o Security operation and process.

Microsoft

Role	Responsibilities
Delivery Manager	• Manage and coordinate the overall Microsoft project.

Role	Responsibilities
	• Serve as a single point of contact for escalations, billing problems, personnel matters, and contract extensions.
Microsoft Project Manager	• Manage and coordinate Microsoft project delivery. • Take responsibility for problem and risk management, change management, project priorities, status communications, and status meetings. • Coordinate Microsoft and Microsoft subcontractor resources but not Customer resources. • Project management may be delivered remotely
Microsoft Domain Solution Architect	• Provide technical oversight. • Verify that Microsoft-recommended practices are being followed. • Take responsibility for overall technical solution management.
Microsoft Consultants	• Lead workshop and produce document deliverables. • Provide technical design leadership. • Provide technical support during the Customer-led completion of preparation tasks. • Take responsibility for development of technical deliverables and complete all in-scope implementation work.

4. Customer responsibilities and project assumptions

4.1. Customer responsibilities

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

- Provide information:
    - o This includes accurate, timely (within 3 business days or as mutually agreed upon), and complete information.
- Provide access to people and resources.
    - o This includes access to knowledgeable Customer personnel, including business user representatives, and access to funding if additional budget is needed to deliver project scope.
    - o This includes the identification of key personnel (stakeholders, decision makers, architects, and subject matter specialists) to participate in the workshops, design sessions, and testing activities described in the Approach section.
    - o This includes allocating enough qualified staff to run the workstreams in parallel.
- Provide access to systems.
    - o This includes access to all necessary Customer work locations, networks, systems, and applications (remote and onsite).
    - o The Customer is responsible for configuring and controlling all Azure subscriptions and consumption.
- Provide a work environment.
    - o This consists of suitable workspaces, including desks, chairs, and Internet access.
- Provide the following:
    - o At least one physical server that can run virtual machines on Hyper-V will be used for the build and production environment.
    - o Five (5) unused and unopened laptops or desktops that will be used as production PAWs.
    - o Test data and personnel who will be needed to conduct solution system testing, including interfaces.
    - o Test data and personnel who will be needed to conduct Customer acceptance testing of the solution, including interfaces.
- Manage non-Microsoft resources.
    - o The Customer will assume responsibility for the management of all Customer personnel and vendors who are not managed by Microsoft.
- Manage external dependencies.
    - o The Customer will facilitate any interactions with related projects or programs to manage external project dependencies.

4.2. Project assumptions

The project scope, services, fees, timeline, and our detailed solution are based on the information provided by the Customer to date. During the project, the information and assumptions in this SOW will be validated, and if a material difference is present, this could result in Microsoft initiating a change

request to cover additional work or extend the project duration. In addition, the following assumptions have been made:

- Workday:
    - The standard workday for the Microsoft project team is between 8 AM and 5 PM, Monday through Friday.
- 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's location on a weekly basis, resources will typically be on site for three (3) nights and four (4) 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.
    - Resource availability and dispatch may affect timelines.
    - Microsoft will engage specific resources as deemed necessary by Microsoft to support a specific technical area. This could require multiple individuals engaged to support the engagement, based on technical specialty.
    - The number of hours per role are estimated for this project and the actual number of hours by role may vary during the project life but will be monitored by Microsoft project team members. Significant variations in estimated hours should be managed using the change management process.
- Informal knowledge transfer:
    - Customer staff members who work alongside Microsoft staff will be provided with information knowledge transfer throughout the project. No formal training materials will be developed or delivered as part of this informal knowledge transfer.

- Other assumptions:

    - All work is to be contiguously scheduled. Any breaks in the engagement calendar must be scheduled **four (4)** weeks in advance or will be billed without interruption.
    - Customer Lab and / or development facility is available.
    - Any delay on delivering customer required items could impact the delivery schedule.
    - Customer agrees that Microsoft, under this Work Order, may associate Customer's Online Services with Professional Services accounts through configuration of the Customer's subscriptions or Azure resources.