# 

Statement of Work

Azure Tier 0 Administrative Environment

Prepared for

Prepared by

Date: February 28th Feb, 2020

Version: 1.1 Final

Table of contents

[Introduction 2](#_Toc32328928)

[1. Project objectives and scope 2](#_Toc32328929)

[1.1. Objectives 2](#_Toc32328930)

[1.2. Areas in scope 4](#_Toc32328931)

[1.3. Areas not in scope 9](#_Toc32328932)

[2. Project approach, timeline, and deliverable acceptance 12](#_Toc32328933)

[2.1. Approach 12](#_Toc32328934)

[2.2. Timeline 21](#_Toc32328935)

[2.3. Deliverable acceptance process 21](#_Toc32328936)

[2.4. Project governance 22](#_Toc32328937)

[2.5. Project completion 23](#_Toc32328938)

[3. Project Organization 24](#_Toc32328939)

[3.1. Project roles and responsibilities 24](#_Toc32328940)

[4. responsibilities and project assumptions 27](#_Toc32328941)

[4.1. responsibilities 27](#_Toc32328942)

[4.2. Project assumptions 27](#_Toc32328943)

[5. Figures 29](#_Toc32328944)

[5.1. Cloud PAW Overview 29](#_Toc32328945)

[5.2. AzureAD Bastion Tenant 30](#_Toc32328946)

[5.3. AzureAD Bastion Tenant 31](#_Toc32328947)

This Statement of Work (SOW) and any exhibits, appendices, schedules, and attachments to it are made pursuant to Work Order TBC and describes the work to be performed (Services) by Microsoft (“us,” “we”) for (“Customer,” “you,” “your”) relating to Azure Tier 0 Administrative Environment (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

like many organizations in both the commercial and government sectors, faces an increasingly challenging cyber threat environment. Attackers have become sophisticated in both attack methodologies and in navigating business/social structures to obtain the information they are seeking. These modern cyber-attackers are adept at rapidly gaining administrative access to computing environments.

Protecting against these attacks is a key priority for .

# Project objectives and scope

## Objectives

In 2019 and Microsoft worked together on a program of work aimed at raising ’s cyber security posture. Three workstreams were carried out at this time;

* Active Directory Hardening – Deployment of the tier model to segregate control of critical infrastructure.
* Privileged Access Workstation – A secure administration path to tier 0 with dedicated hardware.
* Privileged Access Management – Providing a “Just in time” admin solution with a dedicated secure forest.

In order to assist in taking the next steps in the security and deployment maturity journey, this engagement has two main objectives;

* Extend the existing on-premise Tier 0 solution into Azure to provide the resilience and scalability of cloud services.
* Provide a secure path for the administration of Azure resources by means of a Privileged Access Workstation for Cloud Service Management.

The workstreams of this project are listed for each workstream in the following table.

| Workstream | Objectives |
| --- | --- |
| Privileged Access Workstation (PAW) for cloud services management | * Design and implement a PAW for the security-enhanced management of Azure services by privileged user roles. This PAW is used by Azure Active Directory accounts with Tier 0 privilege, such as global administrators. * The PAW will itself be configured and managed using cloud services to minimize security dependencies on ’s on-premises environment. |
| Secure Azure platform deployment and management | * Create dedicated “Security” Azure Tennant to host Tier 0 resources. * Activate and configure Azure Active Directory security controls to support solution. * Activate and configure Azure Multi-Factor Authentication (MFA) and configure Azure Active Directory conditional access policies for a tenant, applying controls to Azure Active Directory–integrated applications. * Establish basic monitoring and management functionality for Azure using Azure Monitor, Alerts, and Log Analytics. * Setup Azure Update Management to update Windows virtual machines in Azure. * Set up and configure Azure Backup as an integrated cloud backup for up to 10 Azure virtual machines in a single recovery services vault. |

## Areas in scope

### General project scope

Microsoft will provide Services in support of the following scope.

### Project management and governance

| Area | Description | Assumptions |
| --- | --- | --- |
| Project management and governance | Microsoft will support with project management and governance on ’s adoption of the Azure based Tier 0 Administrative Environment through the following activities.   * Act as single point of contact for all Microsoft-related activities in the context of this project. * Perform weekly and monthly reporting of progress. |  |

### Secure Azure platform design and implementation

| Area | Description | Assumptions |
| --- | --- | --- |
| Azure platform design and implementation | **Insights**   * Develop an initial Azure design proposal for this design iteration.   **Design**   * Conduct a design workshop to present, discuss, and explore the Azure design proposal.   **Implement**   * Configure the new Azure Active Directory Tenant. * Deploy foundational management infrastructure that will support the extension of the existing Tier 0 workload into Azure.   **Patch Management**   * Conduct a 4-hour workshop providing an overview of Azure analytics and its capabilities to manage the software update process across Windows servers hosted on Azure IaaS. * Document the patch management design. * Assist with streamlining the software update management process. * Assist with the setup and configuration of the Azure update management solution.   **Backup and Recovery**   * Conduct a 4-hour workshop that provides an overview of Azure Backup. * Lead a planning session to discuss Azure Backup requirements, policies, and configuration. * Document the Azure Backup design. * Assist with deploying an Azure Backup solution. * Create and configure one Recovery Service Vault(s) for backing up Azure Virtual Machines. * Configure Azure Backup on up-to 10 Azure Virtual Machines. * Assist with reviewing backup reports   **\*Note at time of writing backing up on-premise servers running “core” versions of operating systems is not supported via the use of the Microsoft Azure Recovery Services agent. \*** | **Implement**   * will participate in all implementation step activities, including planning, implementation, demonstration, and retrospective activities. * The implementation timeframe will be determined in coordination with . * Implementation is timeboxed to the build and stabilize phases of the project. * Microsoft will not configure the physical routers or network virtual appliances. * provided Palo Alto firewall will be used for outbound access from the Tier 0 virtual machines. Responsibility for Firewall configuration remains with . * will configure VPN connectivity between to their on-premises environment, to provide network connectivity between Tier 0 vNets and on-premises domain controllers. * New Azure Active Directory Tenant will be created for this solution. * provides new Azure AD Tenant. * This tenant and subscriptions associated with it are for the sole purpose of the Tier 0 Admin Environment and will not be used for other applications. * Overall effort for this service is time bound to a maximum of four (4) weeks duration. |

### PAW for cloud services management

| **Area** | **Description** | **Assumptions** |
| --- | --- | --- |
| PAW for cloud services management | * Deploy up to 5 PAW devices on 1 supported hardware model. * Configuration of devices using Windows Autopilot. * Configure a Microsoft Intune compliance policy for PAW devices * Configure Microsoft Intune configuration policies to harden PAW devices * Configure Windows Update for Business policies * Configure Intune to deliver identified administrative and support applications for PAW devices. This activity is time-boxed to 16 hours of effort. * Utilize the existing MDT Server for base build of PAW-CSM. * Configure a ‘Deploy’ task sequence to deploy the Windows 10 version to PAW devices and configure the device for Autopilot enrolment | * Only one hardware profile will be supported for PAW deployments. * Administrative and support applications include PowerShell modules for: Azure compute, AAD, MSOnline, and AAD PIM |
| Azure Platform Management | **Monitoring**   * Conduct a 4-hour workshop to deliver the monitoring design session. * Design the monitoring solution. * Build out the monitoring design on up to 10 agents. * Create up to 10 Azure alerts. | * Integration of Azure logging with third party SIEM is a responsibility. |
| Azure Security Center | * Activate Azure Security Center (ASC) for 2 Azure Subscription or Management Group. * Creation of 1 Azure (Security) Policy assignment based on the built-in “Initiative” created for ASC onboarded subscriptions. * Onboard PAW devices in ASC for monitoring of security state. This activity is timeboxed to 8 hours of effort. * Configuration of JIT access for up to 10 Azure-based Windows VMs. * Skills transfer and handover to operations. This activity is timeboxed to 4 hours of effort. | * Monitored computers must be running an operating system supported by the Microsoft Management Agent (MMA). |

### Threat Protection Technologies

Microsoft recommends the use of its Defender Advanced Threat Protection solution for tier zero devices.

However, has deicide to proceed with a third party EDR solution and Microsoft Defender P is out of scope for this engagement.

### SIEM Solutions

Third Party SIEM solutions such as Splunk & ARCsight provide connectors to allow them to consume logs from Microsoft Azure, either directly from the platform or via an Event Hub. The configuration of these connectors is out of scope for this engagement and the responsibility of .

### Software products and technologies

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

| Product and technology item | Version | Ready by |
| --- | --- | --- |
| Azure subscription | Not applicable | Project start date |
| Power BI Desktop edition | Power BI Desktop edition at no cost | Project start date |
| Microsoft Enterprise Mobility and Security (EMS) | E5 | Plan phase |
| Microsoft 365 (for a separate tenant) | E5 | Plan phase |
| Active Directory Domain Services | 2019 | Start of the project |
| Azure Active Directory | Premium | Start of the project |
| Azure Active Directory Premium. P2 is required for Azure Active Directory Identity Protection and Privileged Identity Management | P2 | Start of the project |
| Windows Server | 2019 | Project start date |
| Windows | 10 Enterprise x64 | Project start date |

### Environments

The following environments will be required to deliver the project.

| Environment | Location | Responsibility | Ready by |
| --- | --- | --- | --- |
| Test | 2 regions selected by |  | Project start |
| Production | 2 regions selected by |  | Project start |

### Testing and defect remediation

#### Testing

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

| Test type (environment) | Description | Responsibility | | |
| --- | --- | --- | --- | --- |
| Has responsibility  for testing? | Provides data or test cases | Provides guidance and support |
| System testing (development) | * System testing focuses on determining whether functionality meets design. During the Plan phase a high-level test plan will be created to guide testing activities. This test plan is a Microsoft Excel workbook listing up to 5 test cases, expected results, and observed results. Testing is focused on -specific scenarios as opposed to generic testing of Azure fundamentals. * The Microsoft effort to support this testing is limited to the Build and Stabilize phases. | Microsoft |  |  |

#### Defect remediation

If defects are identified during testing, the priority of the item will be jointly agreed upon by and Microsoft. The Microsoft team will attempt to fix all in-scope P1 and P2 defects. If this troubleshooting does not result in root cause identification and resolution within five business days, then additional time can be requested through the Change management process described in this SOW. Defect prioritization is defined in the following table.

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

## Areas not in scope

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

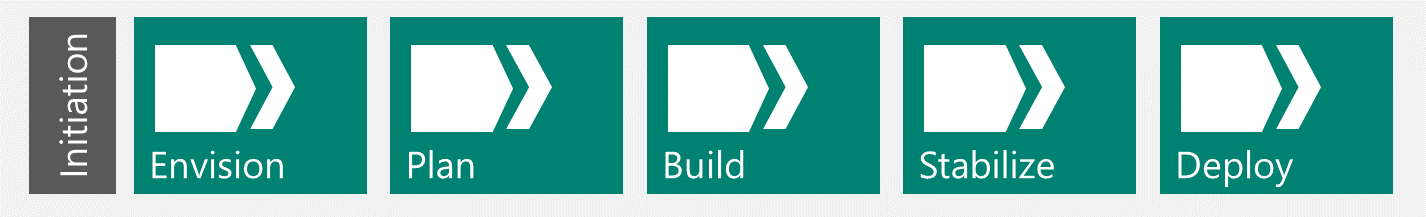
| Area | Description | | |
| --- | --- | --- | --- |
| Product licenses and subscriptions | Product licenses (Microsoft or non-Microsoft) and cloud service subscriptions are not included. | |
| Hardware | Microsoft will not provide hardware for this project. | |
| Integration with third-party software | Microsoft will not be responsible for integration with third-party software. | |
| Data migration | Data migration activities are not in scope for this project. | |
| Product bugs and upgrades | Product upgrades, bugs, and design change requests for Microsoft products are not in scope for this project. | |
| Source code review | 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. | |
| change management | Designing—or redesigning—’s functional is not included. | |
| Networking | Configuration of physical network devices, such as routers and firewalls, and virtual network appliances deployed on Azure is not in scope. | |
| Certification and accreditation | regulatory compliance certification and accreditation activities outside of general support for existing processes are not in scope. | |
| Workloads | Workload application compatibility, custom application remediation, configuration, or integration of workloads, whether Microsoft or third-party, is not in scope. | |
| Import of existing agile boards | Import of existing agile boards is out of scope. | |
| Physical server setup, management, and maintenance | | The following is not in scope:   * Physical server setup, installation, and networking interfaces or evaluation of new hardware or software * Ongoing production operational support |
| Networking configuration and hardware token usage and management | | Internet Protocol Security, smart cards, and FIDO2 devices are out of scope. |
| PAW as a virtual machine | | Deploying PAWs or productivity workstations as virtual machines on the “PAW for cloud service management” devices is not in scope. |
| Discovery | | Discovery and categorization of administrative tasks and applications are not in scope. |
| Virtual private network (VPN) integration | | Integration of ’s VPN solution is out of scope. |
| Azure Application Insights | | Monitoring web applications is not in scope. |
| Azure Automation Runbooks | | Creating Azure Automation runbooks is not in scope. |
| Azure Application Autoscale | | Autoscale of applications is not in scope. |
| Event Hubs | | Sending Azure Monitor data to Azure Event Hubs is not in scope. |
| Azure Logic Apps | | Creating Azure Logic Apps for use with Azure Alerts is not in scope. |
| Ingest and export APIs | | Using APIs to create custom action to either ingest or export Azure Monitor data is not in scope. |
| AD FS | | The following is not in scope:   * Customization of AD FS sign-in pages * AD FS integration with applications or services beyond Azure Active Directory |
| Azure Active Directory integration | | The following is not in scope:   * Azure AD Connect * Implementation of Azure Active Directory B2B * Installation and configuration of AD FS and WAP roles |
| Azure Active Directory: Identity Management | | Changes to individual group objects to accommodate self-service management in Azure Active Directory, including conversion of synchronized groups to cloud-based groups, are not in scope. |
| Improving the security on any Services other than DCs and associated forest or domain-level administration accounts | | This project looks only at securing Tier-0 of the Active Directory infrastructure. Providing a secure administration environment for standard user workstations or laptops and for applications servers (such as Exchange, SharePoint, or SQL Server) is out of scope. |
| General production domain hardening | | TIER 0 helps secure only domain admins user accounts; it does not secure other components of Active Directory Domain Services. General hardening of servers such as DCs is out of scope. |
| On-premises deployment | | Deployment of on-premises servers is out of scope. |
| Organisational Change Management | | Design or re-design of ’s functional organization unless specifically included in scope. |
| Third party EDR solutions. | | Deployment of third party EDR / Security solutions is out of scope for this engagement |
| Third Party SIEM solutions | | The configuration of third party SIEM solutions is out of scope for this engagement |

# Project approach, timeline, and deliverable acceptance

## Approach

The project will be structured following the Microsoft solution delivery methodology across four distinct phases: Envision, Plan, Build, and Stabilize. 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 or meeting to initiate team formation and communicate expectations. * Document the project launch prerequisites using input from this SOW. * Track the status of launch prerequisites and adjust the engagement initiation phase start date accordingly. * Conduct a detailed walk-through of the SOW with to agree upon an initial project schedule and approach. * Create an initial timeline to be presented during the kick-off meeting. * Prepare and share the detail plan for the Discovery phase and tentative plan for the Design phase, including suggested dates and an agenda. * Identify key personnel from side. * Develop a responsibility assignment matrix (RACI) for and Microsoft. |
| **activities** The activities to be performed by | * Attend and participate in the preinitiation call. * Assign project initiation and launch prerequisites responsibilities to accountable leadership and establish target completion dates. * Complete the project initiation and launch prerequisites. * Staff the project with the required resources in the time frames that were agreed upon in the preinitiation call. * The establishment of an VPN connectivity between the Azure environment and their on-premise environment. Configuration of this connection is a responsibility. |

### Envision

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

|  | |
| --- | --- |
| Category | Description |
| **Microsoft activities** The activities to be performed by Microsoft | * Participate in the joint kick-off of the discovery workshop with cloud lead. * Conduct the discovery workshop, topics include:   + Cloud Strategy.   + Cloud Governance and Management.   + Identity and Access Management.   + Security.   + Networking.   + Monitoring.   + Backup and Recovery. * Facilitate participation from SMEs and decision makers. * Lead with open-ended questions about critical design areas. * Perform dedicated note taking and team note taking. * Conduct a close out meeting to review action items, parking lot items, set expectations for the Insights phase, and begin scheduling the Design phase. |
| **activities** The activities to be performed by | * Participate in the joint kick-off of the discovery workshop with the Microsoft tech lead. * Share by leading discussion and whiteboarding sessions to help Microsoft understand ’s current and desired future state. * Facilitate participation from SMEs and decision makers. * Procure new Azure AD Tenant. * Procure all required licensing and enable it in the new Azure AD Tenant * Verify that prerequisites are met to connect datacenter to Azure. A VPN connection is required at the beginning of the engagement. * Procure a non-trial two Azure subscriptions or verify that an Azure enrolment is in place. |
| **Key assumptions** | * The relevant SMEs and decision makers are available for the discovery workshop. Scheduling will occur during the Pre-engagement phase. * representatives are expected to present the current environment in detail to the Microsoft team. |

#### Deliverables

| Name | Description | Acceptance required? | Responsibility |
| --- | --- | --- | --- |
| None | Microsoft will report on what we learned during the Discovery step in the Design step (Plan). | No | Microsoft |

### Plan

During the Plan phase, the team will develop a detailed plan for the project that includes a list of activities that are to be completed, and the project schedule.

|  | |
| --- | --- |
| Category | Description |
| **Microsoft activities** The activities to be performed by Microsoft | **Azure platform design and implementation**   * Conduct the internal Insights workshop to review discovery data and arrive at an initial design proposal.   + Map ’s requirements to Microsoft’s: demonstrated practices, design guidance, and reference patterns.   + Create an initial design proposal. Highlight key areas and key requirements addressed by the design.   + Prepare the design documentation: presentation, design and plan document, preparation checklist, test plan, backlog. * Conduct the design workshop with   + Present the initial design proposal to , topics include:     - Subscription Organization and Governance.     - Identity and Access Management.     - Policy Management.     - Platform Management and Monitoring.     - Automation.   + Explore key areas of the design to empower to take decisions.   + Explore ’s key requirements addressed by the design.   + Assist with obtaining approval of this design iteration.   **PAW for cloud services management**   * Conduct a solution overview and planning workshop to inform how the Cloud PAW 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. * Produce a draft of the PAW implementation document.   **Azure platform management**   * Conduct a workshop up to 8 hours in length to gather requirements, information about the current environment, and necessary decisions. * Produce a preparation checklist. * Produce a design and plan document.   **Patch Management**   * Workshop on the software update process and the Update Management solution.   **Backup and Recovery**   * Workshop regarding Azure Backup architecture, components used, storage options, backup policy, and reporting. * Recovery vault planning. * Backup configuration planning. * Azure Backup report planning.   **Azure Active Directory**   * Conduct an assessment and planning workshop to gather requirements, information about the current environment, and design decisions. * Produce a preparation checklist that details the tasks that must be completed to facilitate implementation of the integration solution, including the resources that must be procured. * Produce a design and plan document. * Conduct an assessment and planning workshop to gather requirements and information about the current environment, provide education related to Azure MFA and Azure Active Directory conditional access capabilities, and facilitate design decisions. * Design Azure Active Directory conditional access policies based on requirements. * Produce a preparation checklist. * Produce a design and plan document. * Provide general guidance and answer questions during -led completion of identified preparation tasks. * Provide input to end-user communications related to the solution.   **Azure Tier 0 solution design and implementation**   * Workshop on the TIER 0 solution design. * Create Architecture and Design document. |
| **activities** The activities to be performed by | * Manage all Change and Release Management activities associated with implementation. * Manage all end-user communication associated with implementation. * Participate in any demonstrations or operational handover workshops for skills and knowledge transfer.   **Azure platform design and implementation**   * Confirm external network connectivity to Azure. |
| **Key assumptions** | * ’s Azure environment must be ready for the Build phase. * Items in the preparation checklist can be remediated within 5 days Environmental changes must be made in a manner that supports the overall schedule. Delays can affect the overall schedule and require a change order. * will provide access to necessary documentation and/or IT operations SMEs, Process SMEs, and IT administrators. * will provide access to necessary decision makers for making changes to environment. |

#### Deliverables

| Name | Description | Acceptance required? | Responsibility |
| --- | --- | --- | --- |
| Preparation checklist | Microsoft to provide with a Excel spreadsheet that documents the tasks which must be completed by and the resources that must be procured to allow for the completion of in-scope work. are responsible for executing all tasks. | Yes  *Acceptance Criteria: Delivery of the final document* | Microsoft and |
| Design and plan | A Microsoft Word document that captures design decisions made during the workshop, documents the design for the solution, and details the high-level plan for the completion of in-scope work | Yes  *Acceptance Criteria: Delivery of the final document* | Microsoft |
| Operations Guide | Guide to the processes and procedures required for the ongoing operation and support of the solution. | No | Microsoft |
| PAW Management Guide | The guide:   * defines PAW user/admin onboarding processes and mechanisms (e.g., readiness, approvals), * defines additions and changes to existing IT operations processes to accommodate introduction of PAW, and includes the Service Map | No | Microsoft |

### Build

During the Build phase, the team will build all of the aspects of the solution and prepare it for final testing.

|  | |
| --- | --- |
| Category | Description |
| **Microsoft activities** The activities to be performed by Microsoft | **PAW for cloud services management**   * Provide general guidance and answer questions during -led completion of identified preparation tasks. * Finalize the PAW implementation document. * Produce test cases that will be used to validate the solution functions as designed. * Implementation activities necessary to deliver PAW devices:   + Azure Active Directory configuration.   + Microsoft Intune configuration.   + Azure Security Center configuration.     - Enable Security Center.     - Assign Administrator Roles/Permissions.     - Configure Log Analytics Workspace.     - Configure Azure Security Policy.     - Onboard Azure and non-Azure computers.     - Enablement of VMs for JIT Access. * Produce Delivery Summary document.   **Azure platform management**   * Install and configure Log Analytics workspace. * Install Windows Management agents. * Configure Azure Monitor for VMs solution. * Install and configure Agent Health solution in Log Analytics. * Create Azure dashboard.   **Patch Management**   * Activate and configure the Azure Update Management Solution. * Assess the current Software Update Management process. * Install Microsoft Monitoring Agents ((MMA) on up to 10 identified IaaS servers to be managed. * Assist in developing the update deployments: * Update deployment computer groups. * Update deployment exclusions. * Update deployment sequenced cycles (schedules).   **Backup and Recovery**   * Configure Azure Backup infrastructure.   + Create a recovery services vault.   + Configure recovery services vault.   + Configure backup (storage replication type).   + Select servers to protect. * Monitoring and alerting.   + Configure backup alerts.   + Configure notifications. * Azure Backup report infrastructure.   + Configure Power BI.   **Azure Active Directory**   * Complete validation testing for the solution. * Produce a delivery summary document. * Configure and demonstrate Azure Active Directory PIM. * Resolve defects. * Implement the Azure Active Directory conditional access policies that were initially scoped for test user accounts. * Implement and configure Azure Active Directory Identity Protection. * Complete validation testing of the solution. * Apply the MFA and conditional access solution to users; this can optionally be performed through a phased rollout. Microsoft will disengage after 1 week of the phased rollout, after which will be responsible for completion. * Demonstrate Azure Active Directory Identity Protection for . |
| **activities** The activities to be performed by | * Perform implementation activities with assistance from Microsoft. * Manage all Change and Release Management activities associated with implementation. * Manage all end-user communication associated with implementation. * Participate in any demonstrations or operational handover workshops for skills and knowledge transfer. * Perform all implementation activities required to deploy CrowdStrike as the Threat Protection Tool for the Tier Zero devices. |
| **Key assumptions** | * Activities in the Build phase are time-boxed as defined in the Timeline section. |

#### Deliverables

| Name | Description | Acceptance required? | Responsibility |
| --- | --- | --- | --- |
| Implementation iteration completion report | This report lists the in-scope items that have been completed during the implementation iteration, any planned work that was not completed, and any project risks or problems. This report is produced as an output of each implementation iteration. | No | Microsoft |
| Test cases | An Excel spreadsheet that documents the test cases which will be implemented to validate that the implemented solution functions as designed. | No | Microsoft |
| Solution demonstration | This deliverable demonstrates the solution as developed thus far. | No | Microsoft |

### Stabilize

During the Stabilize phase, the team will focus on testing the solution and preparing it for release.

|  | |
| --- | --- |
| Category | Description |
| **Microsoft activities** The activities to be performed by Microsoft | * Provide assistance to SMEs as they perform system testing of the solution, update test case documentation, and update the backlog.   **TIER 0 solution design and implementation**   * Support Acceptance Testing * Assist on remediation as required |
| **activities** The activities to be performed by | * Coordinate resources for, and conduct, all testing needed to review features and functionality. * Lead system testing of the solution. * Take ownership of the solution for ongoing management and support. * Perform Acceptance Testing. * Complete required change control processes. |
| **Key assumptions** | * will perform all testing, with Microsoft assistance. * Activities in the Stabilize phase are time-boxed as defined in the Timeline section. |

### Deliverables

| Name | Description | Acceptance required? | Responsibility |
| --- | --- | --- | --- |
| Delivery summary | A Word document that summarizes the work completed, provides any relevant maintenance guidance (i.e. back-up and patching) and documents any recommended next steps | No | Microsoft |
| Implementation iteration completion report | This report lists the in-scope items that have been completed during the implementation iteration, any planned work that was not completed, and any project risks or problems. This report is produced as an output of each implementation iteration. | Yes  *Acceptance Criteria: Delivery of the final report* | Microsoft |
| Test cases | An Excel spreadsheet that documents the test cases which will be implemented to validate that the implemented solution functions as designed | Yes  *Acceptance Criteria: Delivery of the final document* | Microsoft |
| Solution demonstration | This deliverable demonstrates the solution as developed thus far. | No | Microsoft |

## Timeline

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

NOTE: Delay in the availability of the System Integration and Environment readiness may result in scope and cost changes

## 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 ’s review and approval.

Within three business days of the date of submittal, 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; must include a complete list of reasons for rejection.

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

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

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

## Project governance

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

### Project communication

The following will be used to communicate during the project:

* **Communication plan**: this document will describe the frequency, audience, and content of communication with the team and stakeholders. It will be developed by Microsoft and 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).
* **Analyse and prioritise** assess the potential impact and determine the highest priority risks and problems that will be actively managed.
* **Plan and schedule**: determine the strategy for managing priority risks and issues and identify a resource who can take responsibility for mitigation and remediation.
* **Track and report**: monitor and report the status of risks and problems.
* **Escalate**: escalate to project sponsors the high impact problems and risks that the team is unable to resolve.
* **Control**: review the effectiveness of risk and issue management actions.

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

### Change management process

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

* **The change is documented**: all change requests will be documented by Microsoft in a Microsoft change request form and submitted to . The 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 change is accepted or rejected**: has three business days to confirm the following to Microsoft:
  + Acceptance— must sign and return change request form.
  + Rejection—if 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 problems.
* Approving significant change requests.

| Role |  | |
| --- | --- | --- |
| Project sponsor |  |
| Account Delivery Executive | Microsoft |

## Project completion

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

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

# Project Organization

## Project roles and responsibilities

The key project roles and the responsibilities are as follows.

| Role | Responsibilities |
| --- | --- |
| Project sponsor | * Make key project decisions. * Serve as a point of escalation to support clearing project roadblocks. |
| Project manager | * Serve as the primary point of contact for the Microsoft team. * Manage the overall project. * Deliver the project on schedule. * Take responsibility for resource allocation, risk management, and project priorities. * Communicate with executive stakeholders. |
| Technical team lead | * Serve as the primary technical point of contact. * Take responsibility for technical architecture and driving decisions that facilitate the Azure design creation. * Coordinate the installation and configuration activities of the required hardware elements. |
| Network lead | * Serve as the primary point of contact for the subject area. * Verify connectivity to Azure by VPN * Take responsibility for managing and performing the installation and configuration of subject area components. |
| Storage or backup lead | * Serve as the primary point of contact for the subject area. * Take responsibility for managing and performing the installation and configuration of subject area components. |
| Security lead | * Serve as the primary point of contact for the subject area. * Take responsibility for managing and performing the installation and configuration of subject area components. |
| Identity and Active Directory lead | * Serve as the primary point of contact for the subject area. * Take responsibility for managing and performing the installation and configuration of subject area components. |
| Operations lead | * Serve as the primary point of contact for the subject area. * Verify that Azure services will be integrated in the existing management environment. * Take responsibility for managing and performing the installation and configuration of subject area components. |
| Application or workload lead | * Serve as the primary point of contact for the subject area. * Provide insights into current or planned workloads deployed on Azure. * Take responsibility for managing and performing the installation and configuration of subject area components. |

#### Microsoft

| Role | Responsibilities |
| --- | --- |
| Account Delivery Executive | * Manage and coordinate the overall Microsoft project. * Serve as a single point of contact for escalations, billing problems, personnel matters, and contract extensions. * Coordinate Microsoft and Microsoft subcontractor resources but not resources. |
| 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 resources. |
| Azure architect | * Serve as the technical lead for the entire project and take responsibility for the scope. * Lead the Fit/Gap analysis and architecture sessions and deliver selected workshops. * Take responsibility for the Azure reference design document and drive the decision process with . * Assist with Azure configuration and other solution build activities. * Assist with solution testing. * Support the solution walk-through. |
| Azure consultants | * Perform the Fit/Gap analysis. * Deliver the architecture design sessions. * Lead the solution development activities. * Lead solution testing. * Lead the solution walk-through. |
| Microsoft security consultants | * Deliver the architecture design sessions for security. * Lead the ASC configuration and other solution build activities related to security. * Contribute to the solution development activities. * Contribute to solution testing. * Contribute to the solution walk-through. |

# responsibilities and project assumptions

## responsibilities

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

* Provide information.
  + This includes accurate, timely (within three business days or as mutually agreed upon), and complete information.
* Provide access to people and resources.
  + This includes access to knowledgeable personnel, including business user representatives, and access to funding if additional budget is needed to deliver project scope.
  + This includes the identification of key personnel (stakeholders, decision makers, architects, and subject matter specialists) to participate in the workshops, design sessions, and testing activities described in the Approach section.
  + This includes allocating enough qualified staff to run the workstreams in parallel.
* Confirm key personnel availability and coordinate personnel participation.
  + Key personnel will attend workshops and design sessions to provide requirements and participate in the discussions and decision making.
  + Key personnel identified to participate must be empowered to make decisions on behalf of and to engage and coordinate with other teams.
  + Key personnel will be able to make and approve binding design decisions in three days.
  + Key personnel required for the project will complete all identified preparation tasks to facilitate implementation of the solution
* Provide access to systems.
  + This includes access to all necessary work locations, networks, systems, and applications (remote and onsite).
  + is responsible for configuring and controlling all Azure subscriptions and consumption.
* Provide a work environment.
  + This consists of suitable workspaces, including desks, chairs, and Internet access.
* Manage non-Microsoft resources.
  + will assume responsibility for the management of all personnel and vendors who are not managed by Microsoft.
* Manage external dependencies.
  + will facilitate any interactions with related projects or programs in order to manage external project dependencies.

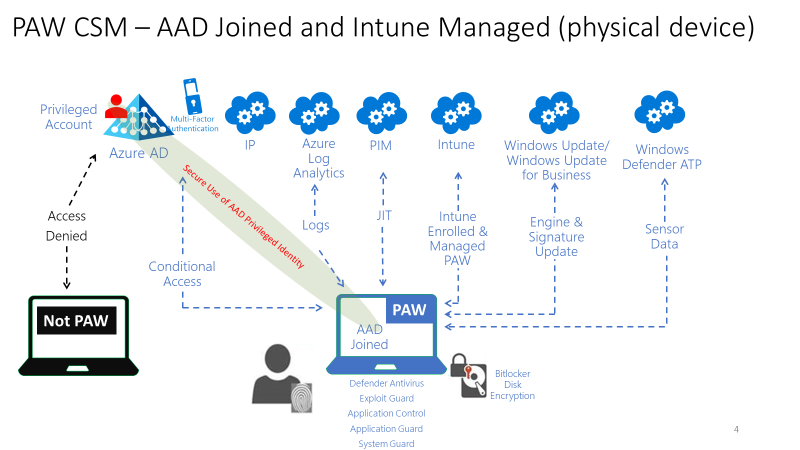
## Project assumptions

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

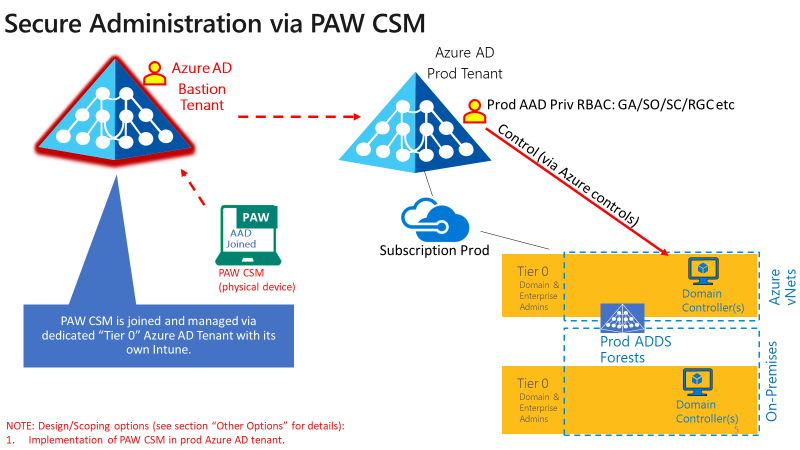
* Workday:
  + The standard workday for the Microsoft project team is between 8 AM and 5 PM, Monday through Friday.
  + When travel to a location is required, the arrival time, especially on Mondays, might vary depending on the travel time. This also applies for departure time on Fridays.
* Standard 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 location on a weekly basis, resources will typically be on site for three nights and four days, arriving on a Monday and leaving on a Thursday.
* Staffing:
  + If necessary, Microsoft will make staffing changes. These can include, but are not limited to, the number of resources, individuals, and project roles.
  + Microsoft resources will be mobilized up to four weeks from the date of the Work Order signature.
  + If work is interrupted, the activities may be resumed once requested and agreed to by Microsoft. In this case Microsoft may require up to six weeks to mobilize the resources and have the complete project team in place. In this situation Microsoft cannot guarantee that the team members will be the same team members who worked previously in the project.
* Informal knowledge transfer:
  + 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.
* Mobilisation
  + Mobilisation of project resources typically takes from two to six weeks, depending on resource availability and visa processing requirements.
  + The actual project start date will be mutually agreed once the associated work order is fully executed.

# Figures

## Cloud PAW Overview



## AzureAD Bastion Tenant



## AzureAD Bastion Tenant

