# 

Statement of Work

Statement of Work

Modern Workplace Security Essentials

Prepared for:

Date: June 22, 2020

Version: 2.3

Table of contents

[Introduction 1](#_Toc27678227)

[1. Project objectives and scope 1](#_Toc27678228)

[1.1. Objectives 1](#_Toc27678229)

[1.2. Areas in scope 1](#_Toc27678230)

[1.3. Areas out of scope 6](#_Toc27678231)

[2. Project approach, timeline, and deliverable acceptance 9](#_Toc27678232)

[2.1. Approach 9](#_Toc27678233)

[2.2. Timeline 19](#_Toc27678234)

[2.3. Deliverable acceptance process 20](#_Toc27678235)

[2.4. Project governance 20](#_Toc27678236)

[2.5. Project completion 22](#_Toc27678237)

[3. Project organization 22](#_Toc27678238)

[3.1. Project roles and responsibilities 22](#_Toc27678239)

[4. Customer responsibilities and project assumptions 25](#_Toc27678240)

[4.1. Customer responsibilities 25](#_Toc27678241)

[4.2. Project assumptions 26](#_Toc27678242)

This Statement of Work (SOW) and any exhibits, appendices, schedules, and attachments to it are made pursuant to Work Order [insert Work Order number] and describes the work to be performed (Services) by Microsoft (“us,” “we”) for (“Customer,” “you,” “your”) relating to Modern Workplace Security Essentials (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

This SOW describes the Microsoft Services Modern Workplace Security Essentials Offer for the Microsoft 365 solution, and does not include the purchase or activation of the Microsoft 365 solution which must be purchased through a separate order. Prior to signing the Work Order that references this SOW, the Customer will have had an opportunity to review the latest Microsoft 365 Service Descriptions. Microsoft strongly recommends that review those Service Descriptions with relevant internal stakeholders. acknowledges that the Service Descriptions meet or exceed the Customer’s minimum requirements for the selected Services.

# Project objectives and scope

## Objectives

The objectives of this project are to provide the Customer with additional support for requirements planning and implementation of the enhanced security capabilities of the Microsoft 365 solution.

The project will include the following components.

| ID | Component name |
| --- | --- |
| OTPM-01 | Office 365 Threat Protection and Management |
| DLP-01 | Office 365 Data Loss Prevention (DLP) |
| WTP-01 | Microsoft Defender Advanced Threat Protection |
| AADIS-03 | Azure Active Directory Multi-Factor Authentication (MFA) and Conditional Access |

## Areas in scope

### General project scope

The Modern Workplace Security Essentials project components are specified in the following table. All activities are to be completed in the Customer’s Microsoft 365 environment and do not include on-premises configuration unless otherwise specified.

| Component (ID) | Description | Assumptions |
| --- | --- | --- |
| Office 365 Threat Protection and Management (OTPM-01) | * Configure and test Microsoft Office 365 Exchange Online Protection (EOP) and Advanced Threat Protection (ATP) including the following:   + Mail exchanger (MX) record (inbound) and outbound mail routing for EOP (limit: one Send Connector (to EOP) rule)   + Sender Authentication (Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM) and Domain-Based Message Authentication, Reporting, and Conformance (DMARC)) set up and configured for single domain.   + EOP configuration for anti-spam, anti-malware, and anti-phishing/spoofing set up and configured (single default policy configuration for each function)   + ATP-based Safe Attachments and Safe Links set up and configuration (single default policy configuration for each). * The work described above is time-boxed to up to 120 hours. | EOP and ATP can be configured for applicable workloads in an Office 365 tenant provided by the Customer. |
| Office 365 Data Loss Prevention (DLP-01) | * Configure and test up to 5 data loss prevention policies in the Microsoft Office 365 Security and Compliance Admin Center that are based on the identification of sensitive information types across Microsoft Exchange Online, Microsoft SharePoint Online, and Microsoft OneDrive for Business workloads—specific to up to 3 Customer use cases.   + The work described above is time-boxed to up to 80 hours. | The Customer has an Office 365 tenant with 1 or more of the in-scope workloads enabled that can be used for DLP configuration. |
| Microsoft Defender Advanced Threat Protection  (WTP-01) | * Lead 1 workshop with the objective to validate Windows Defender Advanced Threat Protection (ATP) design decisions. * Activate Microsoft ATP on up to 10 supported Windows 10 client or Windows Server 2016 and 2019 endpoints. * Lead 1 workshop during which knowledge about the operations of Microsoft Defender ATP will be transfered. | * The Customer will allow endpoints to communicate directly with the Microsoft Defender ATP service endpoint. * Windows devices will be running in a supported version or build for Microsoft Defender ATP. |
| Azure Active Directory Conditional Access and Multi-Factor Authentication (AADIS-03) | * Configure Azure Multi-Factor Authentication (MFA) and Azure Active Directory conditional access in 1 Customer tenant to help secure Azure Active Directory–integrated applications and services, including Office 365. Microsoft will deliver the following to achieve this:   + Configuration of Azure MFA to Customer specifications   + Design and implementation of Azure Active Directory conditional access policies in the tenant   + If the Customer is using AD FS for federated authentication to Azure Active Directory, AD FS issuance authorization rules will be configured to implement controls for legacy authentication. * Implementation and configuration of Azure Active Directory Identity Protection to Customer specifications and demonstrate it to the Customer if the Customer is licensed for Azure Active Directory Premium P2. | * Only applications that are integrated with Azure Active Directory will be subjected to MFA or conditional access policy. * If Office 365 will be protected by the solution, the Customer has deployed an Office client that supports modern authentication (Microsoft Office 2013, Microsoft Office 2016, or Office 365). * If access is to be restricted to managed or compliant devices, Microsoft Intune will be used for mobile device management and hybrid Azure Active Directory join will be used for domain-joined computers. Implementation of these services is scoped separately. |

### Software products and technologies

The products and technology that are listed in the following table are required for project delivery. The Customer is responsible for obtaining all identified licenses and products. Microsoft assumes that any product version used during the project is either in mainstream support or is covered by an extended support agreement procured by the Customer.

| Component ID | Product and technology item | Version | Ready by |
| --- | --- | --- | --- |
| All | Office 365 and Intune tenant | Not applicable | Project start |
| OTPM-01 | Office 365 tenant, Exchange Online enabled | Latest version | Project start |
| WTP-01 | Windows 10 E5 | 1903 (or the latest version) | Start of the Remediate phase |
| Windows Server including the appropriate licenses | Windows Server 2016, 2016 version 1803, 2019) | Start of the Remediate phase |
| AADIS-03 | Azure Active Directory Premium (required for Multi-Factor Authentication with Conditional Access) | P1 or P2 | Start of the Enable phase |
| Modern Office client | Office 2013, 2016, or 365 | Start of the Enable phase |

### Environments

The following will be used for implementation and configuration activities that are included in the baseline project scope:

| Environment | Location | Responsibility | Ready by |
| --- | --- | --- | --- |
| Nonproduction tenant (Office 365) | Customer | Customer | Project start |
| Production tenant (Office 365) | Customer | Customer | Project start |
| Test on-premises environment | Customer | Customer | Project start |
| Production on-premises environment | Customer | Customer | Project start |
| Test Azure Active Directory subscription | Azure datacenters | Customer | Project start |
| Production Azure Active Directory subscription | Azure datacenters | Customer | Project start |

### Testing and defect remediation

| Test type (environment) | Description | Responsibility | | |
| --- | --- | --- | --- | --- |
| Has responsibility  for testing? | Provides test data | Provides guidance and support |
| Configuration per test case plan (non-production) | Completion of test cases in a nonproduction environment. | Microsoft | Customer | Customer |
| Configuration per test case plan (production) | Completion of test cases in production environment. | Microsoft | Customer | Customer |

#### Defect remediation

If defects are identified during testing, the priority of the item will be jointly agreed upon by the Customer and Microsoft. Defect prioritization is defined in the following table.

| Priority | Description | Remediation in scope? |
| --- | --- | --- |
| P1 | **Blocking defect**  Development, testing, or production launch cannot proceed until this type of defect is corrected. A defect of this type blocks further progress in this area. The solution cannot ship and the project team cannot achieve the next milestone until such a defect is corrected. | Yes |
| 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 out of scope

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

| Component ID | Area | Description |
| --- | --- | --- |
| All components | Office 365 tenant onboarding and general configuration | Office 365 tenant onboarding needs to be done prior to commencement of this engagement. |
| 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. |
| Client | Deployment and configuration of client software is out of scope for the project unless explicitly listed as in scope in the General project scope. |
| Integration with third-party software | Microsoft will not be responsible for integration with third-party software. |
| Product bugs  and upgrades | Product upgrades, bugs, and design change requests for Microsoft products |
| Source code review | The Customer will not provide Microsoft with access to non-Microsoft source code or source code information. For any non-Microsoft code, Microsoft Services will be limited to the analysis of binary data, such as a process dump or a network monitor trace. |
| Process reengineering | Designing functional business components of the solution |
| Organizational change management | Designing—or redesigning—the Customer’s functional organization is not included. |
| Lab environment | Creation of a development or testing lab environment |
| Performance testing | Performance or stress testing for any environment |
| Production environment conformity | Establishing full fidelity between any non-production environment and the Customer’s production tenant |
| Full-scale production environment planning | Planning and configuration work required to scale to full production (across the enterprise) |
| Communication of and training related to settings changes for users | IT communications, training, and adoption |
| OTPM-01 | Exchange on-premises enablement | Must be set up ahead of time if to hybrid to be used. |
| Centralized Mail Transport (CMT) configuration for on-premises Exchange | Must be set up ahead of time if routing via CMT to be employed. |
| Exchange hybrid configuration | Must be configured ahead of time if to be used. |
| Multiple domain configuration for Sender Authentication | Sender authentication for multiple domains requires add-on scope. |
| Additional policies (i.e. beyond the default policy setup) for the following: anti-malware, anti-spam, anti-phishing, ATP Safe Links, and ATP Safe Attachments. | Requires add-on scope. |
| DLP-01 | Information classification | Define information classification for the Customer if none is available. |
| Custom Sensitive Information Types (using XML) | Creation of custom information types not using the Out-of-the-Box (OOTB) admin UI. |
| Configuration of end-point DLP that leverages the Windows Information Protection (WIP) client | This requires the configuration of a Sensitivity Label involving end-point protection. |
| Azure Information Protection-based configuration of DLP | Configuration of DLP capabilities via AIP |
| Microsoft Cloud Application Security (MCAS)-based configuration of DLP | Configuration of DLP capabilities via MCAS |
| Labels | Details on the creation and publishing of Office 365 labels |
| Custom DLP Solutions | Custom security and compliance solutions using the Activity API are also out of scope, including custom DLP alerting reporting applications, integrated auditing solutions, etc. |
| Cloud App Security alerting | Managing advanced alerting through Office 365 Cloud App Security (a separate online service) |
| WTP-01 | Microsoft Defender Advanced Threat Protection | * Security Information and Event Management (SIEM) integration * Response and remediation of any threats that Microsoft Defender ATP might detect in the duration of the engagement * Assistance in engaging with a Microsoft Threat Expert through the Microsoft Defender Security Center portal * Implementation of any remediation activities or security recommendations suggested by the Threat and Vulnerability Management dashboard * The implementation of Attack Surface Reduction rules and policies * Activation of Microsoft Defender ATP on Linux endpoints |
| AADIS-03 | Azure MFA server or third-party MFA providers | * Deployment of the on-premises Azure MFA server is outside the scope of this project, as is integration with a third-party multi-factor authentication provider. |
|  | Remote access using Azure application proxy | * Implementation of Remote Access using Azure Application Proxy |

# Project approach, timeline, and deliverable acceptance

## Approach

The project will be structured following the Online Solution Lifecyle delivery methodology and will consist of three distinct phases: Assess, Remediate, and Enable. The final Migrate phase is not applicable for this project. Each phase has distinct activities and deliverables that are described in the following sections.



The activities for each in-scope project component will be organized into these phases, and components will generally progress through project phases together. The Assess phase activities for most components, for example, will be completed before the project proceeds to the Remediate phase, and the Remediate phase activities for most components will be completed before the project proceeds to the Enable phase. Microsoft reserves the right to delay the start of individual project components, when necessary, for the purposes of work prioritization or staffing optimization. During the Assess phase, a project plan will be produced that documents the detailed delivery schedule.

As part of this project, various deliverables will be created. If a deliverable requires formal review and acceptance (a process described in the Deliverable acceptance process section), this is indicated in the following sections.

### Engagement initiation

Before beginning the project, the following prerequisites must be completed.

| Category | Description | |
| --- | --- | --- |
| **Microsoft activities** The activities to be performed by Microsoft | * Conduct a preinitiation call to initiate team formation and communicate expectations. * Document the project launch prerequisites using input from this SOW. * Track the status of launch prerequisites and adjust the engagement initiation phase start date accordingly. * Conduct a detailed walk-through of the SOW with the Customer and reach agreement on an initial project schedule and approach. |
| **Customer activities** The activities to be performed by the Customer | * Attend and participate in the preinitiation call. * Assign project initiation and launch prerequisite responsibilities to accountable Customer leadership and establish target completion dates. * Complete the project initiation and launch prerequisites. * Staff the project with the required Customer resources in the time frames that were agreed upon in the preinitiation call. |

### General project activities

The following table describes the general activities for the project, organized by phase. These activities will be combined with the activities defined for in-scope [project components](#_Project_components_and) to establish the overall project approach.

| Category | Description | |
| --- | --- | --- |
| **Microsoft activities** The activities to be performed by Microsoft | **Assess phase**   * Prepare for, and conduct, the project kickoff meeting. * Document, discuss, and review conditions of satisfaction and define critical success factors of the project. * Create a risk, actions, issues, decisions (RAID) log and review it with the Customer. * Generate a project communication matrix that can be used to identify meeting cadence, key stakeholders, and the general communications strategy. * Create a preliminary project status report to review with the Customer project manager and refine as necessary based on that person’s input. * Deliver workshops and complete other Assess phase activities for in-scope components as defined in the Project components and deliverables section. * Produce a preparation checklist that details the tasks that are needed to complete the in-scope Enable phase activities, including the resources that must be procured by the Customer. * Produce, design, and plan the project documentation. * Produce a project plan for Microsoft project activities. * Remediate phase * Generate a weekly project status report and facilitate project status review meetings with the project team.   **Enable phase**   * Produce test cases that will be used to validate the implemented solution functions as designed. * Complete the Enable phase activities that are related to in-scope components as defined in the Project components and deliverables section. * Complete in-scope testing for the project. * Produce delivery summary documentation for the project. |
| **Customer activities** The activities to be performed by the Customer | **Assess phase**   * Provide project manager resources to work with the Microsoft project manager and manage Customer resources and assigned project activities. * Manage scheduling and logistics for project workshops. * Provide project resources and subject matter experts (SMEs) to participate in workshops and follow-up meetings. * Make necessary design and planning decisions in a timely fashion in order to facilitate completion of the Assess phase within the timelines documented in the Timeline section. * Review the RAID log with the Microsoft project manager and assign appropriate resources to actions, issues, and risks. * Develop a project communication matrix. * Provide templates or review existing templates that will be used for weekly status reports and steering committee reports. * Review all Assess phase deliverables. * Produce and manage the project plan for Customer project activities.   **Remediate phase**   * Complete all tasks identified in the preparation checklist and procure all required resources for the project within the timelines established for remediation as documented in the General project scope section. * Update the project plan with updates to project activities and statuses received from Customer project team members. * Assist in facilitating weekly project status review meetings. * Prepare user communications for the project.   **Enable phase**   * Provide required production access to Microsoft resources or resources who can work alongside Microsoft to facilitate completion of in-scope implementation tasks. * Update the project plan with statuses received from Customer project team members. * Implement and configure phase project deliverables * Review test cases * Participate in in-scope testing for the project and complete any testing activities assigned to the Customer. * Assist in facilitating weekly project status review meetings. * Manage the Change management process to facilitate timely completion of production implementation tasks. * Take ownership of the solution for ongoing management and support. * Manage all user communications associated with implementation tasks. |
| **Key assumptions** | * If the defined duration or effort for remediation is exhausted before the completion of critical path (blocking) remediation and preparation tasks, a change will be submitted following the Change management process in order to adjust project scope, timeline, and cost as necessary * The Customer will make all necessary design and planning decisions during the Assess phase of the project. Acceptance of the design and plan deliverable constitutes finalization of all options for implementation. Changes to Customer decisions after deliverable acceptance will be subject to a project change request. |

#### General project component deliverables:

Microsoft will produce the following project deliverables that include content from in-scope project components in the phases shown. Not all components will be covered in all deliverables; and the Project components and deliverables section documents how each component will be covered in these project deliverables. Deliverables will either be prepared as combined documents with content for all in-scope components, or multiple component-specific instances of these deliverables will be produced. During the Assess phase of the project, Microsoft and the Customer will mutually agree on a consolidated or per-component deliverable structure and then use that structure for all deliverable acceptance.

Additional component-specific deliverables might be produced for the project and any such deliverables are described in the Project components and deliverables section.

| Name | Description | Phase | Acceptance required? | Responsibility |
| --- | --- | --- | --- | --- |
| Project plan | Includes key Microsoft activities, milestones, dependencies, and durations. | Assess | No | Microsoft |
| Preparation checklist | An Excel spreadsheet that documents the tasks that must be completed by the Customer and the resources that must be procured in order to complete the in-scope work. | Assess | No | Microsoft |
| Design and plan | A Word document that captures design decisions made during the workshop, documents the design for the solution, and details the high-level plan for completion of the in-scope work. | Assess | Yes | Microsoft |
| Test cases | An Excel spreadsheet that documents the test cases that will be used to validate that the implemented solution functions as designed. | Enable | Yes | Microsoft |
| Delivery summary | A Word document that summarizes the work completed, provides any relevant operational guidance, and documents any recommended next steps. | Enable | No | Microsoft |

### Project components and deliverables

The following subsections describe the activities related to in-scope project components, organized by overall project phase. These activities will be combined with the General project activities to establish the overall project approach. The unique deliverables for each component and the project deliverables to which each component contributes, are also described in the following subsections.

#### Office 365 Threat Protection and Management (OTPM-01)

| **Category** | **Description** |
| --- | --- |
| **Microsoft activities** The activities to be performed by Microsoft | **Assess phase**   * Conduct a design workshop to:   + Provide a brief overview of Office 365 EOP and ATP capabilities   + Review the Customer’s current state hybrid protection capabilities, architecture, requirements and use cases   + Capture related design decisions for the Customer’s Office 365 EOP and ATP configuration and validation testing to be performed during the engagement. * Define a plan for configuring Office 365 EOP and ATP in the Customer’s Office 365 environment during engagement delivery.   **Remediate phase**   * Preparation tasks for Enable phase activities (as required and as defined during Assess phase activities).   **Enable phase**   * Assistance with configuration and testing of Office 365 EOP and ATP as specified in Assess phase documentation. |
| **Customer activities** The activities to be performed by the Customer | **Assess phase**   * Participate in the design workshop, communicate requirements (and use cases), provide current environmental information, and make design decisions.   **Remediate phase**   * Configure (as needed), and participate in, any required preparation tasks as defined in the preparation checklist.   **Enable phase**   * Work with Microsoft resources to implement configuration and testing tasks. |
| **Project deliverables** Content for this project component will be included in these project deliverables. | * Preparation checklist * Design and plan * Test cases |

#### Office 365 Data Loss Prevention (DLP-01)

| **Category** | **Description** |
| --- | --- |
| **Microsoft activities** The activities to be performed by Microsoft | **Assess phase**   * Conduct a design workshop to:   + Provide a brief overview of Office 365 Security and Compliance Center and Exchange Online DLP features and capabilities.   + Gather requirements and information about the Customer’s existing use of DLP (in Office 365 Exchange online and otherwise).   + Identify up to 3 DLP use cases.   + Capture related design decisions for the Customer’s Office 365 DLP configuration/validation testing that is in scope for implementation during this engagement. * Define a plan for configuration and testing of Office 365 DLP in the Customer’s Office 365 environment during engagement implementation.   **Remediate phase**   * Preparation tasks for Enable phase activities.   **Enable phase**   * Assistance with configuration and testing of up to 5 Office 365 DLP policies as specified in Assess phase documentation. |
| **Customer activities** The activities to be performed by the Customer | **Assess phase**   * Participate in the design workshop, communicate requirements (and use cases), provide current environmental information, and make design decisions.   **Remediate phase**   * Enable and participate in any required preparation tasks as defined in the preparation checklist.   **Enable phase**   * Work with Microsoft resources on configuration and testing tasks. |
| **Project deliverables** Content for this project component will be included in these project deliverables. | * Preparation checklist * Design and plan * Test cases |

#### Microsoft Defender Advanced Threat Protection (WTP-01)

| **Category** | **Description** |
| --- | --- |
| **Microsoft activities** The activities to be performed by Microsoft | **Assess phase**   * Conduct one design workshop to:   + Provide a brief overview of Microsoft Defender ATP specific to features and capabilities related to this project.   + Gather customer requirements for Microsoft Defender ATP.   + Capture related design decisions for the customer’s use of Microsoft Defender ATP.   + Define a plan for configuring and testing Microsoft Defender ATP in the Customer’s environment. * Draft a Microsoft Defender ATP design and plan document, review it with the Customer, and update it accordingly. * Draft a preparation checklist, review it with the Customer, and finalize it. * Draft a test cases spreadsheet. Review the test cases with the Customer and finalize them.   **Remediate phase**   * Assist with the remediation activities that have been identified after the workshop, limited to [16 hours for Baseline +1 hour for MacOS enablement add-on + 1 hour for Legacy devices enablement add-on].   **Enable phase**   * Assist with Microsoft Defender ATP configuration; the configuration will be based on workshop design decisions. * Assist with Microsoft Defender ATP configuration on up to [10 devices for Baseline + 10 devices for MacOS enablement add-on + 10 devices for Legacy devices enablement add-on]. * Assist with the solution validation through the test cases. * Provide time-boxed support for the following activities (limited to [4 hours for Baseline + 1 hour for MacOS enablement add-on + 1 hour for Legacy devices enablement add-on]): * Provide guidance to the Customer personnel that can help them triage and remediate identified problems. * Conduct an operations workshop. * Finalize the Microsoft Defender ATP design and plan document. * Finalize the delivery summary document. |
| **Customer activities** The activities to be performed by the Customer | **Assess phase**   * 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 on which Microsoft Defender ATP will be activated.   **Remediate phase**   * 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.   **Enable phase**   * Identify target users for Microsoft Defender ATP configuration. * Assist in validating the functionality. * Support pilot users in their enrollment into Microsoft Defender ATP. * Implement, with Microsoft consultants, Microsoft Defender ATP on the selected endpoints. * Participate in the operations workshops in which skills and knowledge will be transfered to the Customer operations team. |
| **Key assumptions** | **Assess**   * The Customer will coordinate the appropriate resources, attend the design and planning workshop, and will schedule meeting rooms to accommodate the size of the group. * The Customer will participate in the review and approval of the design and plan document and preparation checklist.   **Remediate**   * The Customer is responsible for all remediation activities and will perform them with Microsoft assistance; Microsoft is not responsible for any remediation activities. * The Customer will communicate the actions taken and the results of those actions to Microsoft for inclusion in the updated preparation checklist, design, and plan.   **Enable**   * The Customer will have obtained all 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 ATP will be deployed on a production network. It will be used to monitor production endpoints. * When Microsoft Defender ATP 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, the 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. * The Customer will perform the required configuration changes within the time frame that has been identified for tuning assistance. |
| **Project deliverables** Content for this project component will be included in these project deliverables. | * Preparation checklist * Design and plan * Test cases |

#### Azure Active Directory MFA and Conditional Access (AADIS-03)

| **Category** | **Description** |
| --- | --- |
| **Microsoft activities** The activities to be performed by Microsoft | **Assess phase**   * 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 Customer design decisions. * Design Azure Active Directory conditional access policies based on Customer requirements.   **Remediate phase**   * Provide general guidance and answer questions during Customer-led completion of identified preparation tasks. * Provide input to end-user communications related to the solution.   **Enable phase**   * Configure Azure MFA * 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 the Customer will be responsible for completion * Demonstrate Azure Active Directory Identity Protection for the Customer * Finalize the delivery summary document |
| **Customer activities** The activities to be performed by the Customer | **Assess phase**   * Provide access to key personnel, service-level agreements, current environment, and documentation. * Make decisions when options are presented * Participate in the assessment and planning workshop, communicate requirements, provide current environmental information, and make design decisions   **Remediate phase**   * 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.   **Enable phase**   * Manage all user communication related to the rollout of the MFA and conditional access solution. * If deploying the solution to users through a phased rollout more than 1 week in duration, complete the rollout to users after Microsoft disengages. * Participate in a demonstration of Azure Active Directory Identity Protection |
| **Key assumptions** | **Assess**   * The Customer will coordinate the appropriate resources, attend the design and planning workshop, and will schedule meeting rooms to accommodate the size of the group. * The Customer will participate in the review and approval of the design and plan document and preparation checklist.   **Remediate**   * The Customer is responsible for all remediation activities and will perform them with Microsoft assistance; Microsoft is not responsible for any remediation activities. * The Customer will communicate the actions taken and the results of those actions to Microsoft for inclusion in the updated preparation checklist, design, and plan.   **Enable**   * The Customer will have obtained all 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 ATP will be deployed on a production network. It will be used to monitor production endpoints. * When Microsoft Defender ATP 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, the 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. * The Customer will perform the required configuration changes within the time frame that has been identified for tuning assistance. |

## Timeline

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

## Deliverable acceptance process

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

Within three business days of the date of submittal, the Customer is required to:

* **Accept the deliverable** by signing, dating, and returning a service deliverable acceptance form, which can be sent by email, or by using (or partially using) the deliverable

Or

* **Reject the deliverable** by notifying Microsoft in writing; the Customer must include a complete list of reasons for rejection.

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

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

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

## Project governance

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

### Project communication

The following will be used to communicate during the project:

* **Communication plan**: This document will describe the frequency, audience, and content of communication with the team and stakeholders. It will be developed by Microsoft and the Customer as part of project planning.
* **Status reports**: The Microsoft team will prepare and issue regular status reports to project stakeholders per the frequency defined in the communication plan.
* **Status meetings**: The Microsoft team will schedule regular status meetings to review the overall project status, the acceptance of deliverables, and review open problems and risks.

### Risk and issue management

The following general procedure will be used to manage active project issues and risks during the project:

* **Identify**: Identify and document project issues (current problems) and risks (potential problems that could affect the project).
* **Analyze and prioritize**: Assess the potential impact and determine the highest priority risks and problems that will be actively managed.
* **Plan and schedule**: Determine the strategy for managing priority risks and issues and identify a resource who can take responsibility for mitigation and remediation.
* **Track and report**: Monitor and report the status of risks and problems.
* **Escalate**: Escalate to project sponsors the high impact problems and risks that the team is unable to resolve.
* **Control**: Review the effectiveness of risk and issue management actions.

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

### Change management process

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

* **The change is documented**: All change requests will be documented by Microsoft in a Microsoft change request form and submitted to the Customer. The change request form includes:
  + A description of the change.
  + The estimated effect of implementing the change.
* **The change is submitted**: The change request form will be provided to the Customer.
* **The change is accepted or rejected**: The Customer has three business days to confirm the following to Microsoft:
  + Acceptance—the Customer must sign and return change request form.
  + Rejection—if the Customer does not want to proceed with the change or does not provide an approval within three business days, no changes will be performed.

### Executive steering committee

The executive steering committee provides overall senior management oversight and strategic direction for the project. The executive steering committee for the project will meet per the frequency defined in the communication plan and will include the roles listed in the following table. The responsibilities for the committee include:

* Making decisions about project strategic direction.
* Serving as a final arbiter of project issues.
* Approving significant change requests.

| Role | Organization | |
| --- | --- | --- |
| Project sponsor | Customer |
| Delivery manager | Microsoft |

### Escalation path

The Microsoft project manager will work closely with the Customer project manager, sponsor, and other designees to manage project issues, risks, and change requests as described previously. The Customer will provide reasonable access to the sponsor or sponsors in order to expedite resolution. The standard escalation path for review, approval, or dispute resolution is as follows:

* Project team member (Microsoft or the Customer)
* Project manager (Microsoft and the Customer)
* Microsoft delivery manager
* Microsoft and the Customer project sponsor
* Executive steering committee

## Project completion

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

* All fees available have been utilized for Services delivered and expenses incurred.
* The term of the project has expired.
* All Microsoft activities and in-scope items have been completed.
* The Work Order has been terminated.

# Project organization

## Project roles and responsibilities

The key project roles and the responsibilities are as follows.

#### Customer

| Role | Component ID | Responsibilities |
| --- | --- | --- |
| Project sponsor | All | * Estimated project commitment: 2–4 hours a week * Make key project decisions. * Serve as a point of escalation to support clearing project roadblocks. |
| Project manager | All | * Estimated project commitment: 20 hours a week * Serve as primary point of contact for the Microsoft team. * Manage the overall project. * Deliver the project on schedule. * Take responsibility for Customer resource allocation, risk management, and project priorities. * Communicate with executive stakeholders. |
| Client infrastructure lead | All | * Participate in workshop discussions and take responsibility for activities that address client configuration for online service consumption. * Help the Microsoft team complete the client infrastructure implementation activities. |
| Communications and training lead | All | * Estimated project commitment: part time * Take responsibility for Customer communications related to the project. * Identify and plan for Customer training requirements related to the project. |
| Exchange and Exchange Online leads | OTPM-01 | * Estimated project commitment: part time * Participate in workshops, requirements gathering, specification development and review, testing and implementation review, and the final report presentation. |
| Exchange and SharePoint Online Administrators | DLP-01 | * Estimated project commitment: full time * Participation in workshops, requirements gathering, specification development and review, testing and implementation review and final report out presentation. |
| Office 365 and on-premises security administrators | OTPM-01, DLP-01 | * Estimated project commitment: part time * Participate in workshops, requirements gathering, specification development and review, access to Customer testing and production environments during testing and implementation, and the final report presentation. |
| Office 365 collaboration leads | OTPM-01, DLP-01 | * Estimated project commitment: full time * Participate in workshops, requirements gathering, specification development and review, testing and implementation review, and the final report presentation. |
| Windows 10 Security Leads | WTP-01 | * Estimated project commitment: part time * Participate in workshops, requirements gathering, specification development and review, testing and implementation review and final report out presentation. |
| Device management administrator | WTP-01 | * Estimated project commitment: part time * Participate in workshops, requirements gathering, specification development and review, testing and implementation review and final report out presentation. |
| Compliance Leads | DLP-01 | * Estimated project commitment: part time * Participation in workshops, requirements gathering, specification development and review, testing and implementation review and final report out presentation. |
| Security leads | AADIS-03 | * Provide security requirements for the solution. * Optionally, participate in solution validation testing |
| Identity leads | AADIS-03 | * Provide requirements for the MFA and conditional access solution and make design decisions. * Take responsibility for Azure Active Directory. * Take responsibility for the MFA and conditional access solution going forward. |

#### Microsoft

| Role | Component ID | Responsibilities |
| --- | --- | --- |
| Microsoft delivery manager | All | * Manage and coordinate the overall Microsoft project. * Serve as a single point of contact for escalations, billing issues, personnel matters, and contract extensions. * Facilitate project governance activities and lead the executive steering committee. |
| Microsoft project manager | All | * Manage and coordinate Microsoft project delivery. * Take responsibility for issue and risk management, change management, project priorities, status communications, and status meetings. * Coordinate Microsoft and Microsoft subcontractor resources but not Customer resources. |
| Microsoft lead architect | All | * Design the overall solution * Provide guidance based on Microsoft-recommended practices. |
| Microsoft consultant (or consultants) | All | * Deliver assessment and planning workshops. * Produce project deliverables. * Provide technical assistance during the completion of Customer preparation tasks. * Act as primary technical SME from Microsoft during the project. * Complete in-scope implementation and migration activities. |
| Consultant Exchange and Exchange Online leads |  | * Lead workshops and produce document deliverables. * Provides technical support during the Customer-led completion of preparation tasks. * Complete all in-scope implementation work. |

# Customer responsibilities and project assumptions

## Customer responsibilities

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

* Provide information.
  + This includes accurate, timely (within three business days or as mutually agreed upon), and complete information.
* Provide access to people and resources.
  + This includes access to knowledgeable Customer personnel, including business user representatives, and access to funding if additional budget is needed to deliver project scope.
* Provide access to systems.
  + This includes access to all necessary Customer work locations, networks, systems, and applications (remote and onsite).
* Provide a work environment.
  + This consists of suitable work spaces, including desks, chairs, and internet access.
* Manage non-Microsoft resources.
  + The Customer will assume responsibility for the management of all Customer personnel and vendors who are not managed by Microsoft.
* Manage external dependencies.
  + The Customer will facilitate any interactions with related projects or programs in order to manage external project dependencies.

## Project assumptions

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

* Work day:
  + The standard work day for the Microsoft project team is between 8 AM and 5 PM, Monday through Friday.
* Standard holidays:
  + Observance of consultants’ country-of-residence holidays is assumed and has been factored into the project timeline.
* Remote working:
  + The Microsoft project team may perform Services remotely.
  + If the Microsoft project team is required to be present at the Customer location on a weekly basis, resources will typically be on site for three nights and four days, arriving on a Monday and leaving on a Thursday.
* Language:
  + All project communications and documentation will be in English. Local language support and translations will be provided by the Customer.
* Staffing:
  + If necessary, Microsoft will make staffing changes. These can include, but are not limited to, the number of resources, individuals, and project roles.
* 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.
* Usage of production tenant for testing:
  + If production tenant is used for testing, the Customer understands the risk and agrees to its usage.