# 

Statement of Work

Cloud Security Planning

Prepared for

Prepared by

Date: March 3rd, 2020

Version: 1.0

Table of contents

[Introduction 1](#_Toc33775217)

[1. Project objectives and scope 1](#_Toc33775218)

[1.1. Objectives 1](#_Toc33775219)

[1.2. Areas in scope 2](#_Toc33775220)

[1.3. Areas out of scope 2](#_Toc33775221)

[2. Project approach, timeline, and deliverable acceptance 3](#_Toc33775222)

[2.1. Approach 3](#_Toc33775223)

[2.2. Timeline 5](#_Toc33775224)

[2.3. Deliverable acceptance process 6](#_Toc33775225)

[2.4. Project governance 6](#_Toc33775226)

[2.5. Project completion 8](#_Toc33775227)

[3. Project organization 8](#_Toc33775228)

[3.1. Project roles and responsibilities 8](#_Toc33775229)

[4. Customer responsibilities and project assumptions 9](#_Toc33775230)

[4.1. Customer responsibilities 9](#_Toc33775231)

[4.2. Project assumptions 10](#_Toc33775232)

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 Cloud Security Planning (project).

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

Introduction

has been adopting O365 and Azure capabilities and is looking for Microsoft guidance in applying appropriate security controls and governance. Along with implementing Conditional Access, Multifactor Authentication, and Privileged Access Workstations (PAW), is looking to understand where gaps exist between recommended practices and the current state. There are three areas of specific concern:

* As various business units request onboarding applications into Azure, is concerned about the security and privacy around granting consent to third-party applications to resources within Azure. seeks to understand how to properly govern and manage these requests appropriately.
* Today handles a secure environment, but such practices are unclear for a cloud-based Solution where the overall security posture is shared with Microsoft administrators. seeks to understand what capabilities exist within their current license structure and what a recommended approach would be given their constraints.
* Enabling a highly mobile workforce that can securely access appropriate applications and data is part of ’s long-term strategy. However, the risk of users accessing cloud services from unmanaged devices exists, possibly leading to data breach. seeks to understand protection methods available with Mobile Application Management (without enrollment) and guidance around implementation and management of these, and other, security controls.

Microsoft proposes using a Cloud Security Planning engagement as described in this Statement of Work to address these concerns and provide with recommendations and a roadmap to align to current recommended practices.

# Project objectives and scope

## Objectives

The objective of the Cloud Security Planning engagement is to provide with a prescriptive roadmap and a set of high-level recommendations that map Microsoft 365 security and compliance capabilities and Customer-controlled features to ’s business and technical requirements.

## Areas in scope

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

### General project scope

Microsoft will provide Services in support of the following scope.

| Area | Description | Assumptions |
| --- | --- | --- |
| Cloud Security Planning | * Delivery of a kickoff workshop and up to four (4) security and/or compliance-related technical planning workshops, including the development of strategic recommendations and a roadmap for each of the following capability areas:  1. Identity and access management 2. Threat protection and management 3. Information protection and governance 4. Security and compliance management   Timeboxed at 80 hours | The organization is interested in further development of a roadmap for the listed capability areas. |

### Software products and technologies

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

| Product and technology item | Version | Responsibility | Ready by |
| --- | --- | --- | --- |
| Power BI Desktop (Free version) | 2.76 or later | Customer | Prior to the report out |

## 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 include the following.

| Area | Description | |
| --- | --- | --- |
| Non-Microsoft 365–related and non-Azure–related security planning | Security planning for non-Microsoft 365 and non-Azure capabilities are out of scope. | |
| Detailed capability planning and/or design | Advanced planning of Microsoft 365 and Azure security capabilities elements, such as planning (and/or design) related to configuration, governance and integration specifications | |
| Product licenses and subscriptions | Product licenses (Microsoft or non-Microsoft) and cloud service subscriptions are not included unless otherwise noted in the Software products and technologies section. |
| Hardware | Microsoft will not provide hardware for this project. |
| Product bugs and upgrades | Product upgrades, bugs, and design change requests for Microsoft products are not in scope for this project. |
| Process reengineering | Designing functional business components of the solution is not included. |
| Organizational change management | Designing—or redesigning—the Customer’s functional organization is not included. |

# Project approach, timeline, and deliverable acceptance

## Approach

Microsoft Services uses the Online Solution Lifecyle delivery methodology, which consists of four distinct phases: Assess, Remediate, Enable, and Migrate. The Cloud Security Planning Offering consists of the Assess phase only; distinct activities and deliverables are described in the following sections. During the Assess phase, a project plan will be produced that documents the delivery schedule.

If a deliverable requires formal review and acceptance (a process described in the Deliverable acceptance process section), this is indicated in the following sections.

Migrate

Assess

Enable

Remediate

Initiation

### Engagement initiation

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

| Category | Description | |
| --- | --- | --- |
| **Microsoft activities** The activities to be performed by Microsoft | * Conduct a pre-engagement conference call to review objectives, deliverables, schedule, audience, and pre-engagement questionnaire * Get pre-engagement questionnaire from customer and pre-populate the Plan doc Discovery section. * Modify workshop templates according to customer interests, per questionnaire and Kickoff workshop discovery responses. |
| **Customer activities** The activities to be performed by the Customer | * Participate in a pre-engagement conference call to review objectives, deliverables, schedule, audience, and pre-engagement questionnaire * Respond to pre-engagement questionnaire |

### Assess

During the Assess phase, Microsoft will conduct a series of workshops to gather design requirements that will be based on the capability areas agreed to with the Customer. Microsoft will then review security capabilities that are currently missing or are of great interest. Finally, Microsoft will provide the Customer with a comprehensive list of recommendations and a suggested implementation roadmap that can be used to address security of the in-scope cloud workload.

|  | | |
| --- | --- | --- |
| Category | Description | |
| **Microsoft activities** The activities to be performed by Microsoft | **Assess Phase**  **Kickoff meeting (approximately 1 day):**   * Review the objectives and agenda. * Stakeholder introductions * Review of pre-engagement questionnaire inputs, including organizational profile, cloud security objectives, capabilities, readiness, and implementation status. * Microsoft security briefing and product overviews * High level discovery and customer priorities identification * Planning and logistics   **Core capability workshops (approximately 1 day each; 4 total).** Core capability workshops will be provided for each of the following four capability areas:   1. Identity and access management 2. Threat protection and management 3. Information protection and governance 4. Security and compliance management   Each workshop will include the following:   * Topic-focused strategic and technical briefings * Discovery * Product deep dives * Recommendations   **Documentation**   * Recording of discovery and recommendations in the Plan Document * Production of recommendations and roadmap materials * Report out production   **Report out**. Present recommendations and roadmap |
| **Customer activities** The activities to be performed by the Customer | * Participate in the workshops. * Communicate business and technical requirements. * Participate in decision making for each capability area. * Participate in the report-out meeting. |
| **Key assumptions** | Customer stakeholders will:   * Have a working knowledge of cloud computing concepts and security or compliance in general * Be able to provide requirements and drive decisions related to the production of the roadmap or output |

#### Deliverables

| Name | Description | Acceptance required? | Responsibility |
| --- | --- | --- | --- |
| Plan Document | Excel spreadsheet that captures data along with a Power BI dashboard that visualizes the customer baseline information, priorities, gaps and a roadmap with recommendations for next steps | Yes | Microsoft |
| Security recommendations and roadmap | PowerPoint summary document that captures customer priorities, gaps and a roadmap with recommendations for next steps | Yes | Microsoft |

## Timeline

The following timeline is a high-level representation; all dates and durations are relative to the project start date and are estimates only.

| Scope Option | Assess |
| --- | --- |
| Baseline | 10 days |
| **Add-on** | N/A |

## 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 after the date of submittal, the Customer is required to:

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

Or

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

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

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

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

## 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, per the frequency defined in the communication plan, to review the overall project status, the acceptance of deliverables, and review open issues 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 and risks (potential issues that could affect the project).

**Analyze and prioritize**: assess the potential impact and determine the highest priority risks and issues that will be actively managed.

**Plan and schedule**: determine the strategy for managing priority risks and issues, and identify a resource who can take responsibility for mitigation and remediation.

**Track and report**: monitor and report the status of risks and issues.

**Escalate**: escalate to project sponsors the high impact issues and risks that the team is unable to resolve.

**Control**: review the effectiveness of risk and issue management actions.

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

### 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 including impact on the project scope, schedule, and fees.

**The change is submitted**: the change request form will be provided to the Customer.

**The change is accepted or rejected**: the Customer has three (3) business days to confirm the following to Microsoft:

* + Acceptance—the Customer must sign and return change request form.
  + Rejection—if the Customer does not want to proceed with the change or does not provide an approval within three business days, no changes will be performed.

### Escalation path

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

* Project team member (Microsoft or the Customer)
* Project Manager (Microsoft and the Customer)
* Microsoft Delivery Manager
* Microsoft and the Customer Project Sponsor

## Project completion

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

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

# Project organization

## Project roles and responsibilities

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

#### Customer

| Role | Responsibilities |
| --- | --- |
| Project Sponsor | * Provide the estimated project commitment: 8 hours per week * Make key project decisions * Serve as a point of escalation to support clearing project roadblocks |
| Project Manager | * Provide the estimated project commitment: 8 hours per 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 |
| Microsoft 365 and Azure product managers | * Participate in workshops and provide requirements related to the organization's existing and planned communication and collaboration service offerings and security (and compliance) requirements for each * Assist with decision making and roadmap development |
| Microsoft 365 and Azure infrastructure manager | * Participate in workshops and provide requirements related to the organization's existing and planned Microsoft 365 deployment. * Assist with decision making and roadmap development |
| Microsoft 365 and Azure security leads | * Participate in workshops and provide requirements related to the organization's security and compliance requirements * Assist with decision making and roadmap development. |
| Business representative or liaison | * Participate in workshops and provide business requirements * Optionally, assist with decision making and roadmap development |

#### Microsoft

| Role | Responsibilities | |
| --- | --- | --- |
| Delivery Manager | * Manage and coordinate the overall Microsoft project * Drive delivery governance and operational excellence * Serve as a single point of contact for escalations, billing issues, personnel matters, and contract extensions |
| Project Manager | * 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. * Project management can be delivered remotely. |
| Architect | * Lead workshops, provide technical expertise, drive decision making and recommendations/roadmap development, and provide/deliver documentation and report out. |
| Domain Solution Architect | * Provide technical oversight. * Verify that Microsoft-recommended practices are followed. |

# Customer responsibilities and project assumptions

## Customer responsibilities

In addition to Customer activities defined elsewhere in this SOW, the Customer will also be required to:

Provide information:

* + This includes accurate, timely (within three (3) business days or as mutually agreed upon), and complete information required for the engagement.

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 workspaces, 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 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:

* + During the first week of delivery, the Microsoft Delivery Architect will be on site for three nights and four days, arriving on a Monday and leaving on a Thursday. The other project resources will participate remotely.
  + During the second week of delivery, entire Microsoft project team will perform Services remotely.

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.

Other assumptions:

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