Cloud Security Planning

Statement of Work

Prepared for

Prepared by

Date: February 28, 2020

Version: 1.0



Table of contents

[INTRODUCTION 1](#_TOC_250012)

1. [PROJECT OBJECTIVES AND SCOPE 1](#_TOC_250011)
   1. [OBJECTIVES 1](#_TOC_250010)
   2. [AREAS IN SCOPE 1](#_TOC_250009)
      1. [General project scope 1](#_TOC_250008)
   3. [AREAS OUT OF SCOPE 2](#_TOC_250007)
2. [PROJECT APPROACH AND TIMELINE 3](#_TOC_250006)
   1. [APPROACH 3](#_TOC_250005)
      1. [Engagement initiation 3](#_TOC_250004)
      2. [Assess 3](#_TOC_250003)
   2. [TIMELINE 5](#_TOC_250002)
3. [PROJECT ORGANIZATION 6](#_TOC_250001)
   1. [PROJECT ROLES AND RESPONSIBILITIES 6](#_TOC_250000)

This **‘Cloud Security Planning’** Statement of Work (SOW) and any exhibits, appendices, schedules, and attachments to it are made with accordance to the Master SOW (**Modern Workplace for Spin-Off**). Each chapter in the Master SOW applies to this document.

# Introduction

This SOW covers the following business scenario of **Modern Workplace Security and Compliance Planning**, and is including the following areas:

* Microsoft 365 Security
* Compliance

# 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 Azure security OR Microsoft 365 security and compliance capabilities and Customer-controlled features to ’ 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: | The organization is interested in further development of a roadmap for the listed capability areas. |
|  | * Identity, access and end-point management * Threat management * Information protection and governance * Compliance and security management |  |
|  | Timeboxed at 80 hours |  |

## 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.

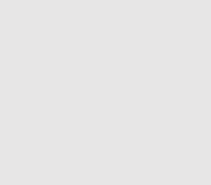
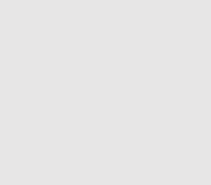
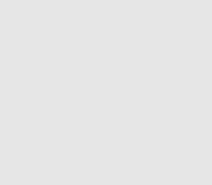
|  |  |
| --- | --- |
| **Area** | **Description** |
| Non-Microsoft 365–related security and compliance planning | Security and compliance planning for non-Microsoft 365 capabilities are out of scope. |
| Detailed capability planning and/or design | Advanced planning of Microsoft/Office 365 security and compliance 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 1.2.1 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 and timeline

## 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.



Assess

Remediate Enable

Migrate

Initiation

### Engagement initiation

Before beginning the project and dispatching resources, the following prerequisites must be completed (remotely when applicable). Microsoft will support the customer in the following areas marked as “Microsoft activities”:

|  |  |
| --- | --- |
| **Category** | **Description** |
| **Microsoft activities**  The activities to be performed by Microsoft | * Conduct a pre-engagement conference call to review objectives, 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, 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. Microsoft will support the customer in the following areas marked as “Microsoft activities”:

|  |  |
| --- | --- |
| **Category** | **Description** |
| **Microsoft activities—Modern Workplace Security and Compliance Planning**  The activities to be performed by Microsoft | **Kickoff meeting (approximately 8 hours):**   * Review the objectives and agenda. * Stakeholder introductions * Review of pre-engagement questionnaire inputs, including organizational profile, cloud security and compliance 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, i.e. 4 total).** Core capability workshops will be provided for each of the following four capability areas:   * Identity, Access and End-Point Protection * Threat protection * Information protection and governance * Compliance and security 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 doc * 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 |

|  |  |
| --- | --- |
| **Category** | **Description** |
| **Other activities**  Content for this project component will be included in these documents**.** | Plan Document - Word document that captures customer baseline information, priorities, gaps and a roadmap with recommendations for next steps  Security recommendations and roadmap - PowerPoint summary document that captures customer priorities, gaps and a roadmap with recommendations for next steps |

## 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 |

# Project organization

## Project roles and responsibilities

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

#### Customer

|  |  |
| --- | --- |
| **Role** | **Responsibilities** |
| Project Sponsor | * Make key project decisions * Serve as a point of escalation to support clearing project roadblocks |
| Project Manager | * 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/Office 365 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/Office infrastructure manager | * Participate in workshops and provide requirements related to the organization's existing and planned Microsoft/Office 365 deployment. * Assist with decision making and roadmap development. |
| Microsoft/Office 365 security and compliance 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** |
| Architect | * Lead workshops, provide technical expertise, drive decision making and recommendations/roadmap development, and provide/deliver documentation and report out. |

|  |  |
| --- | --- |
| **Role** | **Responsibilities** |
| Domain Solution Architect | * Provide technical oversight. * Verify that Microsoft-recommended practices are followed. |