# 

Statement of Work

Cybersecurity Risk Review

Prepared for

Prepared by

Date: June 22, 202019

Version: 2.0

Table of contents

[Introduction 1](#_Toc6832767)

[1. Project objectives and scope 1](#_Toc6832768)

[1.1. Objectives 1](#_Toc6832769)

[1.2. Areas in scope 1](#_Toc6832770)

[1.3. Areas out of scope 6](#_Toc6832771)

[2. Project approach, timeline, and deliverable acceptance 7](#_Toc6832772)

[2.1. Approach 7](#_Toc6832773)

[2.2. Timeline 12](#_Toc6832774)

[2.3. Deliverable acceptance process 12](#_Toc6832775)

[2.4. Project governance 13](#_Toc6832776)

[2.5. Project completion 15](#_Toc6832777)

[3. Project organization 15](#_Toc6832778)

[3.1. Project roles and responsibilities 15](#_Toc6832779)

[4. Customer responsibilities and project assumptions 17](#_Toc6832780)

[4.1. Customer responsibilities 17](#_Toc6832781)

[4.2. Project assumptions 17](#_Toc6832782)

This Statement of Work (SOW) and any exhibits, appendices, schedules, and attachments to it are made pursuant to Work Order 6CZE1912-270079-320759 and describes the work to be performed (Services) by Microsoft (“us,” “we”) for (“Customer,” “you,” “your”) relating to Cybersecurity Risk Review (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

Cybersecurity Risk Review is an assessment that organizations can use to evaluate their current security environments related to technical, organizational, and operational controls.

Cybersecurity Risk Review will use current Microsoft recommendations and align to industry standards and frameworks such as ISO/IEC (International Organization for Standardization/International Electrotechnical Commission) 27001:2013, 27002:2013, and 27017:2015 standards, and National Institute of Standards and Technology Cybersecurity Framework.

# Project objectives and scope

## Objectives

The objectives of this engagement are defined as follows:

* Assess current organizational and technical security practices and identify any potential security gaps that could expose the Customer information assets to risk.
* Produce an assessment report that documents security gaps.
* Produce a roadmap to help the Customer improve its security posture in the assessed areas.
* Provide recommendations on how to remediate findings based on recommended industry practices, Microsoft recommendations, and security policies approved and documented by the Customer.

## Areas in scope

### General project scope

Microsoft will provide Services in support of the following scope.

| Area | Description | Assumptions |
| --- | --- | --- |
| Educational workshop (IT) | Microsoft will conduct 1 education workshop, time-boxed to 2 hours.   * Information security management * Relevant ISO/IEC 27000 standards:   + ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements   + ISO/IEC 27002:2013 Information technology - Security techniques - Code of practice for information security controls   + ISO/IEC 27017:2015 Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services   Assessment scope and details:   * + Overview of the assessment scope   + Detailed description of the domains | The Customer has made the appropriate personnel available to gain value from the workshop and has provided an appropriate facility or room that can be used to host the meeting. |
| Interview (IT) | Interviews with key stakeholders to assess the security posture as compared to recommended practices  16 meetings or interviews (up to 2 hours each) covering:   * Information security policy * Organization of information security * Human resource security * Asset management * Access control * Cryptography * Physical and environmental security * Operations security * Communications security * System acquisition, development, and maintenance * Supplier relationships * Information security incident management * Information security aspects of business continuity management * Compliance * Cloud * Privacy | * The Customer has equipped personnel to accurately answer the interview questions available to the assessors (refer to the engagement preparation guide document for the interview or meeting stakeholder list). * Pre-engagement scheduling has been completed by the Customer. * The Customer has securely shared any relevant documentation that can be reviewed by the consultant prior to arriving onsite (such as, but not limited to):   + Information security policy   + Organization charts   + Human resources re-hire and termination policies   + Asset management plan and procedures   + Access control policy   + Cryptography policy   + Physical security processes and procedures   + Software development life cycle procedures   + Management of supplier relationships procedures   + Incident response plan |
| Review | A review of the assessment results with the Customer (up to 10 hours) | The Customer has equipped the personnel to accurately review the assessment results available to the assessor. |
| Roadmap development workshop | A workshop held to create a remediation roadmap tailored to the Customer’s needs, situation, and capacity (up to 10 hours) | The Customer has verified the availability of personnel who have the decision-making authority to create the remediation roadmap.  The Microsoft delivery team will be on site but can be adjusted to a remote site based on the Customer’s preference. |

## Areas out of scope

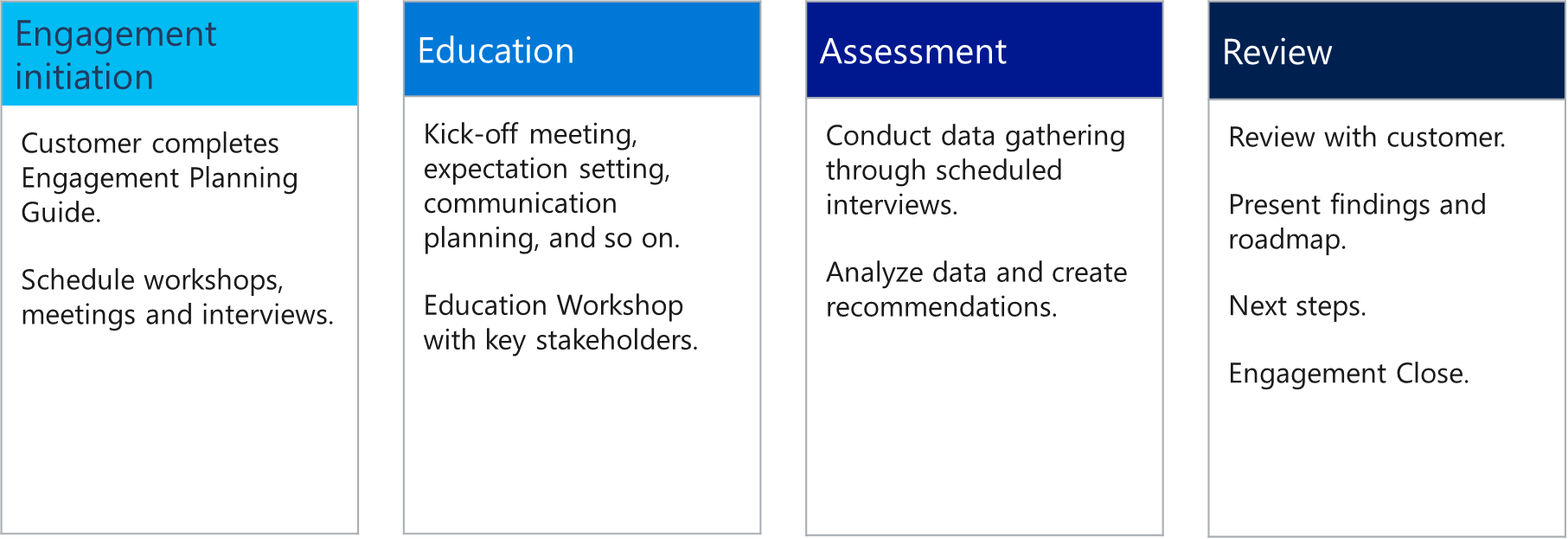
Any area not explicitly included in the areas in scope section is out of scope for Microsoft during this project. Areas out of scope for this project are listed in the following table.

| Area | Description |
| --- | --- |
| Device analysis | Risk analysis of particular devices such as the one used in Partner Learning Center and Supervisory Control and Data Acquisition is not in scope. |
| Physical network | Review and design of a physical network and configurations are not in scope. |
| Formal audit | The engagement is not a formal audit of the organization to meet a standard, framework, certification, or attestation. |
| Compliance assessment | The engagement is not a compliance assessment with any standard or framework. It uses frameworks solely as a guide to help organizations address line items within these frameworks. |
| Remediation efforts | Remediation efforts or actions are not in scope. |
| 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. |
| System integration | System integration and interfaces 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 | 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 network monitor trace. |
| 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

The project will be structured as shown in the following figure. 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 in order 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 in order to agree on an initial project schedule and approach. |
| **Customer activities** The activities to be performed by the Customer | Complete the engagement preparation guide document and send it to Microsoft 1 week before the kickoff meeting.  Attend and participate in the preinitiation call.  Assign project initiation and launch prerequisites 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. |

### Education

During the Education phase, the team (Microsoft and the Customer) will kick off the engagement and conduct the education workshop to level-set everyone involved on the methodology and approach for the engagement.

| Category | Description |
| --- | --- |
| **Microsoft activities** The activities to be performed by Microsoft | Lead a kickoff meeting.  Lead an education workshop. |
| **Customer activities** The activities to be performed by the Customer | Host the kickoff meeting and the education workshop. |
| **Key assumptions** | The Customer will have completed all items in the engagement preparation guide document prior to the kickoff.  The Customer will verify that the appropriate personnel are present and dedicated to these tasks. |

### Assessment

During the Assessment phase, the Microsoft team members will conduct the core interviews needed to gather data for the deliverables.

| Category | Description |
| --- | --- |
| **Microsoft activities** The activities to be performed by Microsoft | Conduct and lead assessment interviews. There will be 16 interviews in total, 1 for each assessment domain. Each interview is time-boxed for a maximum of up to 2 hours. The assessment domains are:   * Information security policy * Organization of information security * Human resource security * Asset management * Access control * Cryptography * Physical and environmental security * Operations security * Communications security * System acquisition, development, and maintenance * Supplier relationships * Information security incident management * Information security aspects of business continuity management * Compliance * Cloud * Privacy   Analyze and generate a draft report in Microsoft Word format. |
| **Customer activities** The activities to be performed by the Customer | The Customer will identify personnel who can participate in the assessment interviews and provide answers to the assessment domains. |
| **Key assumptions** | As scheduled, key personnel identified by the Customer during the Pre-engagement phase will be available for these interviews. |

#### Deliverables

| Name | Description | Acceptance required? | Responsibility |
| --- | --- | --- | --- |
| Findings list | A Microsoft Excel spreadsheet that lists review findings across the assessed domains, their priority, and recommendations | No | Microsoft |
| Draft Cybersecurity Risk Review report | A Word document that details the areas of analysis, findings, and a roadmap in which actions are suggested for the short-term, mid-term, and long-term time periods | No | Microsoft |

### Review

During this final phase, the team will review the assessment results with the Customer and conduct a remediation roadmap workshop.

|  | |
| --- | --- |
| Category | Description |
| **Microsoft activities** The activities to be performed by Microsoft | Conduct an assessment review with the Customer, including a review of the contents of the Word report that was delivered in the previous phase.  Present the remediation roadmap. The Microsoft team will conduct a presentation which includes:   * + A review of the project goals and objectives.   + An overview of the risk review process and analysis framework.   + The roadmap of recommendations. |
| **Customer activities** The activities to be performed by the Customer | Attend the assessment review and remediation roadmap workshop. |
| **Key assumptions** | Key personnel identified by the Customer during the Pre-engagement phase will be available for the assessment review and remediation roadmap workshop. |

#### Deliverables

| Name | Description | Acceptance required? | Responsibility |
| --- | --- | --- | --- |
| Final Cybersecurity Risk Review report | A Word document that details the areas of analysis, findings, and a roadmap in which actions are suggested for the short-term, mid-term, and long-term time periods | Yes | Microsoft |
| Cybersecurity Risk Review recommendations roadmap | A Microsoft PowerPoint presentation that summarizes key findings for each assessed domain and recommends a remediation roadmap | No | Microsoft and Customer stakeholder |

## 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.

## 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.

Review and acceptance of the solution or custom source code is based on completion and acceptance of user acceptance testing as described in the Testing and defect remediation section.

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 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.

### 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

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.

#### Customer

| Role | Responsibilities |
| --- | --- |
| Project sponsor | Provide the estimated project commitment: 0.5hour per week  Make key project decisions.  Serve as a point of escalation to support clearing project roadblocks. |
| Project manager | Provide the estimated project commitment: 1 hour per week  Serve as the 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. |
| Subject matter specialists | Provide the estimated project commitment: 16 hours per week  Take authority over the assessment domains that are defined in the engagement preparation guide. |

#### Microsoft

| Role | Responsibilities |
| --- | --- |
| Delivery manager | Manage and coordinate the overall Microsoft project.  Serve as a single point of contact for escalations, billing issues, personnel matters, and contract extensions. |
| Microsoft 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. |
| Cybersecurity architect | Provide overall engagement oversight to help make sure the solution methodology is followed, review all engagement deliverables, and identify and manage risk. |
| Senior consultant | Take responsibility for the delivery of all engagement components, including workshops, interviews, and the creation of all engagement deliverables. |

# Customer responsibilities and project assumptions

## Customer responsibilities

In addition to 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 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 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:

* Workday:
  + The standard workday for the Microsoft project team is between 8 AM and 5 PM, Monday through Friday.
* Standard holidays:
  + Observance of consultants’ country-of-residence holidays is assumed and has been factored into the project timeline.
* Remote working:
  + The Microsoft project team may perform Services remotely.
  + If the Microsoft project team is required to be present at the Customer 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.