|  |
| --- |
| Microsoft Logo |
| Microsoft Security Assessment  Delivery Guide |
| v2.0 - July 2019 |

Table of Contents

[1 Introduction 5](#_Toc14435655)

[1.1 Delivery Guide 5](#_Toc14435656)

[1.2 Audience 5](#_Toc14435657)

[2 Engagement overview - high level 6](#_Toc14435658)

[2.1 Week 3 - modular delivery model 7](#_Toc14435659)

[2.1.1 Secure Score Assessment - Sample delivery schedule 8](#_Toc14435660)

[2.1.2 Secure Score and Shadow IT Assessments - Sample delivery schedule 9](#_Toc14435661)

[2.1.3 Secure Score, Shadow IT and Windows Security Assessments - Sample delivery schedule 10](#_Toc14435662)

[2.1.4 Secure Score, Shadow IT, Windows Security and Attack Simulator Assessments - Sample delivery schedule 11](#_Toc14435663)

[2.2 Estimated engagement partner effort 12](#_Toc14435664)

[2.3 Engagement Objectives 13](#_Toc14435665)

[2.4 Engagement scoping 13](#_Toc14435666)

[2.4.1 In Scope 13](#_Toc14435667)

[2.5 Customer requirements 13](#_Toc14435668)

[2.6 Targeted customers 15](#_Toc14435669)

[2.7 Resource requirements 15](#_Toc14435670)

[2.7.1 Recommended customer resources 15](#_Toc14435671)

[2.7.2 Recommended partner resources 15](#_Toc14435672)

[3 Activity details 17](#_Toc14435673)

[3.1 Pre-engagement Call 17](#_Toc14435674)

[3.2 Prepare and send Microsoft Security Assessment Questionnaire 19](#_Toc14435675)

[3.3 Kick-off Meeting 20](#_Toc14435676)

[3.4 Customer Requirements and Strategy 22](#_Toc14435677)

[3.5 Component 1 - Secure Score Assessment 24](#_Toc14435678)

[3.5.1 Activity 1.1 - Readiness - Secure Score Overview 24](#_Toc14435679)

[3.5.2 Activity 1.2 - Hands-on - Secure Score Analysis and Report Creation 26](#_Toc14435680)

[3.6 Component 2 - Shadow IT Assessment 28](#_Toc14435681)

[3.6.1 Activity 2.1 - Readiness - Microsoft Cloud App Security Overview 28](#_Toc14435682)

[3.6.2 Activity 2.2 - Hands-on - Shadow IT Analysis and Report Creation 30](#_Toc14435683)

[3.7 Component 3 - Windows Security Assessment 32](#_Toc14435684)

[3.7.1 Activity 3.1 - Readiness - Microsoft Defender ATP Overview 32](#_Toc14435685)

[3.7.2 Activity 3.2 - Hands-on - Windows Security Analysis and Report Creation 34](#_Toc14435686)

[3.8 Component 4 - Attack Simulator Assessment 36](#_Toc14435687)

[3.8.1 Activity 4.1 - Hands-on - Attack Simulator Analysis and Report Creation 36](#_Toc14435688)

[3.9 Engagement Close-out 38](#_Toc14435689)

[4 Engagement Tools 40](#_Toc14435690)

[4.1 Microsoft Secure Score 40](#_Toc14435691)

[4.1.1 Hands-on Delivery Guidance 40](#_Toc14435692)

[4.1.2 Technical Preparation 43](#_Toc14435693)

[4.2 Microsoft Cloud App Security 48](#_Toc14435694)

[4.2.1 Hands-on Delivery Guidance 48](#_Toc14435695)

[4.2.2 Technical Preparation 50](#_Toc14435696)

[4.3 Microsoft Defender ATP and Windows Secure Score 51](#_Toc14435697)

[4.3.1 Hands-on Delivery Guidance 51](#_Toc14435698)

[4.3.2 Technical Preparation 52](#_Toc14435699)

[4.4 Attack Simulator 54](#_Toc14435700)

[4.4.1 Hands-on Delivery Guidance 54](#_Toc14435701)

[4.4.2 Technical Preparation 54](#_Toc14435702)

[Appendix A - Setup and preparation Microsoft Security Assessment Demo 56](#_Toc14435703)

[Appendix B - Readiness and technical content 57](#_Toc14435704)

[Appendix C - Microsoft Security Assessment Toolkit content 58](#_Toc14435705)

#### Version History

|  |  |  |
| --- | --- | --- |
| Version | Changes | Date |
| 1.0 | Initial Release | 12-Apr-2017 |
| 1.1 | Minor typo and grammar corrections  Changes to remediation instructions  Updated readiness file names  Updated header URL  Added additional information on providing the security assessment as a managed security service | 16-Jun-2017 |
| 1.2 | Changed name of the assessment to the Microsoft Security Assessment to align with the change to Microsoft Secure Score.  Added optional assessment component for:   * Shadow IT Overview to provide visibility into Shadow IT usage * Attack Simulations to test spear phishing and password attacks * Windows Secure Score using Microsoft Defender ATP to assess client security controls   Added readiness to cover Microsoft 365 security products. | 01-Jul-2018 |
| 1.3 | Minor changes to align with the updates to Secure Score.   * Updates to the Remediation Checklist Tool   Additional information on how to store and query Secure Score data using Azure Log Analytics, including using data as part of an Azure or Power Bi dashboard | 31-Oct-2018 |
| 2.0 | Updated engagement structure and flow of engagement and guidance. | 01-Jul-2019 |

#### Disclaimer

© 2019 Microsoft Corporation. All rights reserved. This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. Microsoft 365 customers and partners may copy, use and share these materials for planning, deployment and operation of Microsoft 365 features.

#### We look forward to your feedback!

|  |  |
| --- | --- |
| Microsoft 365 Security and Compliance Partners | Thank you for your continued trust and partnership. The resources within this toolkit will be iteratively improved upon based on product releases as well as direct feedback from delivered engagements. We encourage you to provide feedback to help us improve our products and toolkits. Please use the feedback process available through following web site: <https://aka.ms/securityassessmentfeedback> |

# Introduction

This document contains the delivery guidance for the Microsoft Security Assessment Toolkit. The Microsoft Security Assessment is a structured engagement which includes four separate assessment components to help evaluate and prioritize security recommendations for an organization. The Microsoft Security Assessment offering has been designed to help you as a partner create and present a customized, prioritized and actionable roadmap based on the recommendations to your customers.

The purpose of this document is to provide guidance on how to deliver the Microsoft Security Assessment, including details about the resources included within the toolkit.

**Important.**

*We advise you to customize the resources within this toolkit to align to you as a partner, your own value proposition, workflows, delivery methodologies, related work streams and offerings.*

The Microsoft Security Assessment toolkit includes following assessment components:

You can use any combination of above assessment components to build a custom Microsoft Security Assessment engagement for your customer dependent on their requirements and priorities.

## Delivery Guide

This delivery guide describes a multi-step engagement that a partner can offer to a customer to help them evaluate and prioritize security controls for their Microsoft 365 deployment. For each step, this guide provides execution guidance and tips, discusses resources and deliverables while focusing on a successful engagement and valuable outcome.

## Audience

The document is primarily intended to be used by Microsoft Security Partners as preparation for customizing and delivering the Microsoft Security Assessment.

# Engagement overview - high level

On a high level, the activities for the Microsoft Security Assessment engagement can be categorized into three stages. The illustration below depicts these three stages and their associated activities. In the upcoming paragraphs the individual activities will be further described and detailed.



Week 1 - Pre-engagement

The engagement will start with a remote preparation meeting. This customer pre-engagement call typically is an online meeting organized two weeks prior to the actual on-site activities. During this online meeting, the partner will introduce the customer to the Microsoft Security Assessment engagement, discuss the upcoming activities and align expectations and timelines. For customers that have had no prior exposure to the products and tools that will be used during the engagement, it is possible to include a high-level introduction and demo explaining the features and functionality. At the end of the pre-engagement call, the customer will be provided with the Microsoft Security Assessment questionnaire and is asked to respond to the questions in the week following the call.

Week 2- Prepare for on-site activities

The second week of the engagement will be used by the customer to answer the questions from the Microsoft Security Assessment questionnaire and prepare for the on-site activities as discussed during the pre-engagement call.

You need to work with the customer to complete technical preparation work for the assessment components you in include as part of the Microsoft Security Assessment:

* Secure Score - Export Secure Score data
* Shadow IT - Create snapshot report
* Windows Security - Configure MDATP Agent
* Attack Simulator - Prepare email templates and password lists

Week 3 - On-site activities

In the third week of the engagement the partner team will be on-site at the customer to work with them to perform the Microsoft Security Assessment. The on-site activities will consist of strategy and readiness workshops, hands-on assessments and an engagement close-out meeting where you would report back the results of the assessment. The model in which the customer engages with the partner can be fully customized depending on the customers’ needs and requirements. The next paragraph will describe the modular delivery model for the activities in week 3 and provides four example delivery schedules that can be used as-is or further customized for better alignment.

## Week 3 - modular delivery model

The Microsoft Security Assessment engagement is developed in a modular setup. Each assessment component focusses on a specific technology, functionality or service and encompasses both readiness and hands-on activities. The illustration below provides an overview of all engagement components and their associated activities.



All activities outlined in the illustration above are described in detail in chapter *3 Activity details* . Per activity relevant information such as objectives, deliverables, duration, preparation, etc. is provided together with applicable delivery guidance.

Customizing the delivery model.  
The delivery model for the Microsoft Security Assessment engagement in week 3 can be customized to better align with the customer’s needs, requirements and the specific assessment components that they would like to include as part of the assessment. The next paragraphs provide four example delivery schedules that, if needed, can be further customized prior to the delivery of the Microsoft Security Assessment engagement:

* Secure Score Assessment,focuses on analyzing and prioritizing the Secure Score security controls
* Secure Score and Shadow IT Assessments,also includes the Shadow IT Assessment component to provide visibility into Shadow IT usage
* Secure Score, Shadow IT and Windows Security Assessments,also includes the Windows Security Assessment component to provide visibility into the current security posture of Windows 10 clients
* Secure Score, Shadow IT, Windows Security and Attack Simulator Assessments,also includes the Attack Simulator Assessment component to analyze user preparedness for spear phishing attacks and user password quality

### Secure Score Assessment - Sample delivery schedule

The Secure Score Assessment schedule focuses on analyzing and prioritizing the Secure Score security controls.



### Secure Score and Shadow IT Assessments - Sample delivery schedule

This sample delivery schedule also includes the Shadow IT Assessment component to provide visibility into Shadow IT usage.   


### Secure Score, Shadow IT and Windows Security Assessments - Sample delivery schedule

This sample delivery schedule also includes the Windows Security Assessment component to provide visibility into the current security posture of Windows 10 clients.  


### Secure Score, Shadow IT, Windows Security and Attack Simulator Assessments - Sample delivery schedule

This sample delivery schedule also includes the Attack Simulator Assessment component to analyze user preparedness for spear phishing attacks and user password quality.   


## Estimated engagement partner effort

The table below provides a high level estimate of the partner effort for the activities of the overall engagement as outlined in paragraph 2.1.4 Secure Score, Shadow IT, Windows Security and Attack Simulator Assessments - Sample delivery schedule. The numbers provided are to be considered as indicative and can change as a result of customization of the delivery schedule and the individual activities.



**Project/engagement management**  
The typical effort for the Microsoft Security Assessment engagement when including all components is estimated between 40-60 hrs. The estimates do not include time for optional (external) Project/Engagement management resources. If an (external) project/engagement manager is required, additional hours should be added accordingly.

Note that the engagement can be considerably longer under certain conditions. For example, following conditions are likely to require additional time to be added to the engagement:

* The customer has more than a single tenant and would like to assess Secure Score across all their tenants which will have an impact on the Secure Score Assessment component
* The customer would like to include Shadow IT data from multiple user locations and/or firewall/proxy solutions which will have an impact on the Shadow IT Assessment component
* The customer would like to include more than a subset of Windows 10 clients which will have an impact on the Windows Security Assessment component
* The customer would like to create multiple email templates to target individual user groups for the email phishing simulation which will have an impact on the Attack Simulator Assessment component

We recommend that you discuss above conditions with the customer during the pre-engagement call so that you can add additional time if required.

## Engagement Objectives

The objectives for the Microsoft Security Assessment engagement are:

* Analyze requirements, gain a thorough understanding of the customers business and technical requirements and how they drive security objectives and requirements
* Training and knowledge sharing,throughout the engagement, provide recommended practices and deliver training on the assessment tools
* Analyze security posture, for each assessment component, analyze and prioritize security posture and create a results/roadmap presentation with recommendations
* Present results, recommendations and roadmap, provide a prioritized and actionable Microsoft 365 security roadmap based on customer security objectives, requirements and security posture

## Engagement scoping

### In Scope

The standard scope of the engagement includes:

* Gain a mutual understanding of cloud security objectives and requirements
* Provide guidance, recommendations and best practices on how to successfully implement Microsoft 365 security features
* Provide a prioritized and actionable Microsoft 365 security roadmap.
* Map Microsoft 365 security capabilities to customer security objectives and requirements
* Include one or more assessment components with following scope:
  + Secure Score Assessment,to analyze and prioritize Secure Score security controls
  + Shadow IT Assessments,to provide visibility into Shadow IT usage
  + Windows Security Assessments,to provide visibility into the current security posture of Windows 10 clients
  + Attack Simulator Assessments,to analyze user preparedness for spear phishing attacks and user password quality

## Customer requirements

Successful delivery of the engagement is dependent on the customer's involvement in all aspects of the engagement. The customer must ensure that accurate and complete information is provided in a timely fashion as needed, that appropriate resources are committed, and that any activities are completed in a timely and effective manner. The customer will need to perform the tasks, provide the resources, and take ownership of following activities:

**Note***This section describes the customer requirements applicable to the overall engagement. Additional requirements specific to the activities will be outlined in the individual sections below.*

* The customer will need to provide adequate access to the necessary personnel needed to successfully complete the engagement including:
  1. A customer project manager responsible for the overall coordination and for scheduling logistics
  2. IT object owners for identity and security during all phases of the assessment
  3. Executive Sponsor
* The Customer will provide the following to the partner resource:
* Access to any relevant documentation
* Network connectivity, adequate workspace, parking permits, building access and appropriate identification badges within the first day of project the on-site workshop
* Appropriate-sized room with whiteboard and projector for knowledge transfer sessions
* Work together with you as the partner to complete required technical preparation work prior to the on-site workshop
  + Secure Score - Export Secure Score data
  + Shadow IT Assessment - Create snapshot report
  + Windows Security Assessment - Configure MDATP Agent
  + Attack Simulator Assessment - Prepare email templates and password lists

## Targeted customers

At the minimum level, customers who have already decided to adopt the cloud and Office 365 and have an Office 365 tenant already in place. Ideally, customers who have deployed Microsoft 365 including EMS and Windows 10.

## Resource requirements

### Recommended customer resources

**Executive Sponsor**

* Owns the business case
* Keeps project aligned with organization's strategy and portfolio direction
* Governs project risk
* Focuses on realization of benefits
* Provides assurance
* Suggested candidates: CSO, CISO, CEO, CFO, CIO or CTO,

**Architects**

* IT
* Security
* Network
* Client Infrastructure

**Administrators**

* Security
* Network
* Client Infrastructure

**Microsoft 365 Tenant Administrators**

**Security Operations**

### Recommended partner resources

**Security Architect**

* Strong cybersecurity background and knowledge
* Good understanding of Microsoft 365 and the security components of Microsoft 365
* Good understanding of Microsoft Secure Score and how to use it to assess and resolve the assessed security controls
* Has prior design experience with the Microsoft security products including:
  + Microsoft Cloud App Security (CAS)
  + Microsoft Defender ATP (MDATP)
  + Microsoft 365 Advanced Threat Protection and Threat Investigation and Response

**Security Consultant**

* Strong cybersecurity background and knowledge
* Good understanding of Microsoft 365 and the security components of Microsoft 365
* Good understanding of Microsoft Secure Score and how to use it to assess and resolve the assessed security controls
* Has hands-on deployment experience with the Microsoft security products including:
  + Microsoft Cloud App Security (CAS)
  + Microsoft Defender ATP (MDATP)
  + Microsoft 365 Advanced Threat Protection and Threat Investigation and Response

**Project or Engagement Manager (optional)**

* Basic understanding of cybersecurity
* Basic understanding of Microsoft 365 security products
* Experience managing security engagements

# Activity details

## Pre-engagement Call

|  |  |
| --- | --- |
|  | The pre-engagement call typically is an online meeting organized two weeks prior to the actual on-site activities. During this online meeting, the partner will introduce the customer to the Microsoft Security Assessment engagement, discuss the upcoming activities, align expectations and establish timelines. For customers that have had no prior exposure to the products and tools that will be used during the engagement, it is possible to include a high-level introduction and demo explaining features and functionality. At the end of the pre-engagement call, the customer will be provided with the Microsoft Security Assessment questionnaire and is asked to respond to the questions in the week following the call. |

##### Objectives

The objective for the pre-engagement call is to provide an overview of the engagement and agree on the scope, schedule and required resources, particularly the following:

* Introduce the team to the customer and set the stage for the project
* Introduce the Microsoft Security Assessment engagement.
* Describe and discuss upcoming activities
* Align expectations and timelines
* Allocate resources
* Discuss the engagement scope
* Confirm information about the customer’s requirements

##### Format

The pre-engagement call will be delivered as an online meeting

##### Customer resources

* Executive Sponsor
* IT Object Owner
* Security Team

##### Partner resources

* Security Architect/Engineer
* Engagement Manager

##### Supporting materials

* 01 - Microsoft Security Assessment - pre-engagement call.pptx

##### Preparation

Prior to delivering the pre-engagement call, the partner resource leading the meeting will need to familiarize him/herself with:

* The overall engagement format of the Microsoft Security Assessment engagement
* The customer and their organizational structure. (Make sure you research any previous engagements that your organization have delivered to the customer)
* The customer's requirements
* The presentation contents

If a demo is included in the pre-engagement call, the partner resource should prepare for delivering a demo by using either a partner owned demo/lab environment or with the use of the click-through demo. For setup instructions refer to *Appendix A -Setup and preparation Microsoft Security Assessment* Demo

**Important**

*It is important that you adapt the content for your audience. For example, if you are presenting the pre-engagement presentation to a non-technical audience, such as the customer stakeholders and/or project/engagement managers, you can hide the slides demonstrating the tools used as part of the engagement.*

##### Pre-requisites

No Pre-requisites exist.

##### Deliverables

The deliverables of the pre-engagement call are defined as:

* Confirmed schedule with attendee list for sessions for the on-site workshop
* Agreed date for the questionnaire to be completed
* Agreed owner for the technical preparation work
* Agreed date for the technical preparation work
* Agreed date, logistics and attendee list for the on-site workshop

These deliverables will serve as input to the next steps.

##### Guidance

Deliver the meeting using the speaker notes and guidance provided in the *01 - Microsoft Security Assessment - pre-engagement call.pptx* deck.

If a demo is part of the pre-engagement call refer to *Appendix A -Setup and preparation Microsoft Security Assessment* Demo for guidance and setup instructions.

##### Background reading

* To prepare for the delivery of the Microsoft Security Assessment Toolkit, refer to *Appendix B - Readiness and technical content* for links to relevant on-line learning content.

##### Duration and effort

* Preparation 1 Hrs.
* Delivery 1 Hrs.

## Prepare and send Microsoft Security Assessment Questionnaire

|  |  |
| --- | --- |
|  | To be able to prepare for the on-site activities it is important to have a good understanding of the customers production environment. The Microsoft Security Assessment toolkit comes with a questionnaire that the customer will be asked to complete.  Following the pre-engagement call this questionnaire will be sent to the customer. |

##### Objectives

The objectives for these activities are:

* Customize and prepare the Microsoft Security Assessment questionnaire
* Send the questionnaire to the customer

##### Supporting materials

* 02 - Microsoft Security Assessment - ACTION REQUIRED.msg
* 03 - Microsoft Security Assessment - Customer Questionnaire.docx

##### Preparation

Prior to sending the questionnaire to the customer the partner consultant should customize the questions based on the information obtained from the pre-engagement call.

##### Pre-requisites

The activities outlined in paragraph *3.1 Pre-engagement* should be completed prior to starting this activity.

##### Deliverables

* Microsoft Security Assessment Customer questionnaire customized and sent to customer
* Microsoft Security Assessment Customer questionnaire completed by customer

##### Guidance

* Open the *02 - Microsoft Security Assessment - ACTION REQUIRED.msg* e-mail template included in the toolkit
* Customize the message, and include an updated schedule reflecting the included assessment components
* Attach the updated and customized *03 - Microsoft Security Assessment - Customer Questionnaire.docx* file
* Send to the customer

##### Duration and effort

* Preparation 1 Hrs.

## Kick-off Meeting

|  |  |
| --- | --- |
|  | If you have a subset of the customer team present at the pre-engagement call, we highly recommend that you start the on-site workshop with a kick-off meeting where you go through the overview of the engagement to the entire team using the pre-engagement call presentation. This will ensure that all project team members understand the objective and contents of the engagement. During this meeting, the partner will introduce the customer to the Microsoft Security Assessment engagement, discuss the upcoming activities, align expectations and establish timelines. For customers that have had no prior exposure to the products and tools that will be used during the engagement, it is possible to include a high-level introduction and demo explaining features and functionality. |

##### Objectives

The objective for the kick-off meeting is to provide an overview of the engagement and agree on the scope, schedule and required resources, particularly the following:

* Introduce the team to the customer and set the stage for the project
* Introduce the Microsoft Security Assessment engagement.
* Describe and discuss upcoming activities
* Align expectations and timelines
* Allocate resources
* Discuss the engagement scope
* Confirm information about the customer’s requirements

##### Format

The kick-off meeting will be delivered as an on-site workshop.

##### Customer resources

* Executive Sponsor
* IT Object Owner
* Security Team

##### Partner resources

* Security Architect/Engineer
* Engagement Manager

##### Supporting materials

* 01 - Microsoft Security Assessment - pre-engagement call.pptx

##### Preparation

Prior to delivering the pre-engagement call, the partner resource leading the meeting will need to familiarize him/herself with:

* The overall engagement format of the Microsoft Security Assessment engagement
* The customer and their organizational structure. (Make sure you research any previous engagements that your organization have delivered to the customer)
* The customer's requirements
* The presentation contents

If a demo is included in the pre-engagement call, the partner resource should prepare for delivering a demo by using either a partner owned demo/lab environment or with the use of the click-through demo. For setup instructions refer to *Appendix A -Setup and preparation Microsoft Security Assessment* Demo

##### Pre-requisites

No Pre-requisites exist.

##### Deliverables

The deliverables of the kick-off meeting are defined as:

* Agree on any updates to scheduling and/or attendee list for sessions for the on-site workshop

These deliverables will serve as input to the next steps.

##### Guidance

Deliver the meeting using the speaker notes and guidance provided in the *01 - Microsoft Security Assessment - pre-engagement call.pptx* deck.

If a demo is part of the pre-engagement call refer to *Appendix A -Setup and preparation Microsoft Security Assessment* Demo for guidance and setup instructions.

##### Background reading

* To prepare for the delivery of the Microsoft Security Assessment Toolkit, refer to *Appendix B - Readiness and technical content* for links to relevant on-line learning content.

##### Duration and effort

* Preparation 1 Hrs.
* Delivery 1 Hrs.

## Customer Requirements and Strategy

|  |  |
| --- | --- |
|  | **Description**  During this session we will go through the Microsoft Security Assessment Questionnaire that the customer has filled out before the on-site workshops. The answers will be discussed, and unclear or missing information will be updated or added. |

##### Objectives

The objective for this activity is to make sure that all questions within the Microsoft Security Assessment questionnaire have been sufficiently answered and understood.

##### Format

This module will be delivered as an on-site workshop.

##### Customer resources

* Engagement Stakeholder(s)
* Service Owner(s)
* SMEs (Subject Matter Experts)

##### Partner resources

* Security Architect/Engineer

##### Supporting materials

* 03 - Microsoft Security Assessment - Customer Questionnaire.docx

##### Preparation

Prior to delivering this workshop, the partner resource will need to:

* Analyze the answers in the Microsoft Security Assessment Questionnaire
* Mark any questions for follow up that are incomplete or where additional details are needed

##### Pre-requisites

The activities included in:

* Prepare and send Microsoft Security Assessment Questionnaire should be completed prior to starting this activity.
* The Microsoft Security Assessment Questionnaire should be completed by the customer.

##### Deliverables

For this activity the following deliverables have been defined:

* Completed *03 - Microsoft Security Assessment - Customer Questionnaire.docx*
* Session notes

##### Guidance

* Discuss questions that have not been filled in, are incomplete or do not contain enough information
* Update the *03 - Microsoft Security Assessment - Customer Questionnaire.docx* as needed

##### Background reading

* To prepare for the delivery of the Microsoft Security Assessment Toolkit, refer to *Appendix B - Readiness and technical content* for links to relevant on-line learning content.

##### Duration and effort

* Preparation: 1 Hrs.
* Delivery: 1 Hrs.

## Component 1 - Secure Score Assessment

|  |  |
| --- | --- |
|  | The Secure Score Assessment component consists of two activities:   * Readiness, providing guidance on Microsoft Secure Score * Hands-on, Secure Score Analysis and Report Creation   Depending on the customers intentions and requirements, the readiness activities can be modified or removed from the schedule. |

### Activity 1.1 - Readiness –Secure Score Overview

|  |  |
| --- | --- |
|  | The Secure Score Overview session provides an overview of Microsoft Secure Score and how to use it to analyze current security posture in Microsoft 365. |

##### Objectives

The objectives for this activity are to provide information on how Microsoft Secure Score can be used to assess security posture of an organization, covering following topics:

* Educate the customer on how Secure Score can be used to get an insight into their security position by analyzing the recommended actions provided by Microsoft Secure Score
* Discuss how the Secure Score data can be accessed through the Secure Score API
* Demonstrate the functionality of Secure Score using your own demo environment Assessment
* Demonstrate the remediation checklist tool which is included as part of the Microsoft Security Assessment Toolkit

##### Format

This activity will be delivered as an on-site workshop.

##### Customer resources

* Service Owner(s)
* SMEs (Subject Matter Experts)

##### Partner resources

* Security Architect/Engineer

##### Supporting materials

* *05 - Microsoft Security Assessment - Secure Score Overview.pptx*
* *04 - Microsoft Security Assessment - Remediation Checklist Tool.xlsx*

##### Preparation

Prior to delivering this workshop, the partner resource will need to:

* Familiarize him/herself with the *05 - Microsoft Security Assessment - Microsoft Secure Score Overview.pptx* readiness presentation that will be used during the workshop
* Customize the *05 - Microsoft Security Assessment - Microsoft Secure Score Overview.pptx* readiness presentation to align with the customers’ expectations and needs.
* Familiarize him/herself with the *04 - Microsoft Security Assessment - Remediation Checklist Tool.xlsx* spreadsheetthat will be used during the workshop

##### Pre-requisites

* The activities included in *Customer Requirements and Strategy* should be completed prior to starting this activity.

##### Deliverables

For this activity the following deliverables have been defined:

* Understanding of Secure Score and how to use Secure Score to analyze and prioritize improvement actions
* Understanding how to export Secure Score data
* Understanding of how the Remediation Checklist Tool will be used as part of the engagement
* Session notes

##### Guidance

* Delivery guidance for this session can be found in the speaker notes of the related readiness presentation specified in Appendix B - Readiness and technical content

##### Background reading

* To prepare for the delivery of the Microsoft Security Assessment Toolkit, refer to *Appendix B - Readiness and technical content* for links to relevant on-line learning content.

##### Duration and effort

* Preparation: 1 Hrs.
* Delivery: 1 Hrs.

### Activity 1.2 - Hands-on - Secure Score Analysis and Report Creation

|  |  |
| --- | --- |
|  | The Secure Score Analysis and Report Creation session is used to analyze and prioritize the Secure Score improvement actions, documenting the results as part of the included remediation tool and the engagement close-out and results presentation. |

##### Objectives

The objectives for this activity are:

* Guided exploration of Secure Score and the recommended improvement actions making sure you cover:
  + An explanation of each recommended action
  + The Microsoft Rank vs the customers own priority
  + User impact and implementation cost
* Updated Remediation Checklist Tool including custom priority and task or project groupings
* Updated Secure Score results and roadmap section within the close-out presentation considering the potential for risk, difficultly of implementation, and impact ratings suggested by each Microsoft Secure Score improvement action.

##### Format

This activity will be delivered in a hands-on format.

##### Customer resources

* Service Owner(s)
* SMEs (Subject Matter Experts)

##### Partner resources

* Security Architect/Engineer

##### Supporting materials

* *00 - Microsoft Security Assessment Toolkit - Delivery Guide.docx*
* *04 - Microsoft Security Assessment - Remediation Checklist Tool.xlsx*

##### Preparation

Prior to delivering this workshop, the partner resource will need to:

* Familiarize him/herself with the *08 - Microsoft Security Assessment - Engagement Close-out.pptx* deck
* Customize the *08 - Microsoft Security Assessment - Engagement Close-out.pptx* deck to align with the customers’ expectations and needs.
* Familiarize him/herself with Microsoft Secure Score and included improvement actions
* Understand how to export recommended improvement actions from Secure Score
* Understand how to use the *05 - Microsoft Security Assessment - Remediation Tool.xlsx* tool

##### Pre-requisites

* Technical preparation work for Secure Score, as outlined in paragraph 4.1 Microsoft Secure Score, completed prior to the on-site workshop
* The activities outlined in paragraph *3.5.1 Activity 1.1 - Readiness - Secure Score Overview* should be completed prior to starting this activity.
* Access to the Microsoft Secure Score portal

**Important**

*The pre-requisites must be confirmed with the customer during the pre-scoping call or pre-engagement call.*

##### Deliverables

For this activity the following deliverables have been defined:

* All Microsoft Secure Score actions analyzed, prioritized and documented as part of the *04 - Microsoft Security Assessment - Remediation Checklist Tool.xlsx* tool
* Updated and fully customized *08 - Microsoft Security Assessment - Engagement Close-out.pptx* presentation

##### Guidance

* Delivery guidance for this session can be found in paragraph 4.1 Microsoft Secure Score

##### Background reading

* To prepare for the delivery of the Microsoft Security Assessment Toolkit, refer to *Appendix B - Readiness and technical content* for links to relevant on-line learning content.

##### Duration and effort

* Preparation: 1 Hrs.
* Delivery: 3 Hrs.

## Component 2 - Shadow IT Assessment

|  |  |
| --- | --- |
|  | The Shadows IT Assessment component consists of two activities:   * **Readiness,** providing guidance on Microsoft Could App Security * **Hands-on,** Shadow IT Analysis and Report Creation   Depending on the customers intentions and requirements, the readiness activities can be modified or removed from the schedule. |

### Activity 2.1 - Readiness - Cloud App Security Overview

|  |  |
| --- | --- |
|  | The Microsoft Cloud App Security Overview session provides an overview of Microsoft Cloud App security and how to use it to analyze Shadow IT usage. |

##### Objectives

The objectives for this activity are to provide information on how Microsoft Cloud App Security can be used to assess Shadow IT of an organization, covering following topics:

* Educate the customer on the challenges behind adoption of cloud applications and services, Shadow IT being one of them.
* Present Cloud App Security as one of many elements of a holistic approach that Microsoft takes towards cloud security with the Enterprise Mobility & Security suite.
* Describe the Cloud App Security architecture and functionality with an emphasis on the Discovery aspect, as that is the function used in the Shadow IT Assessment.
* Make sure that Information Protection, Threat Detection and In-Session Control aspects are well understood by the customer, as these might be part of the Cloud Usage Visibility and Control Roadmap, one of the deliverables of the engagement.

##### Format

This activity will be delivered as an on-site workshop.

##### Customer resources

* Service Owner(s)
* SMEs (Subject Matter Experts)

##### Partner resources

* Security Architect/Engineer

##### Supporting materials

* *06 - Microsoft Security Assessment - Cloud App Security Overview.pptx*

##### Preparation

Prior to delivering this workshop, the partner resource will need to:

* Familiarize him/herself with the *06 - Microsoft Security Assessment – Cloud App Security Overview.pptx* readiness presentation that will be used during the workshop
* Customize the *06 - Microsoft Security Assessment – Cloud App Security Overview.pptx* readiness presentation to align with the customers’ expectations and needs.

##### Pre-requisites

* The activities included in *Customer Requirements and Strategy* should be completed prior to starting this activity.

##### Deliverables

For this activity, the following deliverables have been defined:

* High-level understanding of Microsoft Cloud App Security
* Session notes

##### Guidance

* Delivery guidance for this session can be found in the speaker notes of the related readiness presentation specified in Appendix B - Readiness and technical content

##### Background reading

* To prepare for the delivery of the Microsoft Security Assessment Toolkit, refer to *Appendix B - Readiness and technical content* for links to relevant on-line learning content.

##### Duration and effort

* Preparation: 1 Hrs.
* Delivery: 1 Hrs.

### Activity 2.2 - Hands-on - Shadow IT Analysis and Report Creation

|  |  |
| --- | --- |
|  | The Shadow IT Analysis and Report Creation session is used to analyze shadow IT activities from the customer’s users, documenting the results as part of the engagement close-out and results presentation. |

##### Objectives

The objectives for this activity are:

* Guided exploration of the Cloud App Security Cloud Discovery Reports including exploration of specific cloud usage in the Cloud App Security portal. Make sure following reports under the Cloud Discovery dashboard are covered:
  + Discovered apps
  + Discovered resources
  + IP addresses
  + Users
  + Machines
* Updated Shadow IT results and roadmap section within the close-out presentation

##### Format

This activity will be delivered in a hands-on format.

##### Customer resources

* Service Owner(s)
* SMEs (Subject Matter Experts)

##### Partner resources

* Security Architect/Engineer

##### Supporting materials

* *00 - Microsoft Security Assessment Toolkit - Delivery Guide.docx*

##### Preparation

Prior to delivering this workshop, the partner resource will need to:

* Familiarize him/herself with *08 - Microsoft Security Assessment - Engagement Close-out.pptx* deck
* Customize *08 - Microsoft Security Assessment - Engagement Close-out.pptx* deck to align with the customers’ expectations and needs.
* Familiarize him/herself with Cloud App Security and specifically the Cloud Discovery features of Cloud App Security

##### Pre-requisites

* Technical preparation work for Shadow IT, as outlined in paragraph 4.3 Microsoft Cloud App Security, completed prior to the on-site workshop
* The activities outlined in paragraph *3.6.1 Activity 2.1 - Readiness - Microsoft Cloud App Security Overview* should be completed prior to starting this activity.
* Access to the Cloud App Security portal

**Important**

*The pre-requisites must be confirmed with the customer during the pre-scoping call or pre-engagement call.*

##### Deliverables

For this activity the following deliverables have been defined:

* Updated and fully customized *08 - Microsoft Security Assessment - Engagement Close-out.pptx* presentation

##### Guidance

* Delivery guidance for this session can be found in paragraph *4.3 Microsoft Cloud App Security*

##### Background reading

* To prepare for the delivery of the Microsoft Security Assessment Toolkit, refer to *Appendix B - Readiness and technical content* for links to relevant on-line learning content.

##### Duration and effort

* Preparation: 1 Hrs.
* Delivery: 3 Hrs.

## Component 3 - Windows Security Assessment

|  |  |
| --- | --- |
|  | The Windows Security Assessment component consists of two activities:   * Readiness, providing guidance on Microsoft Defender ATP * Hands-on, Windows Security Analysis and Report Creation   Depending on the customers intentions and requirements, the readiness activities can be modified or removed from the schedule. |

### Activity 3.1 - Readiness - Microsoft Defender ATP Overview

|  |  |
| --- | --- |
|  | The Microsoft Defender ATP Overview session provides an overview of Microsoft Defender ATP and how to use it to analyze Windows security posture. |

##### Objectives

The objectives for this activity are to provide information on how Microsoft Defender ATP can be used to prevent, detect, investigate and respond to advanced threats, covering following topics:

* Educate the customer on how Microsoft Defender ATP can be used to:
  + Reduce attack surface
  + Protect against emerging threats
  + Detect, investigate and respond to attacks
  + Improve security posture with Windows Secure Score
  + Effectively identifying, assessing, and remediating endpoint weaknesses using Microsoft Defender ATP Threat & Vulnerability Management
* Discuss how Microsoft Defender ATP data can be accessed through an API

##### Format

This activity will be delivered as an on-site workshop.

##### Customer resources

* Service Owner(s)
* SMEs (Subject Matter Experts)

##### Partner resources

* Security Architect/Engineer

##### Supporting materials

* *07 - Microsoft Security Assessment - Microsoft Defender ATP Overview.pptx*

##### Preparation

Prior to delivering this workshop, the partner resource will need to:

* Familiarize him/herself with the *07 - Microsoft Security Assessment - Microsoft Defender ATP Overview.pptx* readiness presentation that will be used during the workshop
* Customize the *07 - Microsoft Security Assessment - Microsoft Defender ATP Overview.pptx* readiness presentation to align with the customers’ expectations and needs.

##### Pre-requisites

* The activities included in *Customer Requirements and Strategy* should be completed prior to starting this activity.

##### Deliverables

For this activity, the following deliverables have been defined:

* High-level understanding of Microsoft Defender ATP
* Session notes

##### Guidance

* Delivery guidance for this session can be found in the speaker notes of the related readiness presentation specified in Appendix B - Readiness and technical content

##### Background reading

* To prepare for the delivery of the Microsoft Security Assessment Toolkit, refer to *Appendix B - Readiness and technical content* for links to relevant on-line learning content.

##### Duration and effort

* Preparation: 1 Hrs.
* Delivery: 1 Hrs.

### Activity 3.2 - Hands-on - Windows Security Analysis and Report Creation

|  |  |
| --- | --- |
|  | The Windows Security Analysis and Report Creation session is used to analyze Windows security posture using Windows Secure Score and Threat and Vulnerability Management recommendations, documenting the results as part of the engagement close-out and results presentation. |

##### Objectives

The objectives for this activity are:

* Guided exploration of the Windows 10 improvement opportunities within Microsoft Defender ATP Secure Score
* Guided exploration of the Security recommendations within Microsoft Defender ATP Threat & Vulnerability Management
* Updated Windows Security results and roadmap section within the close-out presentation

##### Format

This activity will be delivered in a hands-on format.

##### Customer resources

* Service Owner(s)
* SMEs (Subject Matter Experts)

##### Partner resources

* Security Architect/Engineer

##### Supporting materials

* *00 - Microsoft Security Assessment Toolkit - Delivery Guide.docx*

##### Preparation

Prior to delivering this workshop, the partner resource will need to:

* Familiarize him/herself with *08 - Microsoft Security Assessment - Engagement Close-out.pptx* deck
* Customize *08 - Microsoft Security Assessment - Engagement Close-out.pptx* deck to align with the customers’ expectations and needs.
* Familiarize him/herself with Microsoft Defender ATP and specifically the Windows Secure Score features of Microsoft Defender ATP

##### Pre-requisites

* Technical preparation work for Windows Security, as outlined in paragraph 4.4 Windows Secure Score and Microsoft Defender ATP, completed prior to the on-site workshop
* The activities outlined in paragraph *3.7.1 Activity 2.1 - Readiness - Microsoft Defender ATP Overview* should be completed prior to starting this activity.
* Access to the Microsoft Defender ATP portal

**Important**

*The pre-requisites must be confirmed with the customer during the pre-scoping call or pre-engagement call.*

##### Deliverables

For this activity the following deliverables have been defined:

* Updated and fully customized *08 - Microsoft Security Assessment - Engagement Close-out.pptx* presentation

##### Guidance

* Delivery guidance for this session can be found in paragraph *4.4 Microsoft Defender ATP*

##### Background reading

* To prepare for the delivery of the Microsoft Security Assessment Toolkit, refer to *Appendix B - Readiness and technical content* for links to relevant on-line learning content.

##### Duration and effort

* Preparation: 1 Hrs.
* Delivery: 3 Hrs.

## Component 4 - Attack Simulator Assessment

|  |  |
| --- | --- |
|  | The Attack Simulator Assessment component consists of one activity:   * Hands-on, Attack Simulator Analysis and Report Creation |

### Activity 4.1 - Hands-on - Attack Simulator Analysis and Report Creation

|  |  |
| --- | --- |
|  | The Attack Simulator Analysis and Report Creation session is used to analyze results of simulated attacks against internal users and document their overall behavior against phishing campaign and evaluate passwords across the company. |

##### Objectives

The objectives for this activity are:

* Analyze and document the results of the simulated spear phishing attack
* Analyze and document the results of the simulated password attacks
* Document recommended readiness and/or related Microsoft security products and features that can be used to mitigate against spear phishing and password-based attacks as part of

##### Format

This activity will be delivered in a hands-on format.

##### Customer resources

* Service Owner(s)
* SMEs (Subject Matter Experts)

##### Partner resources

* Security Architect/Engineer

##### Supporting materials

* *00 - Microsoft Security Assessment Toolkit - Delivery Guide.docx*

##### Preparation

Prior to delivering this workshop, the partner resource will need to:

* Familiarize him/herself with *08 - Microsoft Security Assessment - Engagement Close-out.pptx* deck
* Customize *08 - Microsoft Security Assessment - Engagement Close-out.pptx* deck to align with the customers’ expectations and needs.
* Familiarize him/herself with Attack Simulator and how to customize email templates and prepare password lists to be used as part of the simulation

##### Pre-requisites

* Technical preparation work for Attack Simulator, as outlined in paragraph 4.5 Attack Simulator, completed prior to the on-site workshop
* The activities outlined in paragraph 3.8.1Activity 2.1 - Readiness - Attack Simulator Overviewshould be completed prior to starting this activity.
* Access to the Attack Simulator tool

**Important**

*The pre-requisites must be confirmed with the customer during the pre-scoping call or pre-engagement call.*

##### Deliverables

For this activity, the following deliverables have been defined:

* Updated and fully customized *08 - Microsoft Security Assessment - Engagement Close-out.pptx* presentation

##### Guidance

* Delivery guidance for this session can be found in paragraph 4.5 Attack Simulator

##### Background reading

* To prepare for the delivery of the Microsoft Security Assessment Toolkit, refer to *Appendix B - Readiness and technical content* for links to relevant on-line learning content.

##### Duration and effort

* Preparation: 1 Hrs.
* Delivery: 3 Hrs.

## Engagement Close-out

|  |  |
| --- | --- |
|  | The close-out meeting is where you will present the results, the assessment findings and recommendations, ensuring that the project team has a clear understanding of the results, and agreeing on a timeline for the roadmap recommendations. |

##### Objectives

The objectives for this activity are:

* Present an overview of the engagement
* Present the final deliverables
* Present the results and recommendations of the assessments
* Agree on a timeline for the roadmap recommendations
* To get the customers official acceptance of the deliverables and results
* To capture any potential outstanding activities and make sure that these are assigned to an owner
* To officially close the engagement

##### Format

This activity will be delivered as an on-site workshop.

##### Customer resources

* Engagement Stakeholder(s)
* Executive Sponsor
* Process Owners(s)
* Service Owner(s)
* SMEs (Subject Matter Experts)

##### Partner resources

* Security Architect/Engineer
* Engagement manager

##### Preparation

Prior to delivering this workshop, the partner resource will need to:

* Familiarize him/herself with *08 - Microsoft Security Assessment - Engagement Close-out.pptx* deck
* Customize *08 - Microsoft Security Assessment - Engagement Close-out.pptx* deck to align with the customers’ expectations and needs.

##### Pre-requisites

* All previous activities should be completed prior to starting this activity.

##### Deliverables

For this activity the following deliverables have been defined:

* Completed delivery of the *08 - Microsoft Security Assessment - Engagement Close-out.pptx* presentation

##### Guidance

* Delivery guidance for this session can be found in the speaker notes and hidden slides of the *08 - Microsoft Security Assessment - Engagement Close-out.pptx* presentation

##### Background reading

* To prepare for the delivery of the Microsoft Security Assessment Toolkit, refer to *Appendix B - Readiness and technical content* for links to relevant on-line learning content.

##### Duration and effort

* Preparation: 1 Hrs.
* Delivery: 1 Hrs.

# Engagement Tools

This section is for use by the partner technical specialists to learn how to use the tools as part of the Microsoft Security Assessment.

## Microsoft Secure Score

Microsoft Secure Score is a security analytics tool which calculates your tenant’s security score based on existing security settings and behaviors compares them to a baseline asserted by Microsoft. It’s a single tool which allows organizations to better understand their current security posture based on features that have been enabled within their Office 365 tenant. In addition, the Secure Score tool will allow you to quickly determine and prioritize improvement actions which can be implemented to reduce risk and will allow organizations to improve and track their Microsoft 365 security posture over time.

Microsoft Secure Score can also integrate with Microsoft Defender ATP and Windows Secure Score to allow assessment and prioritization of security controls for Windows 10 clients. To use Windows Secure Score, you must first enable Microsoft Defender ATP and onboard Windows 10 clients. See additional instructions in paragraph *4.4 Microsoft Defender ATP*.

Note that Secure Score does not account for all possible security controls. Additional improvement actions will be added to the Secure Score tool over time and this fact should be discussed with your customer as you propose the detect, protect, respond security lifecycle of managed services your organization may provide.

### Hands-on Delivery Guidance

The Hands-on Secure Score Assessment activity, delivered as on-site workshop, focuses on a guided exploration of Secure Score and preparing the final report and roadmap as part of the engagement close-out presentation.

* Ask the customer to sign-in to the Secure Score portal and assist (guide) the customer to explore the Overview dashboard and the Improvement actions tab.
* Provide an explanation for each improvement action, what the action does, what the impact to user and implementation cost means and if required, demonstrate the functionality and/or feature using a demo tenant
* Work together to analyze and prioritize the improvement actions from Microsoft Secure Score using the *04 - Microsoft Security Assessment - Remediation Checklist Tool.xlsx* spreadsheet*.* Add additional comments in the remediation tool as needed.
* Determine if a certain improvement action is a task or if it is something more complex, requiring a project to implement. If you determine that this should be a project, try to put a temporary name to the project. You can also group multiple tasks under one or more projects. For example, you can put all security actions related to monitoring and security dashboards under the "Microsoft 365 security dashboard" project name.
* Use the list of the prioritized Microsoft Secure Score improvement actions to update the Secure Score Results section within the close-out presentation, considering the potential for risk, difficultly of implementation, and impact ratings suggested by each Microsoft Secure Score action. Discuss the implications with your customer in depth as you prioritize and build the roadmap of improvement actions. Consider time frames to implement and provide a lifecycle of services to the customer.

**Important.**

*To assist with the prioritization of the improvement actions provided by Secure Score you will use the 04 - Microsoft Security Assessment - Remediation Checklist Tool.xlsx excel spreadsheet. Ask the customer to use the instructions in this section to export the improvement actions to CSV so that you can copy & paste the recommended improvement actions in to the 04 - Microsoft Security Assessment - Remediation Checklist Tool.xlsx excel spreadsheet.*

*Note that the Security Controls for Windows Secure Score are not currently integrated with Microsoft Secure Score and thus won’t be included in the exported security controls. This will be remedied in a future update.*

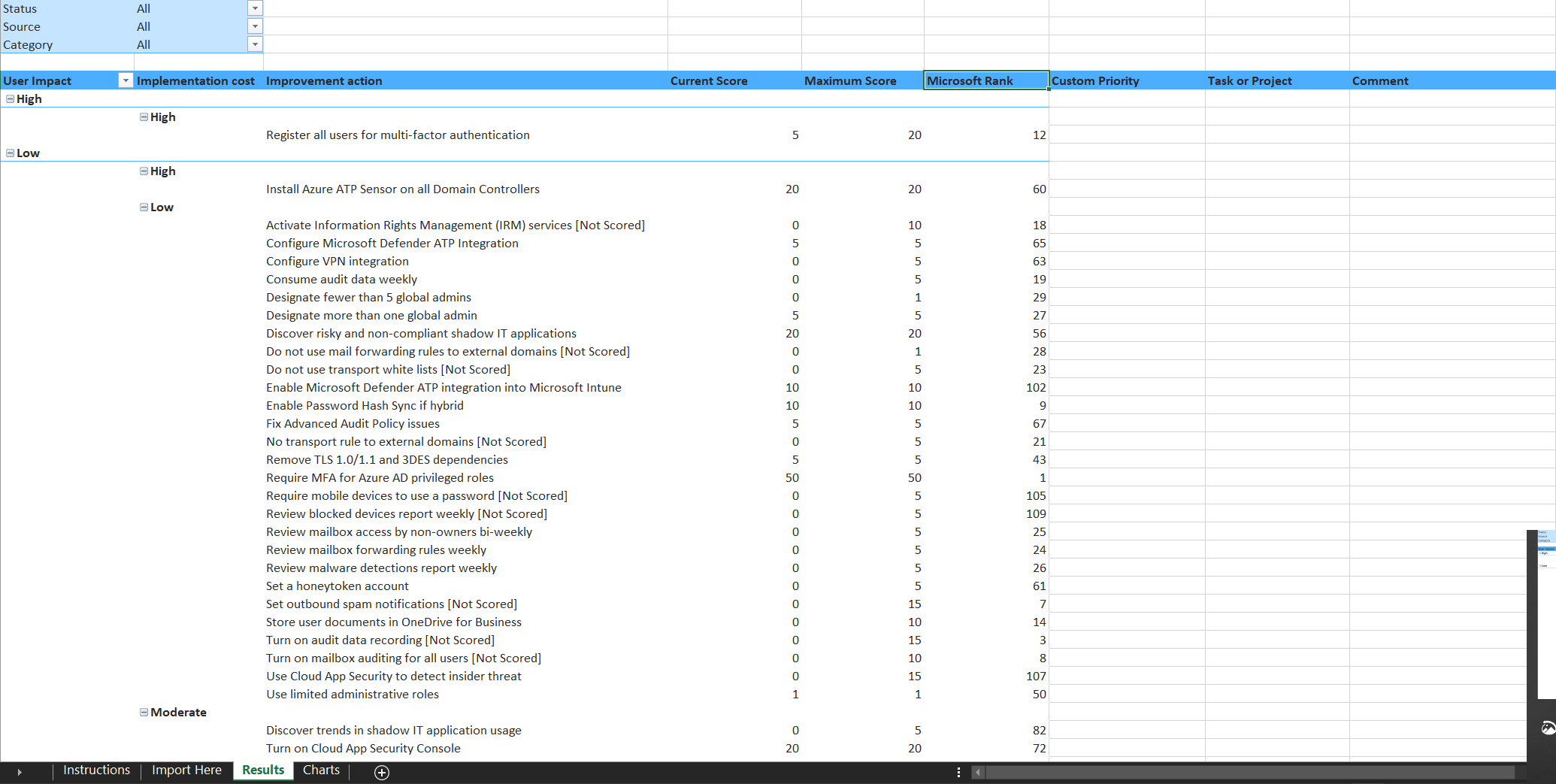
Make sure to consider any managed security services you could provide to close some of the gaps found as part of the security assessment. You should present proposed managed security services as part of the roadmap presentation.

If you don’t currently offer a managed security service, you should consider offering a Microsoft Security Assessment as a managed security service you provide to your customers. Providing an on-going security assessment as a managed security service is highly beneficial. For example, a security assessment as a managed service could provide opportunities to:

1. Help track Secure Score progress by providing enhanced reporting through Office or Power Bi dashboards
2. Advanced integration scenarios including SIEM integration, creating a single security dashboard using the Secure Score API
3. Help manage configuration creep and make sure security actions have been implemented correctly
4. Assess new security controls added to Secure Score
5. Keep an on-going relationship with the customer and their security staff

#### Remediation Checklist Tool

The primary tool to help you verify current Secure Score security actions and prioritize these into an actionable roadmap is the *04 - Microsoft Security Assessment - Remediation Checklist Tool.xlsx* excel spreadsheet.



Use following instructions to make use of the tool:

1. Import the Secure Score data exported by the customer into the tool.
2. As part of the workshops, work together with the customer to understand and prioritize the security actions.
3. Copy the prioritized set of security actions as well as the charts in to the *08 - Microsoft Security Assessment - Engagement Close-out.pptx* presentation which will be delivered at the end of the engagement.

The remediation checklist tools have following Excel tabs:

|  |  |
| --- | --- |
| Excel Tab | Description |
| Instructions | Instructions on how to use the tool. |
| Import Here | Control list data copied from the CSV file exported from Secure Score. |
| Results | Use the results tab to analyze and prioritize security actions as part of the workshops. The prioritized list of security actions needs to be copied to the *08 - Microsoft Security Assessment - Engagement Close-out.pptx* presentation. |
| Charts | The Charts tab contain basic charts, showing an overview of the Secure Score results. The charts need to be copied to the *08 - Microsoft Security Assessment - Engagement Close-out.pptx* presentation. |

The results tab is where you view and prioritize security actions. You can filter the security actions based on following categories:

* Status - Complete or incomplete
* Source - Source of the recommended improvement action
* Category - Category of the recommended improvement action as either Apps, Data, Device or Identity

You will see several columns within the Results tab. Note that all content except the Custom Priority, Task or Project and Comment columns will be automatically filled in after you have inserted the Secure Score data received from the customer and refreshed the data within the excel spreadsheet.

|  |  |
| --- | --- |
| Column | Description |
| User Impact | Impact of implemented security control on users:   * Low - little to no user productivity impact * Moderate - some user productivity impact |
| Implementation Cost | Approximate cost and complexity of implementing the security action:   * Low - Features that can typically be turned on without additional licenses * Moderate - Features that are complex to turn on and/or require additional licenses |
| Improvement Action | Name of improvement action. |
| Current Score | Current score for the improvement action. Can be between 1-50. Higher is better. |
| Maximum Score | Maximum possible score for the improvement action. |
| Microsoft Rank | Microsoft Security rank of each improvement action. |
| Custom Priority | Use this field to prioritize the security action. For example:   * Quick Wins (1-3 months) * 3-6 months * 6 months and beyond |
| Task or Project | If possible, determine if a certain improvement action is a task or if it is something more complex, requiring a project to implement. If you determine that this should be a project, try to put a temporary name to the project. You can also group multiple tasks under one or more projects. For example, you can put all improvement actions related to monitoring and security dashboards under the "Microsoft 365 security dashboard" project name. |
| Comment | Provide additional details if required. |

### Technical Preparation

Complete following tasks in order:

#### Validate License

To use Microsoft Secure Score, the customer needs an Office 365 Business Premium or Enterprise subscription.

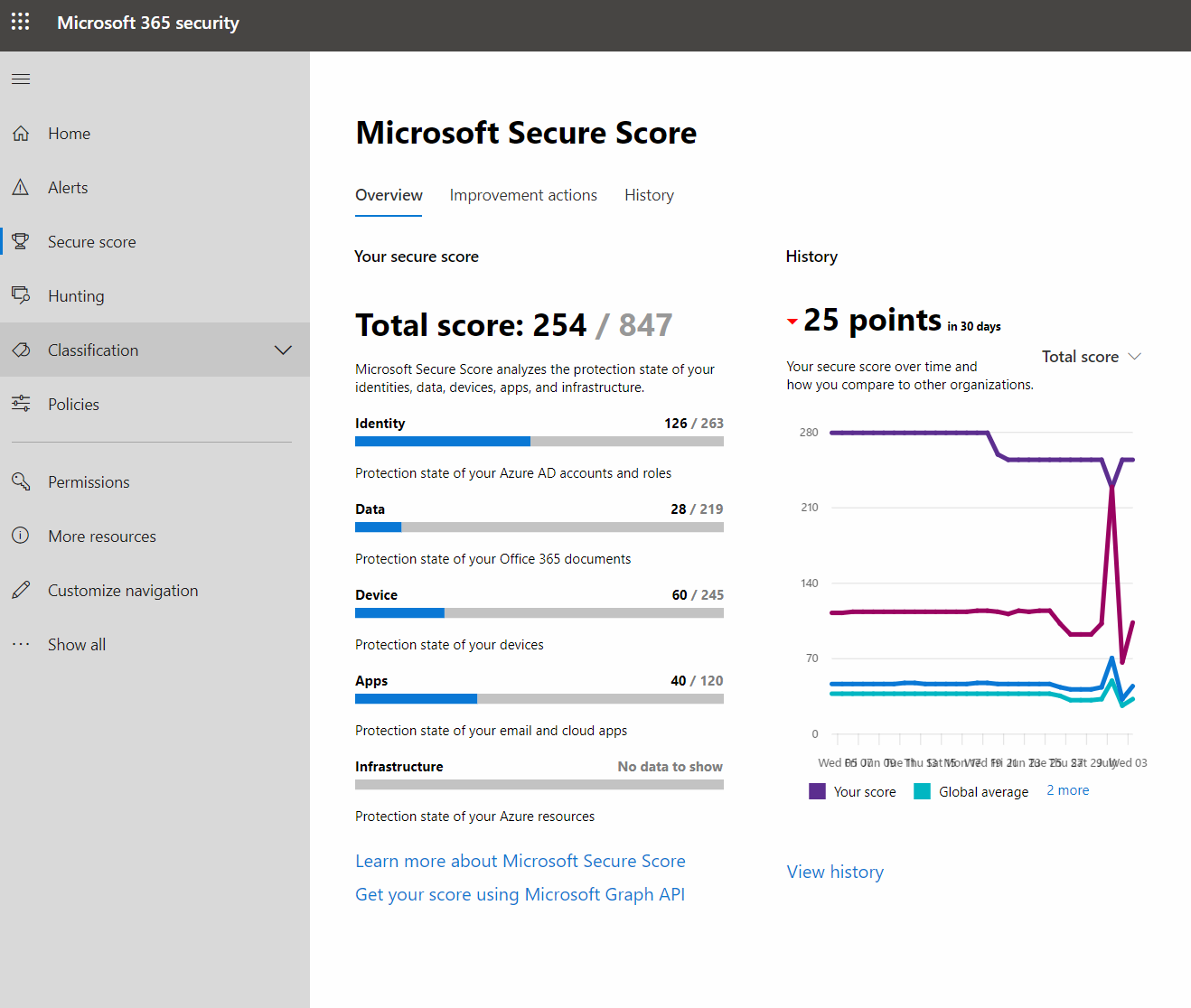
To confirm that you have a valid license, in the Microsoft 365 admin center navigate to Billing > Subscriptions. On the screen you will be able to see all provisioned licenses and their status.

#### Instructions on how to export the Secure Score data

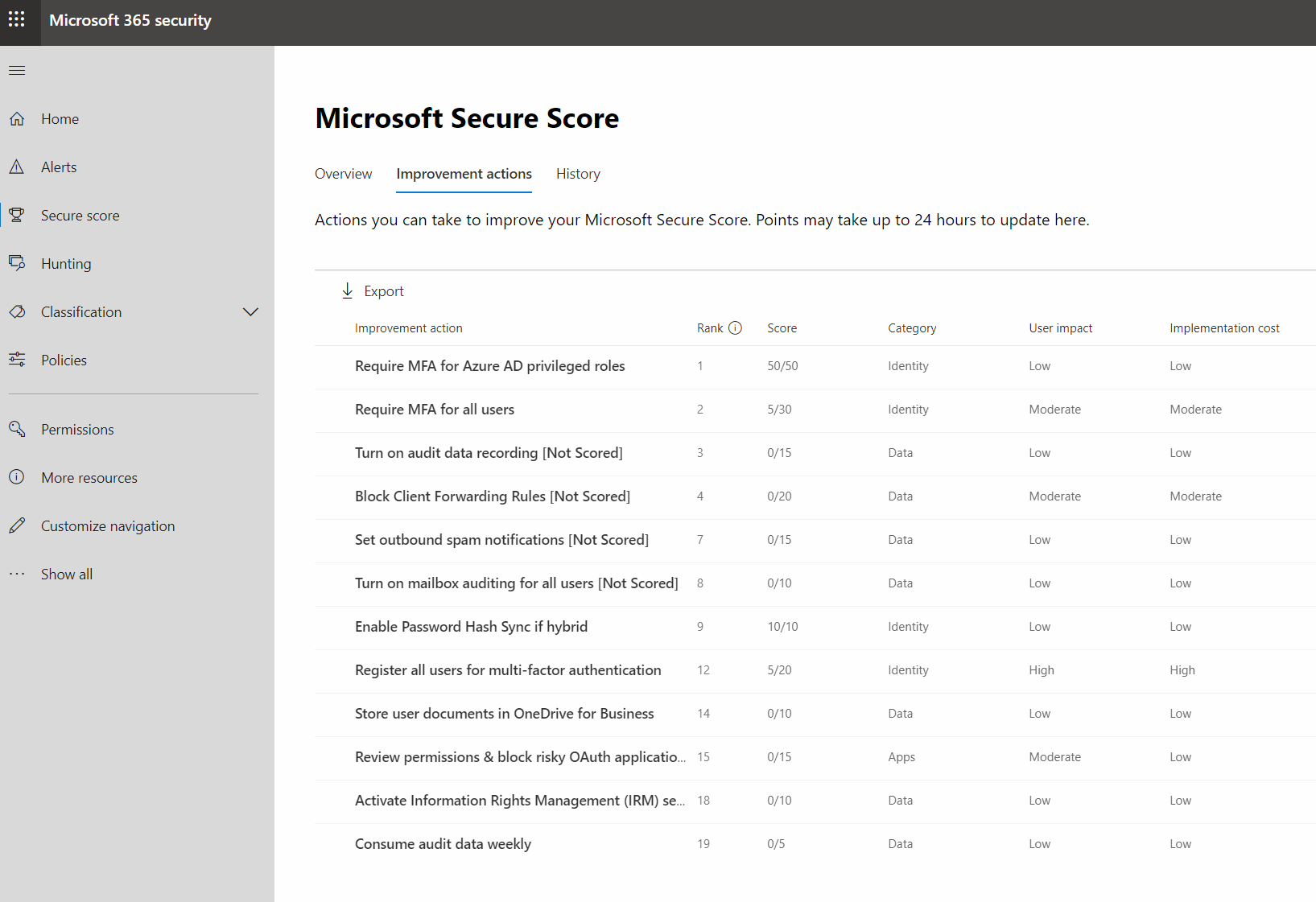
After you have conducted the pre-engagement call, the customer needs to export the Secure Score data and send it to you for analysis. You can either walk through the process over an online meeting or send below instructions to the customer.

Ask the customer to:

1. Open the Microsoft Secure Score tool: [https://securescore.microsoft.com](https://securescore.microsoft.com/). Note that the customer must sign in using their Office 365 tenant admin login credentials.
2. Verify that they have a calculated Secure Score showing in the Secure Score tool.
3. Select the improvement actions tab.



1. Select the Export button and save the CSV file to the local computer.



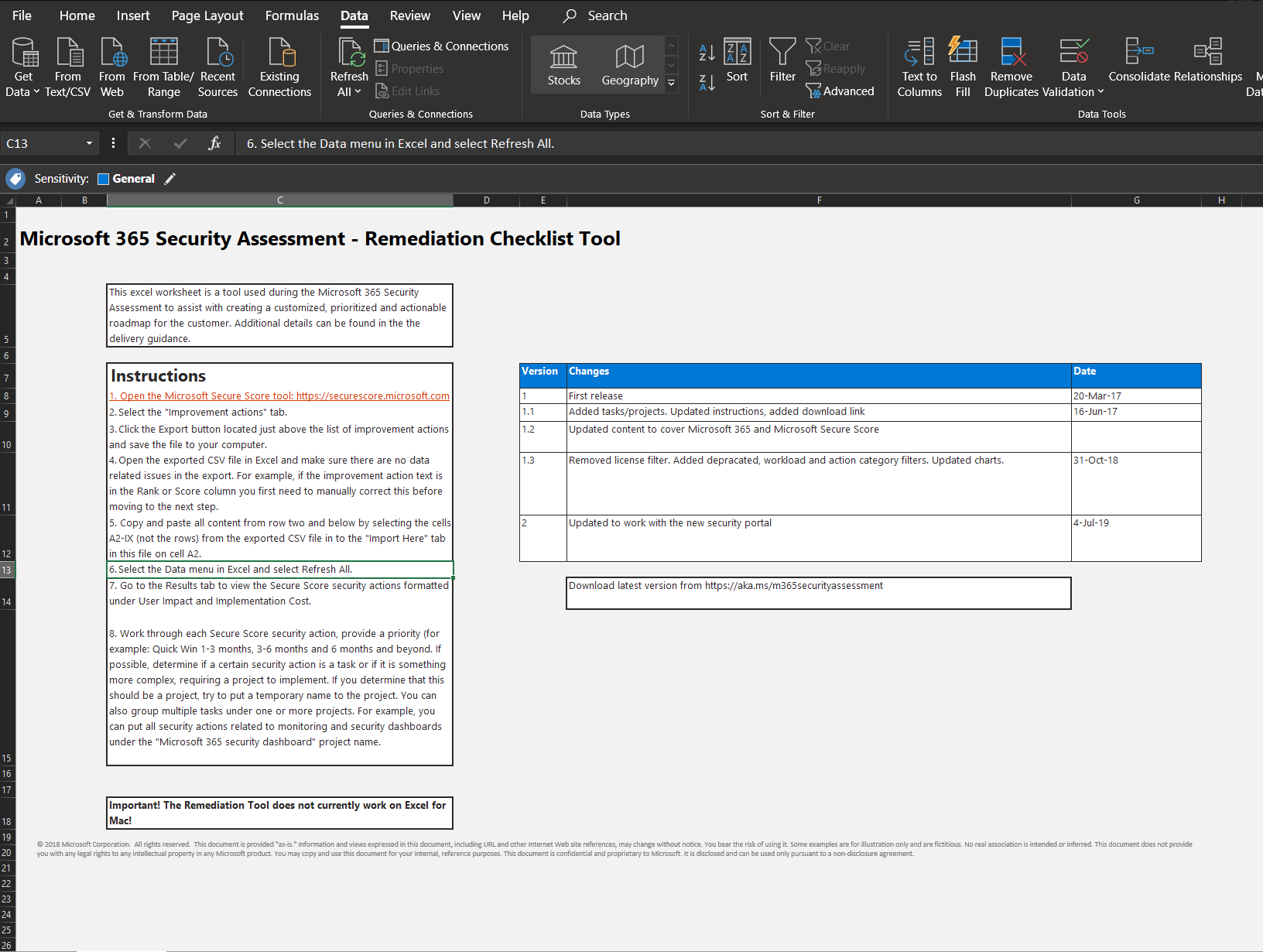
1. Ask the customer to send or share the exported CSV file to you, using a secure method of transfer such as OneDrive.

#### Import the Secure Score data into the Microsoft 356 Assessment-Remediation Checklist Tool

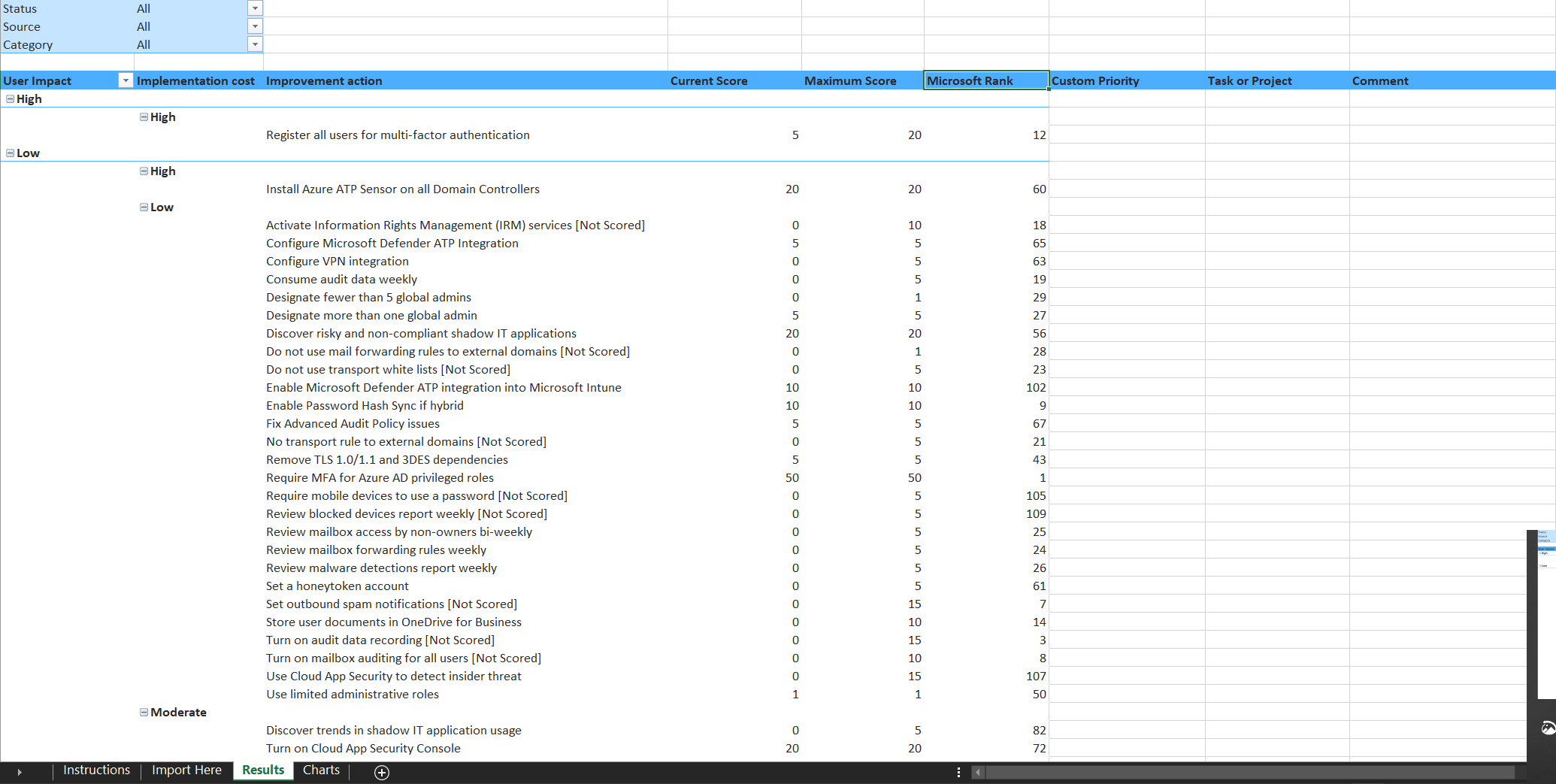
Once you receive the exported file from the customer use following procedure to import the Secure Score data into the *04 - Microsoft Security Assessment - Remediation Checklist Tool.xlsx* tool.

**Important! Always start with the original version of the Remediation Checklist tool to avoid issues with importing and refreshing data.**

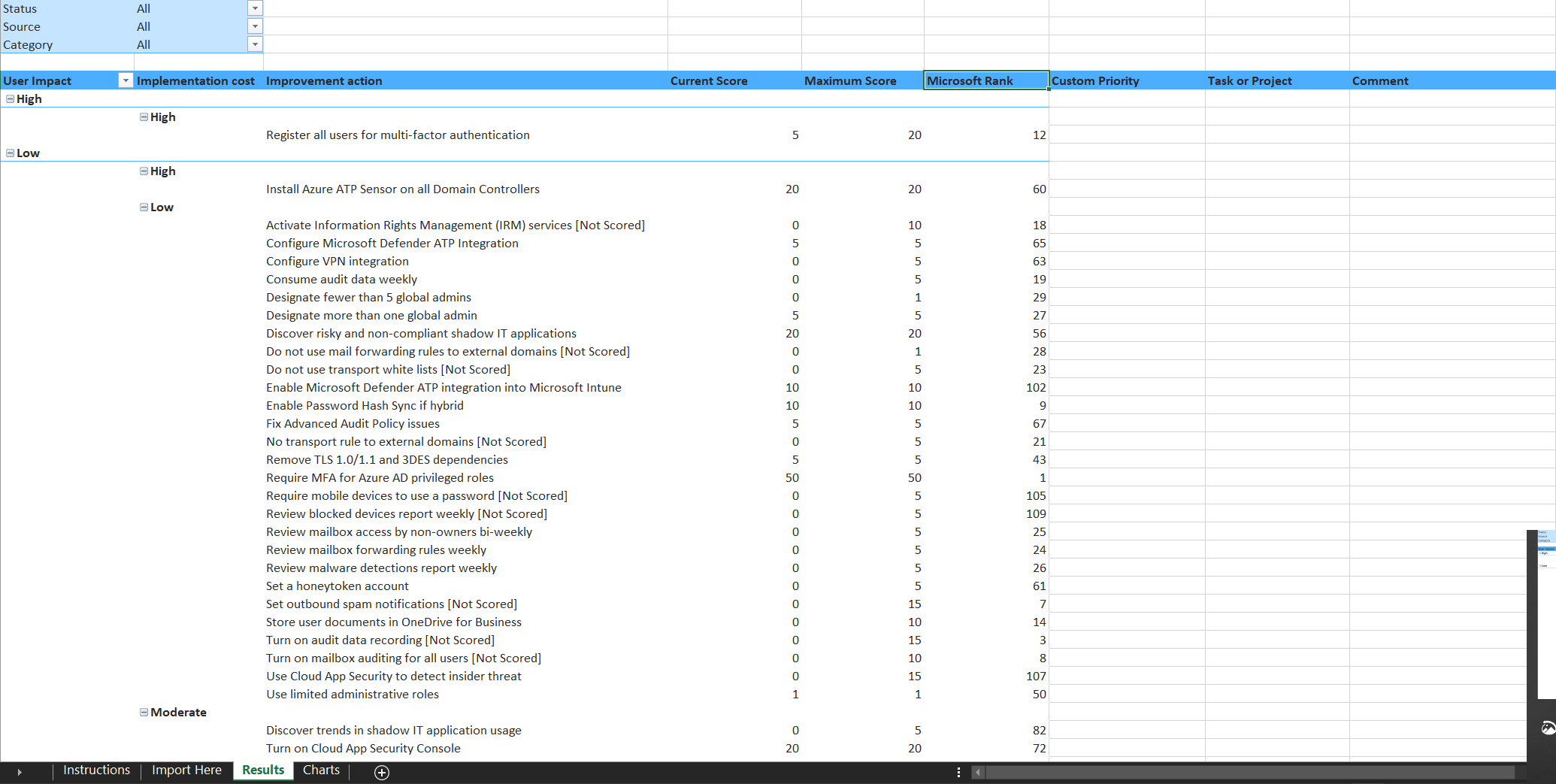
1. Open the exported CSV file in Excel and make sure there are no data related issues in the export. For example, if the improvement action text is in the Rank or Score column you first need to manually correct this before moving to the next step.
2. Copy and paste all content from row two and below by selecting the cells A2-IX (not the rows) from the exported CSV file in to the "Import Here" tab in the *04 - Microsoft Security Assessment - Remediation Checklist Tool.xlsx* tool on cell A2.
3. In the *04 - Microsoft Security Assessment - Remediation Checklist Tool.xlsx* tool, select the Data menu in Excel and select Refresh All. This will update the data model used in the pivot table.



1. Go to the Results tab to view the Secure Score improvement actions sorted under User Impact and Implementation Cost.



1. Work through each Secure Score improvement action and provide a priority based on what you know about your customer’s current and desired security posture. For example: Quick Win 1-3 months, 3-6 months and 6 months and beyond. Additional instructions on how to use the remediation checklist tool can be found in the Remediation Checklist Tool section.



## Microsoft Cloud App Security

Cloud App Security helps global administrators, security administrators, and security readers gain insight into the cloud services people in an organization are using. For example, you can use Cloud App Security to discover where users are storing and collaborating on documents and how much data is being uploaded to cloud application and/or services.

**Important.**

*The Microsoft Security Assessment does not make use of any other Cloud App Security functionality including threat detection and or enhanced control features.*

### Hands-on Delivery Guidance

The Hands-on Shadow IT Assessment activity, delivered as on-site workshop, focuses on a guided exploration of the Cloud Discovery reports in CAS and preparing the final report and roadmap as part of the engagement close-out presentation.

**Important.**

*Due to the potential sensitivity of findings shown in the Cloud Discovery reports, we recommended that the customer drive the exploration, assisted and guided by you as the partner. You should have direct input on which items should be further processed and documented in the final Discovery report.*

* Ask the customer to sign-in to the CAS portal and assist (guide) the customer to explore the Dashboard and each of the Cloud Discovery reports.
* Start in Discovered apps by sanctioning the cloud applications and services that are officially approved in the customer’s organization, and un-sanctioning the cloud applications and services that are unapproved for use or known to be blocked in the customer’s environment.
* Then perform following steps:
  + First explore traffic from the sanctioned cloud applications and services. It is expected that the sanctioned cloud applications and services traffic should constitute a significant majority of the overall traffic mix analyzed by CAS and shown in the Cloud Discovery reports, in any of the available categories.

NOTE: the use of “sanctioned” cloud applications and services should be investigated for “unusual” or “unexpected” peaks of their usage (vs. “usual/typical” or “expected” level), as these situations, if unexplained, this might indicate security breaches. In any case, try to highlight these situations in your Final Discovery report, and recommend that the customer perform further investigation.

EXAMPLE: a sanctioned cloud mail application XYZ, fully approved by the customer organization typically generates traffic of 2 GB daily. However, on a certain day of the week, it is observed that the traffic spiked to 10 GB, and most of this traffic comes from a single IP address. This could mean either full re-synchronization of a single mailbox (e.g. when new device is provisioned for the first time) or it might mean the unauthorized download of that user’s emails. In any case, such “anomalies” should be investigated.

* + Explore traffic from unsanctioned cloud applications and services, if any (in theory - there should be no such traffic). Try to understand with the customer who, when and how much traffic generated towards such cloud applications and services? Is it a single user, small group from the same department, or is it used “across the board” within the organization? Was it used occasionally or is it used permanently? Was the traffic insignificant or heavy? A single or many transactions?

NOTE: the use of “unsanctioned” cloud applications and services isn’t necessarily indication of security threat, although in some cases it might be. Highlight these situations in your final Discovery report, try to investigate them for possible explanation.

EXAMPLE: the customer declared in the “Questionnaire” that cloud storage application XYZ is unapproved in their organization and access to it is blocked on their proxies. However, Cloud Discovery reports from two out of five customer regions show certain number of transactions towards cloud storage application XYZ. Further investigation reveals that blocking filters were incorrectly set in firewalls of the first region. Thus, the recommendation here is to correct the configuration of the firewalls in that region. In case of the second region, the investigation shows that guest Wi-Fi access to Internet is provided through the same firewalls as access to the Internet from the production/internal network. While accessing the cloud storage application XYZ is legitimate from the guest Internet Wi-Fi, the recommendation here is to further exclude traffic from IP ranges dedicated to guest Internet Wi-Fi in in the CAS reports.

* + Explore traffic from “unknown” cloud applications and services. Try to understand with the customer who, when and how much traffic has been generated towards unknown cloud applications and services? Is it a single user, small group from the same department, or is it used “across the board” within the organization? Was it used occasionally or is it used permanently? Was the traffic insignificant or heavy? Single or many transactions? Finally, has it triggered any CAS alerts?

NOTE: use of “unknown” cloud applications and services isn’t necessarily an indication of security threats. It is more likely to be a case of “Shadow IT” activity from users, who are not aware of “approved” cloud applications or services or are missing training on how to use them. Or it might be certain users or even departments that are legitimately using certain cloud applications or services to conduct their business (e.g. sharing information with business partners using their cloud application or services) and these are fully justified activities. Try to investigate these cases and highlight the ones that you find no good explanation for.

EXAMPLE: Cloud Discovery shows a significant number of transactions towards cloud collaboration (chat) services XYZ that are very popular in China. Further investigation reveals that it is being legitimately used to conduct business communication (chat) with Chinese business partners. Since the cloud collaboration services used globally by the customer do not provide federation capabilities to the collaboration cloud service XYZ. The recommendation likely to be given here is to sanction the use of this cloud collaboration service XYZ in CAS, with a comment that it should still be monitored as it is expected that transactions towards this service are coming mostly (or only) from the customer’s network in China.

* Use the data gathered in as part of the exploration to update the Shadow IT Results section within the engagement close-out presentation. Discuss the implications with your customer in depth as you prioritize and build the roadmap of improvement actions. Consider time frames to implement and provide a lifecycle of services to the customer.

**Important.**

*Ask the customer to document (screenshots) discovered cases, as you will need to provide these in the engagement close-out presentation. Make notes and review them with the customer at the end of the hands-on workshop activity. Ask the customer’s permission for using the discovered data.*

*Make sure to consider any security-related services, including recurring managed security services, that you could provide to close some of the gaps found as part of the Shadow IT Assessment. You should describe these proposed security services as part of presentation of the roadmap.*

If you don’t currently offer a managed security service, you can consider offering a Shadow IT Assessment as a managed security service you could provide to your customers. Providing an on-going Shadow IT Assessment as a managed security service is highly beneficial as it could provide you with opportunities to:

* Continuously monitor cloud usage, identifying, assessing, and remediating Shadow IT related issues using CAS
* Providing enhanced periodic reporting
* Support the customer in CAS deployment and customization
* Advanced integration scenarios including SIEM integration
* Assess new features added to CAS
* Keep an on-going relationship with the customer and their security staff

### Technical Preparation

You need to agree on who will be responsible to prepare and configure below tasks as part of the pre-engagement call.

Complete following tasks in order:

#### Validate License

Microsoft Cloud App Security is available in Microsoft Enterprise Mobility + Security E5, Microsoft Enterprise E5 or can be purchased as a standalone license. If the customer does not have a license for Cloud App Security, they can sign up for a free 30-day trial from the Microsoft 365 Admin Center, Billing, Add subscriptions section.

To confirm that you have a valid license, in the Microsoft 365 admin center navigate to Billing > Subscriptions. On the screen you will be able to see all provisioned licenses and their status.

#### Create Snapshot Report

To generate an app discovery report, web traffic log files from a firewall or proxy device must be uploaded to Cloud App Security as part of creating a snapshot report. Cloud App Security then parses and analyzes those files and will generate the app discovery report which you will use as part of the workshop.

**Important.**

*Make sure the traffic data from the proxy or firewall has been imported into Cloud App Security during the week before the on-site workshops to ensure that you have data to analyze during the Shadow IT Overview workshop.*

It’s a good idea to ask the customer about the brand and model of their proxy or firewall as part of the pre-engagement call so that you can verify whether the device is supported by Cloud App Security or if you need to spend additional time using the custom log format option. It’s also useful to have the customer send you a sample log so that you can make sure the import will be successful.

Use following instructions to assist the customer with the import of firewall or proxy logs: <https://docs.microsoft.com/en-us/cloud-app-security/create-snapshot-cloud-discovery-reports>

## Microsoft Defender ATP and Windows Secure Score

Windows Secure Score in Microsoft Defender ATP will allow you to quickly assess the security posture Windows 10 clients within the customer organization, see machines that require attention, as well as recommendations for actions to further reduce the attack surface.

Make sure the Microsoft Defender ATP setup and the onboarding process of the chosen Windows 10 clients have been completed the week before the on-site assessment to make sure you have data to analyze in Microsoft Defender ATP.

### Hands-on Delivery Guidance

The Hands-on Windows Security Assessment activity, delivered as on-site workshop, focuses on a guided exploration of the Windows Secure Score improvement opportunities, the Security recommendations within Microsoft Defender ATP Threat & Vulnerability Management and preparing the final report and roadmap as part of the engagement close-out presentation.

* Ask the customer to sign-in to the Microsoft Defender Security Center portal and assist (guide) the customer to:
  + explore the Windows Secure Score improvement opportunities, making sure you explain each security control and how it impacts Windows 10 security posture
  + explore the Security recommendations within Microsoft Defender ATP Threat & Vulnerability Management, making sure you explain the top security recommendation and the potential business impact on the organizational exposure and configuration scores
* Use the data gathered in as part of the exploration to update the Windows Security Results section within the engagement close-out presentation. Discuss the implications with your customer in depth as you prioritize and build the roadmap of improvement actions. Consider time frames to implement and provide a lifecycle of services to the customer.

**Important.**

*Make sure to consider any security-related services, including recurring managed security services, that you could provide to close some of the gaps found as part of the Windows Security Assessment. You should describe these proposed security services as part of presentation of the roadmap.*

If you don’t currently offer a managed security service, you can consider offering a Windows Security Assessment as a managed security service you could provide to your customers. Providing an on-going Windows Security Assessment as a managed security service is highly beneficial as it could provide you with opportunities to:

* Continuously monitor Windows security posture, identifying, assessing, and remediating endpoint weaknesses using Microsoft Defender ATP Secure Score and Threat & Vulnerability Management
* Providing enhanced periodic reporting
* Support the customer in MDATP deployment and customization
* Advanced integration scenarios including SIEM integration
* Keep an on-going relationship with the customer and their security staff

Additional guidance on how to use Secure Score as part of Microsoft Defender ATP can be located here:  
<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/secure-score-dashboard>

Additional guidance on how to use the Security recommendations within Microsoft Defender ATP Threat & Vulnerability Management can be located here:  
<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/tvm-security-recommendation>

### Technical Preparation

You need to agree on who will be responsible to prepare and configure below tasks as part of the kick-off meeting.

Complete following tasks in order:

#### Validate License

Microsoft Defender Advanced Threat Protection requires one of the following Microsoft Volume Licensing offers:

* Windows 10 Enterprise E5,
* Windows 10 Education E5
* Microsoft 365 E5 (M365 E5) which includes Windows 10 Enterprise E5.

If the customer does not have a license for Microsoft Defender ATP, they can sign up for a free 90-day (or a 30-day trial though the Cloud Solution Provider program) trial from the Microsoft Defender ATP site here: <https://www.microsoft.com/en-us/WindowsForBusiness/windows-atp>

To confirm that you have a valid license, in the Microsoft 365 admin center navigate to Billing > Subscriptions. On the screen you will be able to see all provisioned licenses and their status.

#### Complete Initial Setup

The first time you access the Microsoft Defender ATP portal you need to complete the setup wizard which will guide you through some initial steps and will then create a dedicated cloud instance of Microsoft Defender ATP.

Use following instructions to validate the license and complete the initial setup: <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/licensing-windows-defender-advanced-threat-protection>

#### Select and Onboard Machines

It’s usually not required to onboard all Windows 10 clients to Microsoft Defender ATP as part of the assessment. It should be enough to include a subset of clients, extrapolate the results and, for the most part, assume that issues you find are likely to exist across the larger Windows 10 client environment. Note that only Windows 10 clients will include the Security Analytics needed for the assessment.

You won’t need to install the Microsoft Defender ATP client as its already integrated in Windows 10. Instead, Windows 10 machines need to be configured so that the Microsoft Defender ATP service can get sensor data from them.

**Important.**

*You will need to onboard the Microsoft Defender ATP machines to be included as part of the assessment preferably a week before the on-site workshops, to ensure that you have enough data to analyze as part of the workshop.*

Use following instructions for how to onboard Windows 10 machines:  
<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/configure-endpoints>

Use following instructions to validate sensor health and make sure that you are getting data from the Windows 10 machines:  
<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/check-sensor-status-windows-defender-advanced-threat-protection>

## Attack Simulator

Attack Simulator is used as part of the Microsoft Security Assessment to perform email Spear phishing and Password Attack Simulations. This can help you identify vulnerable users within a customer organization and will allow you to position remediation options as part of the Microsoft Security Assessment.

### Hands-on Delivery Guidance

The Hands-on Attack Simulator Assessment activity, delivered as on-site workshop, focuses on a guided exploration of the simulated spear phishing and password attacks in Attack Simulator, and preparing the final report and roadmap as part of the engagement close-out presentation.

* Ask the customer to sign-in to the Office 365 Security & Compliance portal and assist (guide) the customer to explore the Attack Simulation results
* Use the data gathered in as part of the exploration to update the Attack Simulator Results section within the engagement close-out presentation considering recommendations designed to provide mitigations for phishing and password attacks

Additional guidance on how to use Attack Simulator can be located here:  
<https://docs.microsoft.com/en-us/office365/securitycompliance/attack-simulator>

### Technical Preparation

You need to agree on who will be responsible to prepare and configure below tasks as part of the pre-engagement call.

Complete following tasks in order:

#### Validate License

Microsoft 365 Advanced Threat Protection and Threat Investigation and Response (previously known as Office 365 Threat Intelligence) is available in Office 365 Enterprise E5, Microsoft 365 Enterprise E5 or can be purchased as a standalone Office 365 Advanced Threat Protection Plan 2 add-on license. If the customer does not have a license for Microsoft 365 Advanced Threat Protection and Threat Investigation and Response, they can sign up for a free 30-day trial from the Microsoft 365 Admin Center, Billing, Add subscriptions section.

To confirm that you have a valid license, in the Microsoft 365 admin center navigate to Billing > Subscriptions. On the screen you will be able to see all provisioned licenses and their status.

#### Create Custom Spear Phishing Email Templates

Even though Attack Simulator contains sample spear phishing email templates we highly recommend conducting some basic research of the customer organization and creating one or more custom email templates. This will make sure that the simulated spear phishing emails resemble emails that users within the customer organization would normally receive. Creating custom templates specific to the customer organization will increase the success rate of the email spear phishing attack simulation and is something that a potential attacker is likely to do as well.

#### Prepare Password Lists

Prepare passwords to use as part of the simulated password-spray attack and brute-force password attack. If you don’t have existing passwords lists, you can easily find password lists containing real passwords gathered from data breaches online.

#### Run Simulations

Use following instructions to launch the attack simulations:  
<https://docs.microsoft.com/en-us/office365/securitycompliance/attack-simulator?redirectSourcePath=%252fen-us%252farticle%252fattack-simulator-office-365-da5845db-c578-4a41-b2cb-5a09689a551b>

**Important.**

*You will need to conduct the email spear phishing and password attack simulations at least one week before the on-site workshops to ensure that the simulations have been completed and you have enough data to analyze as part of the session.*

*The phishing simulation should primarily be focused on user education and not about exposing vulnerable users. It is therefore recommended to notify users in advance that you will conduct phishing simulations.*

# Setup and preparation Microsoft Security Assessment Demo

To support the delivery of the readiness activities, a demo environment that can be used during the workshop to explain and showcase functionality is recommended.

Follow the instructions below to setup and configure the demo tenant.

* Create your own Security demo environment
  + Create a demo tenant at <https://demos.microsoft.com>
* Download and go through the “Microsoft Security Management Cross-Product Security Pillar” click through demo from <https://demos.microsoft.com>. This is useful in situations where you do not have access to your demo environment
* Go through the readiness content in *Appendix B -Readiness and technical content*

# Readiness and technical content

This appendix contains recommended learning material that each delivery resource should go through before delivering the Microsoft Security Assessment engagement.

##### General

* Explore and get familiar with the content in the [Microsoft Secure](https://www.microsoft.com/en-us/security/default.aspx) site
* Explore and get familiar with the content in the [Microsoft Cloud Service Trust Portal](https://trustportal.office.com/Client/GetOtherReports)
* Get the latest Microsoft security updates from the [Microsoft Secure Blog](https://blogs.microsoft.com/microsoftsecure/)
* Explore the latest Security readiness resources as part of the [Microsoft Intermediate Security Training](https://www.microsoft.com/microsoft-365/partners/resources/intermediate-security-training)

##### Readiness Presentations

These presentations should be used to deliver the readiness sessions included within the Microsoft Security Assessment.

* [Microsoft Secure Score Presentation](https://transform.microsoft.com/products/microsoft-security-products)
* [Cloud App Security Customer Deck](https://transform.microsoft.com/products/microsoft-security-products)
* [Microsoft Defender ATP Overview Pitch Deck](https://transform.microsoft.com/products/microsoft-security-products)

**Ignite 2018 Sessions**

* [Staying secure with Azure AD and Microsoft Secure Score](https://myignite.techcommunity.microsoft.com/sessions/64577?source=sessions)
* [Using Microsoft Secure Score to harden your security position](https://myignite.techcommunity.microsoft.com/sessions/64332?source=sessions#ignite-html-anchor)
* [How to get visibility into your security position with Microsoft Secure Score](https://myignite.techcommunity.microsoft.com/sessions/64333?source=sessions)
* [Shadow IT discovery beyond the corporate network with Microsoft Defender ATP and Cloud App Security](https://myignite.techcommunity.microsoft.com/sessions/64549?source=sessions)
* [Deploy and manage Cloud App Security in Office 365](https://myignite.techcommunity.microsoft.com/sessions/66404?source=sessions)
* [How to onboard your clients to Windows Defender Advanced Threat Protection](https://myignite.techcommunity.microsoft.com/sessions/66451?source=sessions)
* [Anatomy of an attack in Microsoft 365](https://myignite.techcommunity.microsoft.com/sessions/65775)
* [Raising awareness and education of modern threats to help reduce your organization's risk profile](https://myignite.techcommunity.microsoft.com/sessions/64531?source=sessions)

##### Demos

* [Security Management Security Pillar Video](https://demos.microsoft.com/api/assets/download/96e06afc-750f-4057-b034-03b0eb772d14)
* [Security Management Security Pillar Click Through](https://demos.microsoft.com/demos/details/245)
* Setup your own demo environment using [demos.microsoft.com](https://demos.microsoft.com).
* Populate Azure Security Center with alerts using the “[Azure Security Center Playbook: Security Alerts](https://gallery.technet.microsoft.com/Azure-Security-Center-f621a046)” guide
* Populate Microsoft Defender ATP with alerts using the [Microsoft Defender ATP attack simulations](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/attack-simulations)

##### Product Documentation

* [Microsoft Secure Score product documentation](https://docs.microsoft.com/en-us/office365/securitycompliance/microsoft-secure-score)
* [Microsoft Cloud App Security product documentation](https://docs.microsoft.com/en-us/cloud-app-security/)
* [Microsoft Defender ATP product documentation](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/microsoft-defender-advanced-threat-protection)
* [Attack Simulator product documentation](https://docs.microsoft.com/en-us/office365/securitycompliance/attack-simulator)

Microsoft Security Assessment Toolkit content

The table below lists the files part of the Microsoft Security Assessment Toolkit.

|  |  |
| --- | --- |
| File name | Type |
| 00 - Microsoft Security Assessment - Delivery Guide (This document) | DOCX - Microsoft Word |
| 01 - Microsoft Security Assessment - Pre-engagement Call.pptx | PPTX - Microsoft PowerPoint |
| 02 - Microsoft Security Assessment - ACTION REQUIRED.msg | MSG - Outlook Email |
| 03 - Microsoft Security Assessment - Customer Questionnaire.docx | DOCX - Microsoft Word |
| 04 - Microsoft Security Assessment - Remediation Checklist Tool.xlsx | XLSX - Microsoft Excel |
| 05 - Microsoft Security Assessment - Secure Score Overview.pptx | PPTX - Microsoft PowerPoint |
| 06 - Microsoft Security Assessment - Cloud App Security Overview.pptx | PPTX - Microsoft PowerPoint |
| 07 - Microsoft Security Assessment - Microsoft Defender ATP Overview.pptx | PPTX - Microsoft PowerPoint |
| 08 - Microsoft Security Assessment - Engagement Close-out.pptx | PPTX - Microsoft PowerPoint |