SERVICE ORDER ATTACHMENT
STATEMENT OF WORK

S-266-3149 MICROSOFT CLOUD SECURITY REVIEW

1 OVERVIEW

This Statement of Work ("SOW"), with any appendices included by reference, is part of any agreement that incorporates this document by reference.

1.1 Services Summary

In the modern cloud-driven landscape, the security posture of Azure, Entra ID, and Microsoft 365 (M365) is of paramount importance for businesses of all sizes. Our Microsoft Cloud Security Review service, which covers Azure, Entra ID, and M365, is designed to provide a comprehensive review of your cloud infrastructure and presence.

We leverage both manual and automated techniques to evaluate your services, resources, configurations, policies, and code, identifying vulnerabilities, misconfigurations, and best-practice deviations that could lead to security breaches.

The Customer may choose which of the following options best suits their needs:

Option 1: Microsoft 365 and Entra ID for 1x Tenant

Option 2: Microsoft 365 and Entra ID and Azure for 1x Tenant plus up to 250 resources

Option 3: Microsoft 365 and Entra ID and Azure for 1x Tenant plus up to 500 resources

1.2 Scoping Information

Our Microsoft Cloud Security Review service offers flexible options to meet your specific needs. We can assess any or all components of your Microsoft cloud environment:

Azure: We evaluate your cloud infrastructure, including (but not limited to) virtual machines, storage, networks, and security configurations, to identify publicly accessible assets, risks, and vulnerabilities.

Entra ID (formerly Azure AD): We review your identity management configurations, focusing on authentication settings, permissions, policies, integrated applications, and access controls.

Microsoft 365 (M365): We assess your M365 configurations, including those of specific services within your M365 suite (such as, but not limited to, Exchange Online, Microsoft Defender, and SharePoint), to identify configuration weaknesses and security gaps.

Whether you need a comprehensive review of your entire Microsoft Cloud tenancy or a targeted assessment of individual components, we customize our approach to deliver maximum value.

1.3 Scoping Requirements

To scope and deliver the Microsoft Cloud Security Review, we require information for the following sections. Please note that we only require information for the in-scope sections.

- Azure
    - Is Azure in scope?
    - Number of in-scope Azure tenants
    - Number of in-scope subscriptions
    - Number of total resources
    - Is everything within the tenant(s) in scope? If not, please clarify what is and out of scope

- Entra ID
    - Is Entra ID in scope?
    - Number of in-scope Azure tenants

- M365
    - Is M365 in scope?
    - Number of unique M365 tenants/instances
    - Is everything in scope? If not, please clarify what is in and out of scope

1.4 Methodologies

Below are the high-level actions undertaken by a consultant reviewing **Azure.**

- Manual Expert Assessment
    - Detailed analysis of Azure resources against industry security standards and in-house security recommendations.
- External Exposure Analysis
    - Discovery and cataloging of all internet-facing assets.
    - Targeted scanning to identify publicly accessible resources and risks.
- Blended Expert Analysis
    - Deployment of specialized tools to identify security gaps and misconfigurations.
    - Automated CIS Benchmark assessments to evaluate compliance with industry standards.
    - Configuration extraction and evidence collection for detailed documentation.
- Strategic Recommendations
    - Security findings prioritized by risk level and exploitation potential using an Impact x Likelihood = Risk model and/or CVSS version 4
    - Actionable and tailored remediation guidance from experienced cloud security specialists.
    - Comprehensive reporting with clear visualization of your security posture

Below are the high-level actions that are undertaken by a consultant who is reviewing **Entra ID;**

- Manual Expert Assessment
    - Detailed analysis of Entra ID configurations, such as (but not limited to) user, device, and application configurations
    - Analysis of Entra ID account metadata to determine password age, account configurations, and account type.
    - Evaluation of authentication methods, MFA implementation, and conditional access policies
    - Review of application registrations, service principals, and permission assignments
    - Examination of identity protection settings, risk policies, and threat detection capabilities
    - Directory synchronization configuration and security review
    - Password policy evaluation, including legacy authentication protocols
    - Identity security posture using Microsoft Secure Score.

- Blended Expert Analysis
    - Deployment of specialized tools to identify security gaps, score/rating, and misconfigurations
    - Identification of end-of-life devices within Entra ID devices
    - Automated CIS Benchmark assessments to evaluate compliance with industry standards
    - Configuration extraction and evidence collection for detailed documentation

- Strategic Recommendations
    - Security findings prioritized by risk level and exploitation potential using an Impact x Likelihood = Risk model and/or CVSS version 4.
    - Actionable and tailored remediation guidance from experienced cloud security specialists
    - Comprehensive reporting with clear visualization of your security posture.

Below are the high-level actions undertaken by a consultant reviewing a Microsoft 365 **(M365) tenant.**

- Manual Expert Assessment
    - Comprehensive evaluation of admin configurations across M365, Exchange Online, SharePoint, Teams, OneDrive, and Power Platform
    - Analysis of data protection settings and DLP policies
    - Review of email security configuration, including anti-phishing, anti-spam, and safe attachments
    - Assessment of endpoint protection policies, mobile device management, and application control
    - Evaluation of user permissions, sharing settings, and external collaboration configurations
    - Assessment of joined devices within Intune to identify (where possible) outdated and end-of-life devices

- Blended Expert Analysis
    - Deployment of specialized tools to identify security gaps, score/rating, and misconfigurations

  - Automated CIS Benchmark assessments to evaluate compliance with industry standards
  - Configuration extraction and evidence collection for detailed documentation

- Strategic Recommendations
  - Security findings prioritized by risk level and exploitation potential using an Impact x Likelihood = Risk model and/or CVSS version 4
  - Actionable and tailored remediation guidance from experienced cloud security specialists
  - Comprehensive reporting with clear visualization of your security posture

1.5 Project Deliverables

At the conclusion of the assessment, SilverSky will provide a comprehensive report. The report will include three main sections: (i) an executive summary, (ii) a narrative, and (iii) a detailed findings section. The Customer will have an opportunity to review drafts of the report, and SilverSky will deliver a final version after joint review with the Customer.

Executive Summary - This section summarizes the results of the assessment. It is intended for upper management and boards of directors and includes:

- Overview of assessment results
- Itemization of the risk ratings for each area reviewed during the assessment
- Key findings and recommendations

Consultant Findings – This details the major events and findings discovered during testing. It is interspersed with technical detail and analysis.

Detailed Findings - This section describes the assessment results in detail. It is intended for management, administrators, and other operations personnel and includes:

- An itemized listing of individual vulnerabilities
- A description of each vulnerability
- The severity of the threat likely posed by each vulnerability
- Potentially affected resources
- Recommendations for remediation

1.6 Out of Scope

Any activity not explicitly stated in this SOW is considered out of scope.

If Customer requests additional services, such services will be subject to a change request or additional SOWs, depending on the nature of the Customer's requests.

2 CUSTOMER OBLIGATIONS AND ASSUMPTIONS

Services, fees, and work schedule are based upon the assumptions, representations, and information supplied by the Customer’s fulfillment of these responsibilities is critical to the success of the engagement.

Customer Obligations

- Project Liaison - Designate an authorized representative to authorize completion of key project phases, assign resources, and serve as project liaison
- Access - Ensure SilverSky consultants have access to key personnel and data requested
- Resources - Furnish SILVERSKY with Customer personnel, facilities, resources, and information, and perform tasks promptly
- Cooperation - Ensure all of the Customer's employees and contractors cooperate fully with SilverSky and in a timely manner. SilverSky will advise Customer that increased Customer participation is required in order for SilverSky to perform the Service under this SOW.
- Documentation – Deliver in a timely fashion all documentation requested by SilverSky.

SilverSky Assumptions

- Customer will provide SilverSky with reasonably requested information upon which SilverSky can rely to be current, accurate, and complete.
- Customer will provide access to Customer's personnel with detailed knowledge of Customer's security architecture, network architecture, computing environment, and related matters.
- Customer will provide access to Customer's personnel who have an understanding of Customer's security policies, regulations, and requirements.
- Customer will evaluate SilverSky deliverables and immediately notify SilverSky of any perceived problems or issues with SilverSky's obligations.
- SilverSky will immediately notify the Customer of any perceived problems or issues regarding Customer obligations.
- Customer is responsible for any additional costs if SilverSky cannot perform the Service due to Customer's delay or other failure to fulfill its obligations under this Statement of Work.

3 PROJECT PARAMETERS

3.1 Project

The scope of the project is based on the above description, with the additional details listed as follows:

Project Component	**Parameter(s)**
Project Start Date	Typically, within 30 days of the Effective Date
Project Duration	Approximately 1-2 weeks, subject to project variables
Microsoft Cloud Security Review **S-266-3149**	Microsoft 365 and Entra ID for 1x Tenant
Microsoft Cloud Security Review **S-266-3149**	Microsoft 365 and Entra ID and Azure for 1x Tenant, plus up to 250 resources
Microsoft Cloud Security Review **S-266-3149**	Microsoft 365 and Entra ID and Azure for 1x Tenant plus up to 500 resources

3.2 Location and Travel Reimbursement

The Services defined in this SOW will be performed remotely and do not require any on-site travel.

3.3 Acceptance

Delivery of all stated project deliverables will constitute acceptance of services provided under this SOW.