

SERVICE ORDER ATTACHMENT
STATEMENT OF WORK

S-266-3149 ACTIVE DIRECTORY (AZURE/ON-PREM) BEST PRACTICE ASSESSMENT

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

Most organizations rely on Active Directory (AD) to provide authentication and authorization into their networks, but very few organizations take the time to perform best practice hardening of this environment to make it secure. Since Active Directory serves as a centralized authentication and authorization service in Windows environments, it is a prime target for attackers. Most attackers gain entry into networks based on simple misconfigurations in Active Directory Environments.

SilverSky’s Active Directory Hardening Assessment gives you a comprehensive view of your Azure or On-Prem Active Directory setup. This overview includes the identification of any misconfigurations or attack paths that threat actors could exploit within your environment, optimization of group policy controls, a listing of privileged accounts, and other valuable information. SilverSky will assess your environment and help you prioritize changes to your Active Directory that can significantly increase security and lower risk.

1.2 Project Summary

SilverSky will provide the following primary tasks, subject to modification or extension based on the engagement.

1. Kick-off Meeting
2. Information Gathering/Discovery
3. Controls Review
4. Analysis and Documentation
5. Reporting

1.3 SilverSky Obligations:

Kickoff Call – SilverSky will perform a kickoff call to understand your environment and determine the best action for assessing AD-related components.

Information Gathering Phase - Our engineers will utilize security resources and automated testing tools to gather user information, privilege levels, groups, and policies to combine with data collected for the assessment.

Review Phase -The above-gathered information will be reviewed to determine risks within your environment due to misconfigurations, overreaching policies, and unaddressed vulnerabilities.

SilverSky Proprietary

Analysis and Documentation Phase - SilverSky will compile and review the information gathered, then analyze and document the findings and any test results in detail in a draft iteration of the final reports.

Reporting Phase - All findings will be compiled into a report that includes issues and misconfigurations, potential paths to exploitation in Active Directory, and recommendations for remediation.

1.4 Deliverables

SilverSky will provide a Detailed Findings Report following its review.

The Detailed Findings Report describes the review results in detail. It is intended for mid-level management, administrators, and other operations personnel and includes:

- Itemized listing and description of the areas reviewed.
- Identified deficiencies.
- Overall risks associated with deficiencies.
- Detailed recommendations for addressing deficiencies.

1.5 Out of Scope

Any activity not explicitly included in this SOW is considered out of scope. If the Customer requests additional services, such services will be the subject of a change request.

2 CUSTOMER OBLIGATIONS AND ASSUMPTIONS

Services, fees, and work schedules are based on the assumptions, representations, and information supplied by the Customer. The Customer's fulfillment of these responsibilities is critical to the success of the engagement.

2.1 Customer Obligations

- **Project Liaison** - Designate an authorized representative to authorize the completion of key project phases, assign resources, and serve as project liaison.
- **Access** - Ensure SilverSky consultants can access key personnel and requested data.
- **Resources** - Furnish SilverSky with Customer personnel, facilities, resources, and information and perform tasks promptly.
- **Cooperation** - Ensure all the Customer's employees and contractors cooperate fully and promptly with SilverSky. SilverSky will advise the Customer if an increased level of Customer participation is required for SilverSky to perform the Services under this SOW.
- **Documentation** - Timely delivery of all documentation SilverSky requests, including the Customer's security policies, network diagrams, server listings, and procedures.

2.2 SilverSky Assumptions

- The Customer will provide SilverSky with reasonably requested information upon which SilverSky can rely to be current, accurate, and complete.
- The Customer will provide access to the Customer's personnel with detailed knowledge of the Customer's security architecture, network architecture, computing environment, and related matters.

SilverSky Proprietary

- The Customer will provide access to the Customer’s personnel who understand the Customer’s security policies, regulations, and requirements.
- The Customer will evaluate SilverSky deliverables and immediately notify SilverSky of any perceived problems or issues with SilverSky obligations.
- SilverSky will immediately notify Customer of any perceived problems or issues regarding Customer’s obligations.
- Customer is responsible for additional costs if SilverSky cannot perform the Services due to Customer’s delay or failure to fulfill its obligations under this Statement of Work.

3 PROJECT PARAMETERS

3.1 Project Scope

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	SilverSky will reach out within 30 days of the Effective Date with a date for a kickoff call.
Project Duration	Approximately 1-2 weeks, subject to project variables
	<u>Consulting not to Exceed</u>
Active Directory (Azure/On-Prem) Best Practice Assessment	Includes one Active Directory environment. Not to exceed 60 hours

3.2 Location and Travel Reimbursement

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

3.3 Acceptance

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