**SERVICE ORDER ATTACHMENT**
**STATEMENT OF WORK**
**S-266-2720 SECURITY MATURITY ASSESSMENT**

## 1 OVERVIEW

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

### 1.1 Services Summary

The purpose of the Security Maturity Assessment service is to help management measure the Customer's level of risk and corresponding controls in regard to cyber security. The assessment is based on the NIST Cyber Security Framework and ISO standards concerning cyber security controls. The assessment will help determine if the Customer's behaviors, practices, and processes support cybersecurity preparedness. The service expands on the findings of SilverSky's IT Controls Review (S-266-2278) and, as such is available strictly as an add-on to that service.

**Project Deliverables:**

- Reports: Executive Summary and Detailed Technical Findings Report

### 1.2 Project Summary

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

1. Information Gathering/Discovery
2. Audit and Review
3. Analysis and Reporting
4. Knowledge Transfer

## 2 SCOPE

### 2.1 SilverSky Obligations:

The Security Maturity Assessment relies on full cooperation and participation by the Customer in completing prescribed interviews, walkthroughs, and questionnaires. SilverSky will request copies of security-related documents and will require access to critical IT assets and systems and to physical locations such as server rooms, data centers, and operations facilities. All work is typically performed onsite.

There are four primary phases involved in performing the Security Maturity Assessment:

**Information Gathering Phase** – Gather and examine information security program-related documentation. This documentation includes (but is not limited to): information security policies and procedures, network diagrams, results from prior assessments or reviews, vendor agreements, and the Customer's current Disaster Recovery Plan. SilverSky will review the documentation in detail and use it

to identify areas that might need more focus or attention.

**Audit and Review Phase** – Interview the key parties responsible for the implementation of the security program. These interviews typically involve IT and systems administrators as well as information security and compliance officers, and are conducted to assess the extent to which existing policies and controls have been implemented within the following areas of the Cyber Security Framework:

1. Identify – Assess Customer's understanding and ability to manage cyber security risk to systems, assets, data, and capabilities
2. Detect – Assess how the Customer has implemented appropriate safeguards to ensure the delivery of critical infrastructure services
3. Protect – Assess how the Customer has implemented appropriate activities to identify the occurrence of an information security event
4. Respond – Assess how the Customer has implemented appropriate activities to take action regarding a detected information security event
5. Recover – Assess how the Customer has implemented appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to an information security event

**Analysis and Documentation Phase** – Compile and organize data gathered from the audit and review phases to ensure all defined areas were reviewed and documented. Conduct data analysis and prioritize findings to determine the criticality and potential impact each can have on the Customer. Compare the Customer's current overall security maturity to generally accepted industry standards and any compliance requirements. Develop an initial report detailing the audit findings and results.

**Knowledge Transfer Phase** – Present and review the draft report findings with key Customer personnel. Depending on the scope and extent of the Service, Customer management responses to the findings can be included and documented in the report. Any issues, questions and/or concerns will be jointly discussed and resolved after which SilverSky will deliver final versions of its reports to Customer.

## 2.2 Deliverables

SilverSky will provide an Executive Report and a Detailed Findings Report following its review.

The Executive Report is a high level summary of the review intended for upper management and the Board of Directors and includes:

- One-page executive summary
- Concise list of key findings
- Summary of findings for each area reviewed during the evaluation
- High-level recommendations for addressing deficiencies

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

## 2.3 Out of Scope

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

# 3 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.

## 3.1 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 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 the Customer if an increased level of Customer participation is required in order for SilverSky to perform the Services under this SOW.
- **Documentation** - Timely delivery all documentation requested by SilverSky including Customer's security policies, network diagrams, server listings, and procedures

## 3.2 SilverSky Assumptions

- Customer will provide SilverSky with reasonably requested information SilverSky can rely on to be current, accurate and complete.
- Customer will provide access to Customer's personnel who have detailed knowledge of Customer's security architecture, network architecture, computer environment and related infrastructure.
- Customer will provide access to Customer's personnel who understand Customer's security policies, regulations and requirements.
- Customer will evaluate SilverSky deliverables and immediately notify SilverSky of any perceived problems or issues with SilverSky 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 is unable to perform the Services due to Customer's delay or other failure to fulfill its obligations under this Statement of Work.

# 4 PROJECT PARAMETERS

## 4.1 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 | Typically within 30 days of the Effective Date |
| Project Duration | Approximately 3-4 weeks, subject to project variables |
| | Consulting Hours not to Exceed |
| **S-266-2720** Security Maturity Assessment (advanced) | 70 |
| **S-266-2720** Security Maturity Assessment (core) | 30 |

Pricing is based upon your level of service and you are not allowed to downgrade if the engagement lasts less than your maximum days set forth in the table above. As stated previously, this service is made available strictly as an add-on to the IT Controls Review service (S-266-2278); that said, the service level selected by the Customer for the IT Controls Review service has no bearing on which level they can select for their Security Maturity Assessment.

## 4.2 Location and Travel Reimbursement

The Services defined in this SOW will typically require onsite participation by SilverSky staff at Customer location(s).

For Customer-approved onsite participation, the Customer will be invoiced for all actual SilverSky staff travel and living expenses associated with all onsite visits. An administration fee of ten percent (10%) of all travel and living expenses will be billed to the Customer if the Customer requires an itemized statement of such expenses.

| **Location** | **Scope of Work** |
|---|---|
| | |
| | |
| | |

## 4.3 Acceptance

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