SERVICE ORDER ATTACHMENT
STATEMENT OF WORK

S-200-3152 VCISO ADVISORY PROGRAM- TIER 1 SHIELD PACKAGE

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 Service Background

1.2

SilverSky will assist the Customer by providing a Virtual Chief Information Security Officer (vCISO) services to advise the leadership team and bolster the advancement of their organization-wide cybersecurity measures, adhering to optimal industry norms.

1.3 Objective

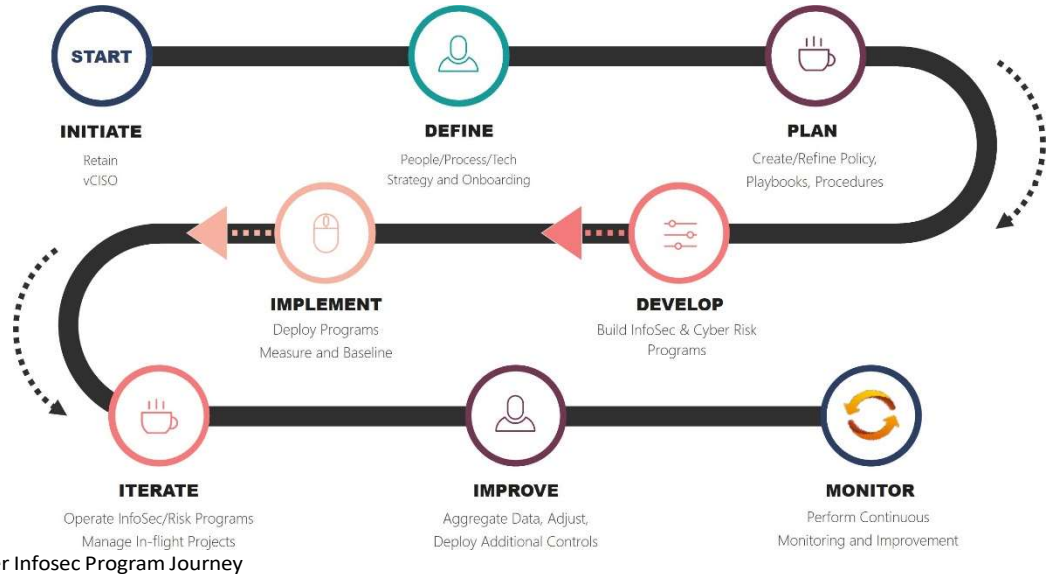
1.4

The goal of this engagement will be for the vCISO to assist Customer in enhancement of it's information security and cyber risk program in a defined manner, focusing on continuous monitoring and improvement via strategic oversight, program management, tactical advisory on initiatives, and reporting of results. SilverSky will assign a vCISO resource who will commit their expertise to the Customer for twelve (12) months, working in close cooperation with the Customer's appointed Primary Point of contact to help provide strategic guidance for the Customer's cyber security program.

2 Shield Package Scope

2.1 Methodology

The SilverSky vCISO Shield Package will help build maturity within the Customer's cyber security by following the following key phases of development.



1 Figure 1-1: Customer Infosec Program Journey

2.2 Program Activities

Through the SilverSky Shield Package, the vCISO will lead corrective and implementation strategies - in coordination with, and through acceptance by Customer - as revealed by the most recently performed point-in-time risk or gap assessment. The vCISO will also provide additional recommendations and advisory to bolster Customer's information security program. The vCISO will provide regular updates to the Customer's leadership team throughout this Statement of Work term.

Examples of strategic advisory and tactical execution activities can include, but are not limited to:

Strategic:

- Facilitate and deliver a "Crown Jewels" exercise, which allows the executive team to take business drivers and align them with cybersecurity improvement mandates for the organization.
- Engage closely with Customer's executive team on steering and governance of security program undertakings, keeping in sync with Customer's organizational objectives.
- Advise on Customer infosec program; participate in associated committees as requested.
- Assist with preparing and delivering reports for the executive team on the status of infosec and cyber risk programs.

Tactical:

- Advisory for remediation of specific findings in the most recent risk or gap assessment. (see Deliverables section)
- Communicate, interact, and liaise with Customer's technical departments and vendors regarding information security program design and strategic actions.
- Offer technical security backing for business goals and provide guidance for technical alterations to align with pertinent information security standards.

2.3 Shield Package Included Activities

Due to the broad nature of this type of engagement and the varying amount of time on a wide range of deliverables, all deliverables will be created and delivered as time allows in the Time Commitment for this Statement of Work. Deliverables may change, and/or additional deliverables can be requested based on Customer's approval. Based on the Consultant's existing templates, The examples below can be provided as PFD, Excel, Word, PowerPoint documents, or SaaS dashboards.

2.3.1 Static Deliverables

A. Recurring Activities

GRC SaaS Tool Licensing

- An enterprise class Governance, Risk Management, and Compliance tool comes baked into the service.
- It's next-gen risk engine and data-centric approach build crystal clear synchronization between your business and cyber goals.

Perform Annual Risk Assessment

- In addition to ongoing risk measurement, the formal risk assessment provides deep insights into your current cyber posture's status, performance, and efficacy.
- The resulting Plan of Action & Milestones (POA&M) allows you to forecast short- and long-term goals, and secure your environment with confidence.

Perform Annual Policy-to-Controls Review

- Current security policies are consistently reviewed to ensure alignment with current organizational processes and cybersecurity best practices.

- Your vCISO makes recommendations for updates, creation, or deletion of policies based on findings.

B. Program Launch Activities

Facilitate and deliver "Crown Jewels" exercise.

- For up to 8 Customer personnel.
- Individual workshops are performed with leadership and subject matter experts to identify your organization's most valuable systems and data.
- A group exercise is then facilitated to build top-down consensus for protecting the most critical parts of your business methods, trade secrets, customer data, and operations - i.e., your Crown Jewels.

The formal creation of the Information Security Program

- Once the organization is aligned on the priority and criticality of it's Crown Jewels, and after data collection and/or risk assessments have completed, a roadmap and recommendations are created.
- The inaugural report is delivered, and the infosec program is launched.

Develop Incident Response (IR) policy and advise on Business Continuity Plan

- Your vCISO will work with your team to create a customized and detailed IR plan.
- Can also advise on strategies and methods to develop the cyber portions of your BC plan.

C. Dynamic Deliverables and Reporting

Performance Audit and Analysis Meeting (Quarterly)

Audience: IT/IS Management

- Cyber initiatives management: issues, requests, and changes
- Cyber-related strategy, tactical, or operational activities for POA&M
- Attend meetings in support of current security initiatives and projects
- Facilitate consensus-building to develop a security culture within the organization

Strategic Audit, Analysis, and Report (Quarterly)

Audience: Executive/IT Leadership

- Current cyber roadmap and status
- Budget status and recommendations
- Critical risks and program performance
- Progress, pivots, and adjustments in the cyber roadmap

2.4 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. Managed Services and ongoing operations of any program items are not included in the scope and will be outlined on a separate SOW.

2.5 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.

- 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 - to include access to critical IT assets, systems and physical locations such as server rooms, data centers, and operations facilities
- 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 of all documentation requested by SilverSky, including Customer's security policies, prior security reviews, network diagrams, server listings, and procedures

2.6 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 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 cannot perform the Services due to Customer's delay or other 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	12 months. Work hours not to exceed 240

3.2 Location and Travel Reimbursement

The Services defined in this SOW will be performed remotely via web meetings. In addition to time spent on Recurring Activities, the vCISO will perform regular activities to facilitate and execute this Statement of Work weekly, with the time spent not exceeding two (2) hours per week.

Any request for onsite work will be at the sole discretion of the vCISO and must be approved by the Customer. For Customer-approved onsite participation, the Customer will be invoiced separately 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.

3.3 Acceptance

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

[End of Document]