

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

The purpose of the Maturity Assessment is to identify the client’s baseline cyber maturity against the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and to outline potential areas for improvement in the Customer’s cyber risk program. The assessment procedures are based on the latest NIST CSF Security Standards (v2.0) as updated by NIST. This project will focus on the Customer’s policies, procedures, practices, information technology (IT) environment, and existing cybersecurity efforts. SilverSky will document identified weaknesses and provide recommendations to help the Customer enhance its security and compliance program.

Project Deliverables:

- Report: Executive Summary & Assessment Detailed Findings
- Plan of Action & Milestones

1.2 Project Summary

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

1. Preparation and Scoping
2. Information Gathering/Discovery
3. Framework Gap Analysis
4. Policy Analysis
5. Reporting & Improvement Roadmap

1.3 Framework Overview

NIST CSF 2.0 is organized around six core Functions:

- Govern: Focuses on how the organization establishes and oversees cybersecurity risk management.
- Identify: Understand the organization’s assets, systems, data, business environment, and risks to know what needs protection.
- Protect: Put safeguards in place to limit or contain cybersecurity events.
- Detect: Develop capabilities to discover cybersecurity events quickly.
- Respond: Act when a cybersecurity incident occurs.
- Recover: Restore operations and services after an incident.

2 Scope

2.1 SilverSky Obligations:

Preparation and Scoping - Meet with key personnel to discuss the Customer’s operational and technical environment. During this initial conversation, SilverSky will determine the scope of the Customer IT environment to be assessed, including considerations for outsourced arrangements, network segmentation, and third-party processing providers. The preparation and scoping phase is used to:

- Set expectations regarding the project scope, objectives, activities, and associated timetables over the course of the engagement
- Establish roles and responsibilities for both Customer and SilverSky teams
- Establish project management standards, including milestone meetings, status reports, and ongoing communications with key personnel
- Facilitate the collection of Customer-specific information that is required to complete the NIST CSF Gap Assessment

Information Gathering - Review existing Customer documents related to NIST CSF compliance and interview Customer personnel. SilverSky may require further interviews and documentation throughout the process. Samples of the requested documentation will include:

SilverSky Proprietary

- Prior IT or Operation Risk Assessments
- Network diagrams
- Security and compliance training programs
- Information security policies and procedures
- Workforce training program documentation
- IT organizational charts
- Security software and hardware lists
- Interview schedules for key personnel

SilverSky will use the information gathered to focus more effectively and streamline client interviews. SilverSky will schedule a combination of group and individual interviews with personnel from various functional areas. The interview process will focus on the areas outlined in the NIST CSF standard.

NIST CSF Gap Analysis - Evaluate the in-scope processes, systems, and documentation against the domain requirements as outlined within the NIST CSF v2.0. SilverSky will examine the security and control structure, or related information systems and business processes, involved in the Customer's collection, use, and disclosure of sensitive information to determine the adequacy of controls. During this phase, SilverSky will:

- Assess how controls have been deployed to support key business processes, technology infrastructure, and relevant systems.
- Interview key system and business stakeholders to identify current policies and practices related to information security
- Identify and assess information security risks within key functional areas associated with the information security program
- Evaluate your current risk management techniques for addressing security risks
- Identify deficiencies and gaps in security and privacy practices through targeted tests and control analysis
- Develop detailed recommendations to assist the Customer's remediation of deficiencies

SilverSky will review the following key control categories for compliance with NIST CSF v2.0 requirements:

1. Security Policy
2. Organization of Information Security
3. Risk Management
4. Asset Management
5. Human Resource Security
6. Physical and Environmental Security
7. Communications and Operations Management
8. Access Control
9. Third-party/supply chain risk management
10. Information Security Incident Management
11. Business Continuity Management
12. Compliance and Legal

NIST CSF Security Policy Review – SilverSky will review customer security policies for compliance with NIST CSF requirements and guidelines. SilverSky will perform a gap analysis of existing Customer policies and procedures against NIST CSF requirements to provide a suggested roadmap for compliance. SilverSky will present all findings during this review to allow for the Customer's remediation of any missing documentation as early as possible. In addition, SilverSky will review the Customer's process documents and plans for all NIST CSF-related requirements (e.g., software development, incident response, access request forms, and termination checklists).

Analysis and Reporting - Analyze the data generated from SilverSky's review. SilverSky will categorize findings and recommendations by risk based on the potential impact of each finding on compliance with the NIST CSF standards. SilverSky will make recommendations to help the Customer formulate a strategic plan to address any non-compliant areas.

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 designed for the Customer's upper management and board of directors and includes:

- 1-page executive summary
- Holistic observations
- Summary of findings for each NIST CSF Function.
- High-level recommendations for addressing deficiencies

SilverSky Proprietary

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

- Itemized listing and description of the areas reviewed
- Identified deficiencies aligned to each of the NIST CSF functions.
- Overall risks associated with deficiencies
- A Plan of Actions & Milestones – Detailed recommendations and timeline priority for addressing deficiencies

2.3 Out of Scope

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

3 Customer Obligations and Assumptions

Services, fees, and work schedule are based upon the assumptions, representations, and information supplied by 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 completion of key project phases, assign resources, and serve as project Liaison.
- **Access** - Ensure SilverSky's consultants have access to key personnel and data requested.
- **Resources** - Furnish SilverSky with the Customer's personnel, facilities, resources, and information, and perform tasks promptly.
- **Cooperation** - Ensure all of Customer's employees and contractors cooperate fully with SilverSky and in a timely manner. SilverSky will advise Customer if an increased level of Customer participation is required for SilverSky to perform the Services under this Service Description.
- **Documentation** - Timely delivery of all documentation requested by SilverSky, including the Customer's security policies, network diagrams, server listings, and procedures.

3.2 SilverSky Assumptions

- Customer will provide SilverSky with reasonably requested information upon which SilverSky can rely to be accurate and complete.
- Customer will provide access to Customer's personnel who have detailed knowledge of Customer's security architecture, network architecture, compute environment, and related.
- Customer will provide access to Customer's personnel who have an understanding of Customer's security policies, regulations, and requirements.
- Customer will evaluate SilverSky's deliverables and immediately notify SilverSky of any perceived problems or issues.
- SilverSky will immediately notify 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 1-2 weeks
S-266-2903 NIST CSF Maturity Assessment	Work hours not to exceed 60 hours.

4.2 Location and Travel Reimbursement

The Services defined in this SOW may 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 incurred for 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.

[End of Document]