

**S-266-3042 GLBA/FINANCIAL COMPLIANCE REVIEW**

## **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**

## SilverSky Proprietary

SilverSky will utilize the information gathered to better focus and streamline the 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 NIST 800-171 security standard.

**Gap Analysis** Evaluate the in-scope processes, systems and applications against the requirements of NIST 800-171 security requirements. SilverSky will examine the security and control structure or related information systems and business processes that are involved in Customer's collection, use and disclosure of credit card data to determine the compliance. During this phase, SilverSky will:

- Interview key system and business stakeholders to identify current policies and practices related to credit card data
- Identify and assess information security risks within key functional areas
- Understand current risk management techniques for addressing security and privacy risks
- Identify deficiencies and gaps in the security practices through control analysis
- Develop detailed recommendations to assist Customer's remediation of deficiencies

SilverSky will review these domains for compliance with the FFIEC's control families listed in the cyber assessment tools, SilverSky will assess each category based on your current maturity levels ranging from baseline, evolving, intermediate, advanced and innovative controls:

- Governance
- Risk Management
- Resourcing
- Training and Culture
- Threat Intelligence
- Monitoring and Analyzing
- Information Sharing
- Preventive Controls
- Detective Controls
- Corrective Controls
- Connections
- Relationship Management
- Incident Resilience Planning
- Detection, Response and Mitigation
- Escalation and Reporting

**Analysis and Reporting** - Analyze the data generated from SilverSky review. SilverSky will categorize the gap analysis by severity depending on the potential impact each gap may have with respect to compliance with the NIST 800-171 security standard. SilverSky

## SilverSky Proprietary

The Detailed Findings Report describes the review results in detail. It's designed 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 Customer requests additional services, such services will be the subject of a change request.

## 3 Customer Obligations and Assumptions

Services, fees and work schedule are based upon the assumptions, representations and information supplied by Customer. 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 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 Customer's employees and contractors cooperate fully with SILVERSKY in a timely manner. SilverSky will advise Customer if an increased level of Customer participation is required in order for SILVERSKY to perform the Services under this Service Description.
- Documentation- Timely deliver 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 upon which SilverSky to be accurate and complete.
- Customer will provide access to Customer's personnel who have detailed knowledge of Customer 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 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 obligations.
- Customer is responsible for any additional costs in the event 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

