

S-266-3042 GLBA/F INANCIAL COMPL program compliance efforts. The assessment procedures are based on CAT tools. This project will focus on Customer policies, procedures, practices and compliance efforts. SilverSky will document identified weaknesses and provide recommendations for security and compliance program.

Project Deliverables:

- x Reports: Executive Summary and GAP/Readiness Detailed Findings

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. Gap Analysis
4. Analysis and Reporting

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 assess the make up of the Customer's IT environment including considerations for outsourced arrangements, network segmentation and third party providers. This preparation and scoping phase is used to:

- x Set expectations regarding the project scope, objectives, activities and associated timetables over the course of the engagement
- x Establish roles and responsibilities for both Customer and SilverSky teams
- x Establish project management standards, including milestone meetings, status reports and ongoing communications with key personnel
- x Facilitate the collection of Customer specific information that is required to complete the gap assessment
 - x Information security policies and procedures
 - x Workforce training program documentation
 - x IT organizational charts
 - x Security software and hardware lists
 - x Interview schedules with key personnel

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 standards.

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:

- x Interview key system and business stakeholders to identify current policies and practices related to credit card data
- x Identify and assess information security risks within key functional areas
- x Understand current risk management techniques for addressing security and privacy risks
- x Identify deficiencies and gaps in the security practices through control analysis
- x 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:

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

Analysis and Reporting - Analyze the data generated from the 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 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 Customer's upper management and board of directors and includes:

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

Project Component	Parameter(s)
Project Start Date	Typically within 30 days of the EffectiveDate
Project Duration	Tier 1: Approximately 1-2 weeks Tier 2: Approximately 2-3 weeks Tier 3: Approximately 3-4 weeks

S266-3042