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 SILVERSKY PCI Gap assessment is to identify potential gaps that may exist in the Customer's ongoing PCI compliance efforts. The assessment procedures are based on the latest PCI Data Security Standards (PCI-DSS) as updated by the PCI Security Council. This project will focus on Customer policies, procedures, practices, information technology (IT) environment and existing compliance efforts. SilverSky will document identified weaknesses and provide recommendations to help the Customer enhance its security and compliance program.

Project Deliverables:

     Reports: Executive Summary and PCI GAP/Readiness Detailed Findings Report

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. Policy Analysis
5. 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 determine the scope of the Customer IT environment that falls under PCI oversight, including considerations for outsourced arrangements, network segmentation and third party processing providers. This preparation and scoping phase is used to:

     Set expectations regarding the project scope, objectives, activities and associated timeQv,urse22mdiof the engagemen   t

Security software and hardware lists
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 the final PCI-DSS security regulation.

Gap Analysis - Evaluate the in-scope processes, systems and applications against the requirements of the PCI-DSS 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 their compliance. During this phase, SilverSky will:

Assess how Customer uses, collects, and discloses credit card information throughout key business, technology infrastructure, relevant systems and business processes
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 associated with credit card data
Understand current risk management techniques for addressing security and privacy risks
Identify deficiencies and gaps in the security practices through targeted tests and control analysis
Develop detailed recommendations to assist the Customer's remediation of deficiencies

SilverSky will review these six domains for compliance with the PCI-DSS requirements:

Build and Maintain a Secure Network
Requirement 1: Install and maintain a firewall configuration
Requirement 2: Do not use vendor-supplied defaults

Protect Cardholder Data
Requirement 3: Protect stored cardholder data
Requirement 4: Encrypt transmission of cardholder data

Maintain a Vulnerability Management Program
Requirement 5: Use and regularly update anti-virus software or programs
Requirement 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures
Requirement 7: Restrict access to cardholder data by business need to know
Requirement 8: Assign a unique ID to each person with computer access
Requirement 9: Restrict physical access to cardholder data

Regularly Monitor and Test Networks
Requirement 10: Track and monitor all access to network resources and cardholder data
Requirement 11: Regularly test security systems and processes

Maintain an Information Security Policy
Requirement 12: Maintain a policy that addresses information security for all personnel

PCI Security Policy and Procedures Review - Review and audit Customer PCI security policies for compliance with PCI requirements and generally accepted industry practices. SilverSky will perform a gap analysis of existing Customer policies and procedures against PCI-DSS 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 PCI-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 the gap analysis by severity depending on the potential impact each gap may have with respect to compliance with PCI security 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 <u>Executive Report</u> 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 SilverSky's findings for each area reviewed during the review
- High level recommendations for addressing deficiencies

The <u>Detailed Findings Report</u> 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 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. 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 of 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 can rely 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 have an understanding of Customer's security policies, regulations and requirements.