SERVICE ORDER ATTACHMENT
STATEMENT OF WORK

S-266-2428 PCI COMPLIANCE AUDIT

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 Payment Card Industry (PCI) qualified security assessor (QSA) Audit and Report of Compliance service is to audit the Customer against the PCI Security Council's data security standard and measure the Customer's PCI compliance efforts. As a QSA of the PCI, SilverSky bases its assessment procedures on the PCI Data Security Standards (PCI-DSS) as updated by the PCI Security Council. This project will focus on performing a comprehensive audit of the Customer's PCI compliance by measuring the existing Customer policies, procedures, practices, information technology (IT) environment and existing compliance efforts against PCI's domains of security. SilverSky will document identified weaknesses and provide a final report on compliance (ROC) that can be submitted to Customer's governing entities.

Project Deliverables:

- Reports: Report on Compliance and Attestation of Compliance

1.2 Project Summary

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

- Preparation and Scoping
- Information Gathering/Discovery
- Gap Analysis
- Policy Analysis
- Analysis and Reporting

Scope

1.3 SilverSky Systems 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's 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 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 collection of Customer's specific information that is required to complete the audit

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

- Prior IT or Operations 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 with key personnel

SilverSky will utilize the information gathered to better focus and streamline the 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.

Audit 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 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 remediation of any missing documentation as early as possible. In addition, SilverSky will review Customer 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 the review to develop a final audit report. SilverSky will develop a list of items that are not satisfactory or are out of compliance with the PCI standard. The Customer will have 60 days to show evidence of compliance with these areas or submit a compensating controls worksheet that details alternative controls in place that meet the PCI criteria.

1.4 Deliverables

At the conclusion of the audit, SilverSky will provide two reports: a comprehensive report on compliance and a letter of attestation on compliance. The Customers will have an opportunity to review drafts of the two reports. SilverSky will deliver a final version after a joint review with the Customer.

Report on Compliance - Formatted in accordance with the requirements set forth in the PCI security standard and includes:

- A detailed breakdown and description of the individually reviewed areas
- Status of compliance within each of the areas reviewed
- Detail of the audit performed on the controls to validate the control
- Overall audit status of the business against the PCI standard

Attestation of Compliance Letter - Formatted in accordance with the requirements set forth in the PCI security standard and includes:

- A letter detailing the scope of the audit and a description of the business
- A summary of the audit results obtained from this assessment
- Key dates and timeframes of the audit work

1.5 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.

2 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.

2.1 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 deliver all documentation requested by SilverSky including Customer's security policies, network diagrams, server listings and procedures

2.2 SilverSky Assumptions

- Customer will provide SilverSky with reasonably requested information SilverSky can rely on 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 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 is unable to 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	Approximately 2-3 weeks, subject to project variables
S-266-2428 PCI QSA Compliance Audit - Tier 3	Organizations with more than 500 Users. Work hours not to exceed 160
S-266-2428 PCI QSA Compliance Audit - Tier 2	Organizations with 251-500 Users. Work hours not to exceed 120
S-266-2428 PCI QSA Compliance Audit - Tier 1	Organizations with less than 250 Users. Work hours not to exceed 80

Pricing is based upon your Tier of service and you are not allowed to downgrade if the engagement last less than your maximum days set forth in the table above.

3.2 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 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.

Location	Scope of Work

3.3 Acceptance

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