SERVICE ORDER ATTACHMENT
STATEMENT OF WORK
S-266-2278 IT CONTROLS 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 Services Summary

The SilverSky Controls Review service addresses critical process areas related to Customer IT security and evaluates the extent to which controls and safeguards have been implemented within those areas. SilverSky will conduct an in-depth review to verify controls through various means such as observation, walkthroughs, and documentation review. SilverSky will compare the controls reviewed to the Customer's existing corporate policies and standards as well as to generally accepted industry standards and guidelines. SilverSky will provide detailed documentation of any deficient or non-compliant controls identified and recommend how to address them.

The SilverSky methodology is largely based on specific guidelines defined by industry experts such as NIST (National Institute of Standards and Technology) and ISACA (Information Systems Review and Control Association).

Project Deliverables:

- Reports: Executive Report and Detailed Findings Report

1.2 Project Summary

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

1. Kick-off Meeting
2. Information Gathering/Discovery
3. Controls Review
4. Analysis and Documentation
5. Reporting

2 SCOPE

Typical areas reviewed during IT Controls Review include:

1. Management
2. Systems Development and Acquisition
3. Operations
4. Contingency Planning
5. Information Security Systems
6. Network Security Controls and Architecture

Management

SilverSky will interview Information Technology (IT) personnel and/or review departmental policies to determine:

- If the organizational structure provides for effective company-wide IT support
- The process of granting of administrative rights and privileges
- Whether the appropriate segregation of duties exists
- If authority, responsibility, and technical skills are clearly defined
- If hiring, training and succession processes are adequate

Systems Development & Acquisition

SilverSky will review the adequacy of system development processes and activities such as development standards/methodologies, adherence to standards, adequacy of quality assurance programs, selection process and review of third party vendors, and sufficiency of standards relating to change management.

Operations

SilverSky will evaluate operating procedures and manuals as they apply to Customer computer and IT operations and controls. This includes processes such as adequacy of IT equipment inventory listings, environmental controls, physical security, performance and availability monitoring, help desk function, and backup procedures.

Contingency Planning

SilverSky will examine the existing contingency planning process and whether Customer has established an ongoing, process-oriented approach to business continuity planning that is appropriate for the size and complexity of the business. This process should include a business impact analysis (BIA), a risk assessment, risk management, risk monitoring, and testing. Overall, this planning process should encompass the Customer's business continuity strategy, which is its ability to recover, resume, and maintain all critical business functions.

Information Security Systems

SilverSky will:

1. Review all critical information systems, associated databases, and system architecture with respect to how information is processed, stored, and accessed
2. Determine whether critical information systems have designated administrators and/or data owners and
    a. determine if a formal process is in place by which designated administrators evaluate and approve all system access requests and changes to the system; and
    b. if users are adequately trained on the system and understand how to securely handle any information and data associated with it
3. Evaluate capabilities within the system to manage user rights and permissions at a granular level; review the system user base to ensure access levels match current job responsibilities

4. Review the effectiveness of access controls for system users considering the type of information accessed

Network Security Controls and Architecture

SilverSky will review Customer network controls, security controls, network architecture diagrams and topologies to understand the physical location of and interrelationship between hardware and security devices, various locations, and 'untrusted' networks. SilverSky will review the adequacy of technical security standards, the network authentication process, review capabilities, and access control change procedures. SilverSky will also assess the effectiveness of controls regarding network user accounts, password administration, firewall technology, and remote access methods.

2.1 SilverSky Obligations:

Information Gathering Phase - Gather and examine Customer's IT controls documentation such as controls policies and procedures, network diagrams, results from prior assessments or audits, reviews, vendor agreements, and the current disaster recovery plan.

Controls Review Phase - Interview key personnel responsible for implementing the Customer's controls in the core areas under review. These interviews typically involve IT and systems administrators as well as information security and compliance officers. SilverSky will use the interviews to assess the extent to which existing policies and controls have been implemented. SilverSky will also do walkthroughs of physical facilities and key IT systems to review and validate various controls in areas such as access/authentication, configuration, logging, architecture, physical security, and redundancy.

Analysis and Documentation Phase - SilverSky will compile and review the information gathered, then analyze and document in detail the findings and any test results in a draft iteration of the final reports.

Reporting Phase - SilverSky will present and disseminate the findings to the Customer's project manager and other key personnel. Any issues, questions, and/or concerns will be discussed and addressed. Once completed, SilverSky will issue a final copy of the review reports.

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

- One-page executive summary
- Concise list of the key findings
- Summary of SilverSky's findings for each area reviewed during the evaluation
- High-level recommendations for addressing deficiencies

The Detailed Findings Report describes the review results in detail. It is intended 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 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.

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, computing environment, and related matters.
- 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's obligations.
- Customer is responsible for any additional costs if that 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	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-266-2278 IT Controls Review (onsite)- Tier 3	Organizations with less than 500+ Users. Work hours not to exceed 80
S-266-2278 IT Controls Review (onsite)- Tier 2	Organizations with less than 251-500 Users. Work hours not to exceed 60
S-266-2278 IT Controls Review (onsite)- Tier 1	Organizations with less than 250 Users. Work hours not to exceed 40

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

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 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**

4.3 Acceptance

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