SERVICE ORDER ATTACHMENT
STATEMENT OF WORK
S-266-2030 IT RISK ASSESSMENT

OVERVIEW

This Statement of Work ("SOW"), with any appendices included by reference, is part of any agreement which incorporates this document by reference.

Services Summary

SILVERSKY IT Risk Assessment services identify and measure known risks affecting Customer's private information through the analysis and prioritization of information assets, threats, and existing controls and safeguards. SILVERSKY bases its methodology largely on specific guidelines defined by industry experts such as NIST (National Institute of Standards and Technology) and ISACA (Information Systems Audit and Control Association). Depending on the scope of the project, SILVERSKY' assessment can include review of Customer's systems and environment from the perspective of Customer's specific regulatory requirements, such as GLBA or HIPAA.

SILVERSKY' assessment methods consider three core principles of information assurance defined by the security industry's CIA triad model standards:

- Confidentiality - assurance of information privacy
- Integrity - assurance of information accuracy and completeness
- Availability - assurance of timely and reliable access to information

Project Deliverables:

- Reports: Executive Report and Detailed Findings Report

Project Summary

SILVERSKY will provide the following primary tasks, subject to modification or extension based on the investigation findings.

1. Kick-off Meeting
2. Information Gathering/Discovery
3. Threat Assessment
4. Risk Assessment
5. Reporting

SCOPE

SilverSky Obligations:

Information Gathering - Identify, categorize, and rank critical information assets within Customer's organization according to criticality and sensitivity. SILVERSKY considers any equipment that handles,

contains, or processes Customer's or its customers' information, or facilitates those functions, to be an information asset.

SILVERSKY familiarizes itself with Customer's environment and information infrastructure. SILVERSKY gathers and reviews relevant documents (e.g., network diagrams, server/device inventory lists, application inventory lists) and interviews key personnel to establish an understanding of Customer's network architecture and the different information systems utilized.

Once SILVERSKY understands Customer's environment, SILVERSKY identifies and groups the information assets into these categories:

- Information Systems - applications such as data processing, reporting, websites
- Information Technology - equipment such as servers, workstations, firewalls
- Physical Information - items such as hard copy reports, backup tapes

SILVERSKY will develop a profile of each asset detailing its general function, purpose and essential components or features.

SILVERSKY will rank each information asset based on the CIA triad. SILVERSKY will collaborate with Customer to refine the assessment scope and determine which information assets to focus on during the remaining phases of this assessment.

Threat Analysis - Create a comprehensive threat profile for each critical information asset. SILVERSKY views anything that could result in unauthorized disclosure, misuse, alteration, or destruction of information or information assets as threats. SILVERSKY reviews reasonable and foreseeable threats to Customer's assets with respect to each asset's confidentiality, integrity and availability. Threat analysis covers a broad spectrum of potential threats; it accounts for those that originate externally or internally as well as those that are technical or non-technical. SILVERSKY works with Customer and uses Customer's industry and security knowledge to assess the potential risks different threats pose to its information assets. SILVERSKY prioritizes and rates each threat according to its likelihood of occurring and its impact if realized.

Threats assessed are logically grouped and may include, but are not limited to:

- Data interception
- Data corruption
- Data theft
- Data entry or modification error
- Environmental hazards
- Malicious code (viruses, worms, spyware, etc.)
- System failure
- Unauthorized access

Risk Analysis - Determine the extent to which Customer mitigates or reduces risks from various threats to information assets. This review consists primarily of interviews with key personnel, system and facility walkthroughs, and reviewing Customer's existing documents -- such as security policies and procedures. Again, SILVERSKY uses the CIA triad to rate Customer's controls in terms of the degree to which Customer implements them and their relative efficacy in addressing specific threats.

Some key control areas SILVERSKY assesses include:

- Access controls (granting rights, authentication process, etc.)
- Audit and review procedures
- Contingency planning and procedures
- Data consistency and verification procedures
- Data handling procedures
- Physical security
- Network security
- Security monitoring and incident response
- Security roles and responsibilities
- Service provider contracts

SILVERSKY compiles, reviews, and compares information gleaned from its risk analysis to the results from the threat analysis to determine the overall risk level for each information asset. After analyzing and defining assets and associated risks, SILVERSKY develops key recommendations to help Customer mitigate or address high-risk areas.

Deliverables

SILVERSKY will provide an Executive Report and a Detailed Findings Report following its assessment.

The Executive Report is a high-level summary of the assessment intended for Customer's upper management and board of directors and includes:

- One-page executive summary
- Summary of the risk ratings for each information asset reviewed during the assessment
- Concise list of the key findings and recommendations grouped according to these asset categories:
    - Information Systems - applications such as data processing, reporting, websites
    - Information Technology - equipment such as servers, workstations, firewalls
    - Physical Information - items such as hard copy reports, backup tapes
- Comprehensive information security plan detailing SILVERSKY' suggested safeguards and process recommendations
- Recommended schedule for performing and testing specific controls

The Detailed Findings Report describes the assessment results in detail. It is intended for mid-level management, administrators, and other operations personnel. This report corresponds closely with the three phases of the assessment and includes:

- Itemized listing and description of Customer's individual information assets
- Identified potential threats affecting assets
- Existing controls and safeguards
- Overall risks associated with each asset and threat

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.

CUSTOMER OBLIGATIONS AND ASSUMPTIONS

Services, fees, and work schedule are based upon the assumptions, representations and information supplied by Customer. Customer's fulfilment of these responsibilities is critical to the success of the engagement.

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 and 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 SOW.
- **Documentation** - Timely deliver all documentation requested by SILVERSKY including Customer's security policies, network diagrams, server listings and procedures

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 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.
- 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 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.

PROJECT PARAMETERS

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	Typically within 30 days of Effective Date
Project Duration	Approximately 3 weeks, subject to project variables
	Consulting Days not to Exceed
IT Risk Assessment (advanced)	29
IT Risk Assessment - (core)	7

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.

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, 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 Customer if Customer requires an itemized statement of such expenses.

Location	**Scope of Work**

Acceptance

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