

**[CLIENT]**

**Vulnerability and Compliance Management**

**Statement of Work #XX**

# **Governing Agreement**

This Statement of Work (including its attachments, if any) is entered into by [CLIENT], Inc. (“Company” and “[CLIENT]”), a subsidiary of [CLIENT], Inc., and [CLIENT] Advisory Services LLC (“Supplier” and “[CLIENT]”) and is by this reference subject to and incorporates herein the terms of the Master Services Agreement by and between [CLIENT], Inc., (“Company”) and [CLIENT] LLC (“[CLIENT] LLP” or “[CLIENT]”:) as previously amended, (the “Agreement”). Capitalized terms used but not defined in this SOW shall have the meanings given to them in the Agreement.

# **1.0 Name of Supplier and Supplier’s Primary Project Lead**

# [CLIENT] Advisory Services, LLC ([CLIENT])

# Engagement Partner = James Doe

# Project Lead = John Smith

**2.0 [CLIENT] Primary Project Manager/Title (Name, Title, Department Name)**

John Smith, Manager, Infrastructure, [CLIENT]

James Doe, Information Security Advisor, [CLIENT]

# **[CLIENT] Governance Policy for Consulting Services**

Effective September 2015, [CLIENT] launched a new [CLIENT] Consulting Governance Policy (the “Governance Policy”) for all projects for consulting services. Specifically the Governance Policy requires the following:

1. All projects over **$750,000,** including any subsequent follow-on phases (e.g. Phase 2), shall be competitively bid via formal RFP process, or
2. If no RFP is conducted, the sole-sourced supplier shall be subject to a mandatory overall discount **equal to or greater than 20%** as compared to the supplier’s MSA rate card with [CLIENT].
3. All projects over **$500,000** shall require a completed “Business Justification Form” which shall clearly identify the expected value to be achieved from the project (part one) and subsequently the value actually realized by [CLIENT] post-engagement (part two).

# **4.0 Background**

[CLIENT] has been engaged to assist the [CLIENT] Desktop Management Team in 1) advising remediation of existing vulnerability backlogs and 2) assessing the efficiency and efficacy of its existing desktop security management processes, with both endeavors scoped to roughly 1,500 endpoints. Doing so will minimize current and future vulnerability remediation times and limit program risk. The project will include identification of critical security processes requiring realignment, deployment of the Tanium solution to in-scope desktop assets, and guidance of resulting remediation efforts against applicable configuration standards, including DISA STIGs.

The engagement will assist [CLIENT] in current and future desktop vulnerability remediation through workshops, walkthroughs, technical agent deployment, prioritizing of existing backlog remediation, and more. The existing vulnerability program assessment along with Tanium and DISA STIGs deployment will take approximately fourteen (14) weeks. The existing vulnerability backlog remediation advisory effort for the fifteen hundred (roughly 1,500) in-scope endpoints will take approximately sixteen (16) weeks and will occur concurrently with the aforementioned first workstream.

**5.0 Definitions**

All capitalized terms used herein shall have the meanings given to them pursuant to the Agreement unless otherwise set forth herein. The following additional definitions shall apply to this SOW.

| **Term / Acronym / Abbreviation** | **Definition / Description** |
| --- | --- |
| **DISA** | Defense Information Systems Agency |
| **STIGs** | Security Technical Implementation Guides |
| **Tanium** | A Risk & Compliance solution that is deployed on endpoints to simplify identifying and remediating vulnerabilities and patch processes. |

# **Project Scope, Objectives and ROI**

## ***Project Scope***

## Vulnerability Program Exploration & Tanium Deployment

## Identify and interview key desktop management personnel while assessing relevant security documentation to understand current desktop vulnerability management processes.

## Deploy the Tanium solution across in-scope endpoints.

## Tanium Configuration, Analysis, and Program Recommendations

## Configure the Tanium solution with necessary policies or DISA STIGs benchmark requirements, where applicable.

## Leverage configured Tanium capabilities to identify underlying sources of existing and future vulnerabilities.

## Develop recommendations for desktop management personnel resulting from the insights provided by interviews, existing documentation, and findings from Tanium.

## Document the recommendations as newly defined vulnerability management processes, including those concerning the usage of Tanium and DISA STIGs, in existing desktop management documentation (policies, procedures, guidelines, etc.).

## Existing Vulnerability Backlog Remediation

## Once Tanium is installed during the Phase 1 workstream, concurrently leverage the solution to advise [CLIENT] on how to efficiently remediate the accumulated backlog of vulnerabilities.

* 1. ***Project objectives***

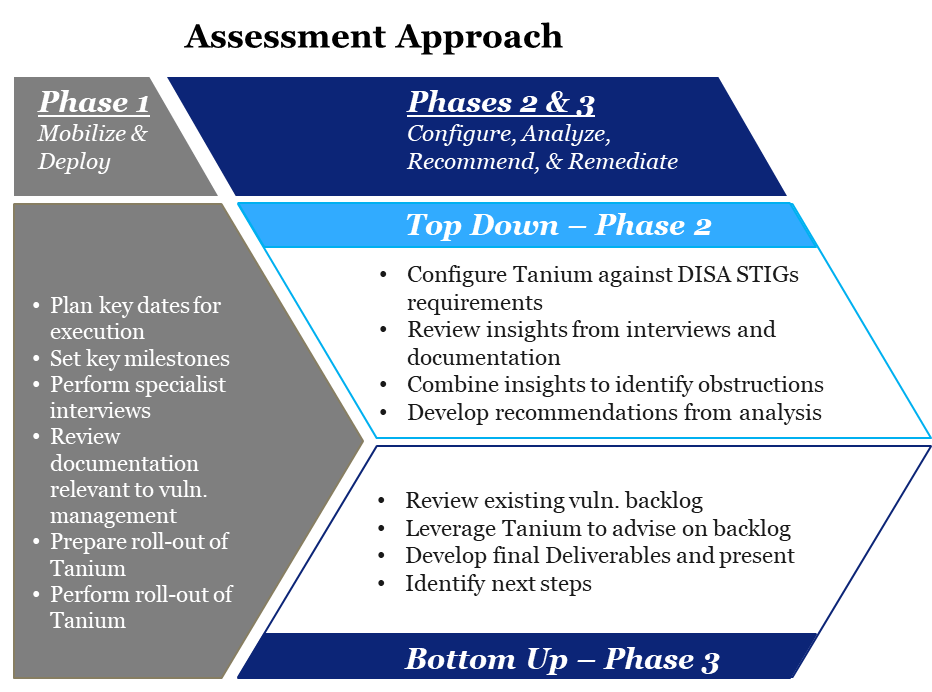
The [CLIENT] team will be utilizing a three-phase process when performing the assessment, transformation, and remediation of Vulnerability and Compliance Management processes and its associated vulnerability backlog within the in-scope desktop management unit.

The engagement will commence with Phase 1, during which the engagement plan and assessment timeline is established, and exploratory interviews about the program lead into Tanium agent deployment for in-scope endpoints.

Upon completion of Phase 1, Phases 2 and 3 will occur simultaneously. Phase 2 will be focused on the “top down” configuration of the recently deployed Tanium agents against DISA STIGs requirements, along with the development and documentation of updated vulnerability management processes as informed by [CLIENT]’s recommendations for the desktop management team. As this “top down” workstream continues, Phase 3 will simultaneously continue from a “bottom up” approach; insights from the deployed Tanium agents will inform guidance of remediation of the existing vulnerability backlog for the roughly 1,500 in-scope endpoints.

The near-simultaneous conclusions of the “top down” Phase 2 and “bottom up” Phase 3 will mark the end of the engagement along with completion and presentation of final Deliverables.

## **7.0Approach and Timeline**



## ***7.1 Phase 1 – Mobilization and Tanium Deployment***

## Phase 1 will focus on project initiation and setup, along with Tanium agent deployment. The [CLIENT] team will first begin by completing the project plan for the engagement which will outline the key activities and responsibilities of the team throughout the three phases of execution. The team will then perform exploratory interviews with key desktop management personnel and ~~review relevant~~analyze relevant vulnerability management documentation. Finally, the team will deploy the Tanium agent across roughly 1,500 in-scope endpoints to leverage in Phases 2, 3, and beyond.

| **Phase 1 Activity** |
| --- |
| Develop and collaboratively finalize the engagement project plan |
| Communicate goals and methodologies to [CLIENT] |
| Establish key dates |
| Conduct project kickoff with [CLIENT]’s identified stakeholders |
| Establish weekly status cadence |
| Perform interviews with key desktop management personnel |
| Request and analyze documentation relevant to vulnerability management program |
| Prepare and deploy Tanium to endpoints to facilitate the data-driven analysis and remediation in Phases 2 and 3 |

## ***7.2 Phase 2 – Tanium Configuration, Analysis, and Program Recommendations***

## Phase 2 will act as the “top down” approach of the latter half of the engagement. It will focus on the proper configuration of the recently deployed Tanium solution, data-driven analysis of fundamental causes of the existing vulnerability accumulation, and the resulting development of recommendations and documentation updates for the vulnerability management program using those insights from the analysis.

| **Phase 2 Activity** |
| --- |
| Begin technical tool readiness (Tanium) |
| Conduct test of Tanium |
| Configure Tanium against integrated DISA STIGs requirements |
| Execute the technical security analysis assessment (Tanium) |
| Analyze insights from specialist interviews and documentation analysis in Phase 1 |
| Combine insights from Phases 1 and 2 to identify obstructions in existing program |
| Develop recommendations for desktop team using subject matter expertise |
| Advise on documentation updates to reflect best practices and recommendations |

## ***7.3 Phase 3 – Existing Vulnerability Backlog Remediation***

## Phase 3 will concurrently act as the “bottom up” approach of the latter half of the engagement. It will focus on utilizing the installed Tanium agents to expedite remediation guidance concerning the existing vulnerability backlog identified by the desktop management team. Phase 3 will conclude simultaneously with Phase 2 with the development and delivery of the Deliverables.

| **Phase 3 Activity** |
| --- |
| Analyze and prioritize existing vulnerability backlog with key stakeholders |
| Leverage Tanium solution to advise on clearing backlog of open items |
| Develop and deliver Executive Summary |
| Develop and deliver vulnerability recommendations report |
| Develop and deliver program recommendations report |
| Perform executive readout with [CLIENT] stakeholders |
| Identify Next Steps for [CLIENT]’s consideration |

* 1. **Relationship Management and Governance**

Supplier shall provide day to day management of resources included in the delivery of Services outlined in this SOW to achieve the Deliverables as described herein.

## ***Meetings***

Supplier shall, at no additional charge, make available to [CLIENT] such Supplier personnel in such frequency to meet and confer with [CLIENT] to discuss the topics instructed by [CLIENT].

## ***Escalation Management***

Any dispute between the parties shall in the first instance be referred to the Relationship Manager from each party, as identified on page one of this SOW, who shall use reasonable efforts to attempt to resolve the dispute through good faith negotiations. If they fail to resolve the issue, such items shall be escalated to senior leadership within each party.

## ***Reports***

Supplier shall, at no additional charge, the following reports to [CLIENT], in form and substance reasonably required by [CLIENT]:

* + 1. Weekly Project Status Reports
    2. And such other reports as reasonably required by [CLIENT]

## ***Service Levels***

* + 1. Supplier will complete the evaluation within the budget provided in section 16 below.
    2. Supplier will complete the Deliverables to a quality standard that is acceptable to [CLIENT].
    3. Supplier will complete the evaluation within the timeframe in section 7 above.

**9.0 Intellectual Property (detail out any exceptions to MSA)**

N/A

# **Deliverables**

* 1. ***Schedule for Deliverables and/or Key Milestones:***

| **Deliverable and/or Critical Milestone** | **Deliverable (or Critical Milestone) Description and Acceptance Criteria** | **Planned Start Date** | **Target Completion Date** |
| --- | --- | --- | --- |
| Executive Summary of Key Findings and Focus Areas | **Description:** The executive summary presentation will provide a high-level overview of the scope of work, identified weaknesses in the program, opportunities for improvement, overview of Tanium deployment and vulnerability remediation, and key next steps.  **Acceptance Criteria:** [CLIENT]’s reasonable satisfaction | 7/18/2022 | 7/29/2022 |
| Vulnerability Remediation and Recommendations Report | **Description:** This report will describe, in depth, metrics detailing the impact of Tanium and its DISA STIGs configuration on the in-scope endpoints and the key numbers informing stakeholders on the effectiveness of the vulnerability backlog remediation.  **Acceptance Criteria:** [CLIENT]’s reasonable satisfaction | 7/6/2022 | 7/29/2022 |
| Program and Process Recommendations Report | **Description:** This report will define, in-depth, opportunities for the desktop management team to update its documentation (policies, procedures, guidelines, etc.) to reflect improved processes and technologies in the vulnerability management program moving forward.  **Acceptance Criteria:** [CLIENT]’s reasonable satisfaction | 7/6/2022 | 7/29/2022 |
| Engagement Project Plan | **Description:** The project plan will identify key tasks and approximate timelines throughout each phase of the assessment.  **Acceptance Criteria:** [CLIENT]’s reasonable satisfaction | 4/4/2022 | 4/15/2022 |
| Engagement Status Reports | **Description:** The weekly project status reports will detail the project status, economics, issues, Deliverables and next steps  **Acceptance Criteria:** [CLIENT]’s reasonable satisfaction | 4/4/2022 | 7/29/2022 |

* 1. ***Deliverables Repository***

Supplier will make available final version copies of all Deliverables to [CLIENT] for the purposes of maintaining a central, searchable repository of all consulting project Deliverables. This knowledge transfer will be accomplished as an attachment upload of the various Deliverable reports, included with the final invoice in Fieldglass. [CLIENT]’s approval for payment of the final invoice will not be given until the Deliverables are attached accordingly in Fieldglass. Should any Change Requests be generated as subsequent work to the SOW, a zip file of the SOW Deliverables will be a required element prior to the approval of any subsequent Change Request.

* 1. **Acceptance**

In addition to the Acceptance Criteria above, all Deliverables and Services shall be delivered by Supplier to [CLIENT] in accordance with the terms of the Agreement and in compliance with [CLIENT]’s standard/compliant processes and guidelines. Further specific Acceptance Criteria may be mutually agreed by the Parties in the applicable Work Order.

## ***Acceptance Process***

The Acceptance process shall be as set forth in the Agreement.

**12.0 RACI**

The Deliverables described below apply to the scope of the Services. The roles will range from:

* **Responsible**: Party which is the "doer" of the work. They must complete the task or objective or make the decision.
* **Accountable**: Party which must finally sign off or approve when the task, objective or decision is complete. This person must make sure that responsibilities are assigned in the matrix for all related activities. Success requires that there is only one Party *Accountable*, which means that "the buck stops there."
* **Consulted**: Party which must give input before the work can be done and signed-off on. These people are "in the loop" and active participants.
* **Informed**: Party which must be kept "in the picture." They need updates on progress or decisions, but they do not need to be formally consulted, nor do they contribute directly to the task or decision.

| **Deliverable** | **Item/Task** | **Supplier’s Role** | **[CLIENT]’s Role** |
| --- | --- | --- | --- |
| Deliverable #1 | | | |
| *Executive Summary of Key Findings and Focus Areas* | N/A | R | C |
| Deliverable #2 | | | |
| *Vulnerability Remediation and Recommendations Report* | N/A | R | C |
| Deliverable #3 | | | |
| *Program and Process Recommendations Report* | N/A | R | C |
| Deliverable #4 | | | |
| *Engagement Project Plan* | N/A | R | C |
| Deliverable #5 | | | |
| *Engagement Status Reports* | N/A | R | C |

**13.0 Permitted Subcontractors**

Subcontractors will not be used to deliver Services or Deliverables under this SOW. The addition of, or modifications to, previously approved subcontractor(s), if any, requires [CLIENT]'s prior written approval in each instance. For the avoidance of doubt and clarification purposes, Supplier may use [CLIENT] Subcontractors (as defined in Section 15.1) for internal administrative and/or regulatory compliance purposes (including, but not limited to, the use of global cloud hosted email and collaborative solution tools).

# **14.0 Knowledge Acquisition / Knowledge Transfer / Responsibility Transfer**

[CLIENT] will transition any requisite knowledge to [CLIENT]-identified individuals at the end of this project.

* 1. **Staffing & Roles**

The members of the project team, as well as stakeholders, identified for the Supplier resources.

| **Staff** | **Role** |
| --- | --- |
| Tim Stoner | Engagement Leader |
| Bryon Blohm | Senior Subject Matter Specialist |
| Jessica Martin | Senior Subject Matter Specialist |
| Manager TBD | Vulnerability Management Specialist |
| Manager/SA TBD | Tanium Deployment Specialist |
| TBD | Technical Analyst |
| TBD | Technical Analyst |

# ***Additional Investments by Supplier***

N/A

* 1. **Compensation and Fees:**

## ***Type of Compensation***

☒ Fixed Fee

☐ Time & Materials

## ***Finances***

This project will start on **4/4/2022** and complete by **7/29/2022.** The total fees for this engagement will be fixed/not to exceed **$797,000**. Total fees for labor shall not exceed $**797,000** and there are no expected expenses. This fee is based on the assumptions and scope outlined in this Statement of Work and will be invoiced upon the completion in accordance with the requirements of this Statement of Work and acceptance of the final deliverable.

**Note:** Anything beyond Maximum Funding Limit and up to the Total Budget for the PO is considered Contingency and can only be released as per [CLIENT] approved change orders.

## ***Payment Schedule***

| **Milestone or Deliverable Name** | **Delivery Date** | **Invoice-able Amount (fees only)** |
| --- | --- | --- |
| Completion of Phase 1 | 5/13/2022 | $175,000 |
| Completion of Phase 2 | 07/29/2022 | $175,000 |
| Completion of Phase 3 | 07/29/2022 | $447,000 |

**17.0 Other Statement of Work Terms and Key Assumptions**

This Statement of Work is based on the following key project assumptions. Material deviations from these assumptions that arise during the proposed project will be managed through the procedure described in the Project Change Request. Assumptions identified within the Master Services Agreement still apply unless noted and agreed upon.

| **Category** | **Assumptions** |
| --- | --- |
| 1. Termination for Convenience | There shall be no fees or charges of any kind for [CLIENT]’s termination for convenience, other than for Fees and Expenses otherwise due and payable by [CLIENT] for Services rendered in accordance with the terms of the Agreement and the SOW prior to the effective date of termination. |
| 2. Engagement | 1. The project will focus on the Desktop Management Team’s identified roughly 1,500 endpoint environment from a scope perspective and will not include environments outside these assets. 2. [CLIENT] will perform the interviews, documentation analysis, compilation of results and the overall project on-site or remotely, as required. 3. All Deliverables will be in [CLIENT] branding. Reports will be provided in MS PowerPoint format or other as determined by the project team. 4. [CLIENT] will provide working papers (document request responses, system architecture, network diagrams, system workflow traceability and interface diagrams, prior audit findings and other project documentation) as requested by [CLIENT], within a timely manner (typically 24 hours, unless otherwise agreed to) to support this specific engagement.    1. [CLIENT] data will be encrypted when being shared with [CLIENT]. [CLIENT] will restrict access to the shared data to only those who need to know. [CLIENT] will not leverage collaboration tools with the [CLIENT] data provided. [CLIENT] will delete from hard drives any [CLIENT] data provided as a result of this work. 5. [CLIENT] will provide a dedicated resource (single point of contact) available to help identify and coordinate [CLIENT] resources (system and project teams) to support project activities at the onset of the project. 6. [CLIENT] is responsible for coordinating participation for meetings for needed individuals. [CLIENT] will work with [CLIENT] to identify the appropriate type of individuals and teams to participate in meetings. Requested meetings will be scheduled within 3 business days of making the request. 7. All deliverables will be deemed 'Accepted' after a five (5) day business period unless feedback is received by the [CLIENT] team prior to the end of the tenth day. 8. [CLIENT] will not provide legal advice, legal opinions, AICPA audit, or attestation services during this engagement. |

| 3. Data Required | Data files and data file types will be identified during the engagement’s interview process and requested by the [CLIENT] team as necessary. Commonly requested file types include:   1. Word Documents (.docx, .doc, etc.) 2. PDF Documents (.pdf) 3. Excel Documents (.xlsx, .csv, etc.) 4. Pictures (.jpg, .jpeg, etc.) 5. PowerPoint Documents (.pptx, .ppt, etc.)   All data file types are inclusive within the 2022 June TDL Submission provided by [CLIENT]. |
| --- | --- |
| 4. Protected Health  Information (“PHI”) | Supplier will not receive any PHI under this SOW. |

# **18.0 Supplier Diversity**

[CLIENT], Inc.'s Supplier Diversity Program has established annual goals of expenditures with Minority-Owned/Women-Owned/Veteran-Owned/Service-Disabled Veteran- Owned/Gay, Lesbian, Bi-sexual, and Transgender (GLBT)-Owned Businesses. As part of this Program and as one of your business solutions to [CLIENT], Inc., Supplier will participate in [CLIENT]'s Supplier Diversity reporting program where the vendor is expected to report quarterly on direct (diversity spend attributable to [CLIENT]) and indirect (diversity spend not attributable to [CLIENT]) spending by your company. [CLIENT]’s 2017 goal for supplier diversity is 12.1%, and the Supplier will partner with [CLIENT] to actively achieve this goal.

# **[Signatures to follow on the next page]**

**19.0 Electronic Signatures**

The Parties expressly agree that electronic signatures may be utilized for execution of the Agreement and any attachments thereto, including but not limited to, this Statement of Work. The Parties acknowledge and agree that (i) the issuance of an electronic signature shall be valid and enforceable as to the signing Party to the same extent as an inked original signature; and (ii) these documents shall constitute “original” documents when printed from electronic files and records established and maintained by either Party in the normal course of business.

|  |  | [CLIENT], Inc. |
| --- | --- | --- |
| Supplier |  | [CLIENT] |
| By: |  | By: |
| Signature |  | Signature |
| Printed Name |  | Printed Name |
| Title |  | Title |
| Date |  | Date |



[CLIENT] Internal Use Only:

| One [CLIENT] Initiative ID #’s (directly supporting, indirectly support, or reasoning why this initiative is not captured in a Transformation Initiative ID) |  |
| --- | --- |
| Cost Center(s) funding – provide % or $$$ amounts if more  than one |  |
| GL Account(s) - provide % or $$$ amounts if more than one |  |
| Labor Categorization (Strategy vs. Specialized Labor) |  |
| Commodity Code |  |
| Finance Contact |  |
| BIG Contact(s) (if applicable) |  |
| AVMO Contact (if applicable) |  |