|  |  |
| --- | --- |
| ReadyPool Technical Services  3119 Bourbon Street Circle Rockwall, TX. 75032 |  |

SOW 791: Professional Services for Client Name

|  |  |  |
| --- | --- | --- |
| Date | Services Performed By: | Services Performed For: |
| June 14, 2021 | ReadyPool Technical Services  3119 Bourbon Street Circle | Client Name  Client Address, City, ST ZIP Code |

**Executive Summary**

ReadyPool Technical Services DBA NIST Assist, will engage with client to provide an intense 90-day sprint with the Primary Objective of instituting a Defendable Risk Management Program. There are many facets to this objective, and they can be listed in a type of maturity continuum as follows:

* Risk Management (includes Risk Register and regular curated meetings)
* Incident Response Program (includes tabletop, attack simulator, practical application of recovery)
* Training and Awareness (includes Insider Threat Program)
* Security and Compliance (includes an executive dashboard that reflects the current state of risk overall, data loss prevention mechanisms, policy and policy acknowledgements, security best practice)
* Continuous Integration and Agile Frameworks (identify where can we improve a business process - may include COBITS)
* Establish Zero Trust / Agile best practices (enables continuous improvements)

While this continuum only scratches the surface of what we will accomplish, the idea here is to establish a roadmap that depicts where you are on the road of digital transformation as a whole (which includes Security and Compliance), the short- and long-term cost impacts of things like automation, and strategies to traverse the next 3 years such that your organization will continue to mature using agile methodologies. It is important to understand the concept of the continuum approach, whereby each milestone enables milestones further downstream. There is a very specific order that must be followed to satisfy “Duty of Care”. The project management style will be agile, with regular weekly scrum meetings and sprints in between.

Later in this document we highlight the overall objective of the program as an exercise in documenting evidence of your efforts to identify, prepare, and cope with a cybersecurity incident or ANY disruption to business through continuous review and improvement. This is an important abstract to take away from our engagement and requires buy in and participation at a fundamental level. The key here is to identify where intellectual property can be monetized, or at least homogenized, and correlate that with your Risk Register such that the majority of your capital expenditure has a direct, and often measurable impact on your bottom line through the “security and compliance” gate. In other words, how do we capitalize on this process? NIST Assist relies on government agencies, industry associations, and departments like the National Institute of Standards and Technology, under the Department of Commerce to answer these and other comprehensive and often abstract questions. Everything we are prescribing is readily available to the general public through Special Publications and regulations from various agencies and industry associations. This statement of work focuses on the proprietary way in which we go about instituting these practices in ways you might not expect or may seem counterintuitive at times. Nevertheless, if you approach security and compliance as a mechanism to enable efficient and repeatable business processes, you will find new opportunities while streamlining your core business.

This Statement of Work (SOW) is issued pursuant to the Consultant Services Master Agreement between Client Name (“Client”) and Company Name (“Contractor”), effective Date (the “Agreement”). This SOW is subject to the terms and conditions contained in the Agreement between the parties and is made a part thereof. Any term not otherwise defined herein shall have the meaning specified in the Agreement. In the event of any conflict or inconsistency between the terms of this SOW and the terms of this Agreement, the terms of this SOW shall govern and prevail.

# Period of Performance

The Services shall commence on or about June 18, and shall continue through September 27, or in the absence of an official start date for a period not to exceed 91 days. After 91-days Client and Contractor will negotiate in good faith a practical long term Managed Service or Employment Agreement commensurate with identified requirements / level of effort (documented in recommended actions located in your Security and Compliance console).

# Engagement Resources / Assumptions

* Access to location during business hours and some off hours pending approval.
* Approximately 20 to 30 hours onsite per week, with private workspace and lockable doors / cabinets.
* Mutual NDA, and agreement not to share content of this SOW, or other information provided during negotiations or work performance that expose the methods used, or other properly marked proprietary content, to third parties not directly associated with the execution of this scope of work.
* Client will provide a notebook computer of adequate performance to conduct all work and will retain ownership of said notebook in perpetuity.
* Client agrees to fund minimum licensing levels for service accounts, advanced threat protection services, or other licenses that may be required to complete a deliverable, or in lieu of such, an equivalent system of record, service, or entity to provide an alternate or Compensating Control as needed or required.
* Client agrees to name NIST Assist as the Digital Partner of Record (DPOR) where applicable, including enrollment in Microsoft Commercial Services, or named Cloud Solution Provider (CSP), or enrollment in a CSP Program if needed or where applicable. (This enables a number of enterprise class resources provided by Microsoft that are too numerous to list here)
* Authority by proxy to invoke policy and direct HR resources to task (I will need to tell some of your IT people what to do).

# Scope of Work

Contractor shall provide the Services and Deliverable(s) as follows:

* Institute a comprehensive Risk Management Program in conjunction with existing System Security Plan (SSP) or equivalent Plan of Action and Milestones (POEM) derived or produced as a result of previous security and compliance remediation.
* Establish a Security and Compliance baseline and directive, to include a full compliance discovery effort to identify all compliance standards.
* Establish a Security and Compliance baseline and directive, to include written policy and procedures in a System of Record that uses a compliant Records Management system (and associated File Plan), approval process, and other controls as directed or exposed in discovery.
* Establish, document, and implement written policies for Security Domain(s) (part and parcel to boundary analysis which is a component of a self-assessment)
* Establish, document, or otherwise implement key “programs” as subsets of systems and software, to include Training and Awareness Program and / or Insider Threat Program (this may include any “program” from the policy baseline or Compensating Control identified in ongoing assessment).
* Unify or segregate as necessary Directory Services and validate efficient and trustworthy authentication methods across the enterprise.
* Establish, document, and implement Organizational Structure as a function of a potentially unified Directory Service.
* Establish, document, and implement written policies and procedures for Security Event Management, up to and including a customized SIEM (Security Incident and Event Management) system if or where applicable.
* Evaluate current help desk functions and formulate strategy for maximum scope and effect. This may include hybrid approaches to some IT related services or convergence of other processes.
* Review of current Line of Business applications and formulate strategy for monetization / digital transformation.

**Deliverables**

* **Security and Compliance Dashboards**
* **Security Incident, Investigation, Remediation Dashboard**
* **Compliance Manager (a System of Record for all compliance related documentation)**
* **Completed 800-171 Assessment (may use 800-53 if applicable)**
* **Completed assessment will be cross refenced with other applicable standards such as, but not limited to, US Banking PII, CISA, NIST RMF, SEC OCIE, SEC Title 17, and others that may be identified accordingly**
* **All required Written Policies (and procedures where required), to include end user / acting agent / Corporate Officer acknowledgements accordingly – cross referenced to the standards for which they are applicable**
* **Curated list of Recommended Actions (continually updated – “your to do list”)**
* **Mechanisms and workflows to drive “programs” (we apply as much automation as we can)**
* **Risk Register with Residual Risk Rating**
* **Unofficially I will do about “310 things” (there is a big spreadsheet with detailed explanations of everything delivered prior to project completion)**

*NOTE: Some sections, including Client and Contractor Responsibilities Removed for this Abridged SOW.*

# Fee Schedule

This engagement will be a fixed cost based on an average assumption of man hours and discounted base rate. Some services may be performed by subcontractors of NIST Assist, or other Microsoft Agents associated with the Microsoft Partner Network, including Microsoft employees and representatives of Microsoft, AWS, or IBM. Time and Materials Rate is $175.00 per hour, discount provided for fixed price. NIST Assist will provide additional hours over and above the base 288 hours at a rate of $110.00 (requires approval by both parties). This figure is based on 288 hours of professional services. Contractor will provide up to 3 resources based on the following functional/rate structure.

| Item Description | Number of Resources (NTE) | Hourly Rate | Number of Hours |
| --- | --- | --- | --- |
|  |  |  |  |
| Professional Service / Managed Services | 3 | 110.00 | 288 |

Upon completion of this Performance Period, Contractor and Client will have the option to renew this agreement for an additional then-stated number of hours at the then-current hourly rate for those resources identified.

|  |
| --- |
| Total Fixed Price:  **$31,680.00** |

# Out-of-Pocket Expenses / Invoice Procedures

Client will be invoice for the first month up front, and each month accordingly. Payment is due on receipt (5 day terms for Credit Card payment).

Client will be invoiced all costs associated with out-of-pocket expenses (including, without limitation, costs and expenses associated with meals, lodging, local transportation and any other applicable business expenses) listed on the invoice as a separate line item. Reimbursement for out-of-pocket expenses in connection with performance of this SOW, when authorized and up to the limits set forth in this SOW, shall be in accordance with Client’s then-current published policies governing travel and associated business expenses, which information shall be provided by the Client Project Manager. The limit of reimbursable expenses pursuant to this SOW is estimated to be 15% of the fees unless otherwise authorized in writing and agreed to by both parties via the project change control procedure outlined within.

Payments for services invoiced that are not received within 30-days from date of invoice will be subject to a 5% penalty per calendar month.

# Completion Criteria

Contractor shall have fulfilled its obligations when any one of the following first occurs:

* Contractor accomplishes the Contractor activities described within this SOW, including delivery to Client of the materials listed in the Section entitled “Deliverable Materials,” and Client accepts such activities and materials without unreasonable objections. Deliverables consist of, but are not limited to, systems and software, configurations and settings, and policies and procedures in electronic form, part of a User Interface, workflow, or service account.
* “Definition of done” will often be referenced in your program and constitutes the length to which the contractor can go to provide the deliverable. Some of the deliverables can only work if the designated roles and responsibilities are followed accordingly. This is an important distinction because from a purely technical point of view, nothing we are doing can be defined as “done”. This is because the overall objective of the program(s) is to document evidence of ongoing effort to identify, prepare, and cope with a cybersecurity incident or ANY disruption to business through continuous review and improvement.
* Contractor and/or Client has the right to cancel services or deliverables not yet provided with 30 business days advance written notice to the other party.

# Project Change Control Procedure

The following process will be followed if a change to this SOW is required:

* A Project Change Request (PCR) will be the vehicle for communicating change. The PCR must describe the change, the rationale for the change, and the effect the change will have on the project.
* The designated Project Manager of the requesting party (Contractor or Client) will review the proposed change and determine whether to submit the request to the other party.
* Both Project Managers will review the proposed change and approve it for further investigation or reject it. Contractor and Client will mutually agree upon any charges for such investigation, if any. If the investigation is authorized, the Client Project Managers will sign the PCR, which will constitute approval for the investigation charges. Contractor will invoice Client for any such charges. The investigation will determine the effect that the implementation of the PCR will have on SOW price, schedule and other terms and conditions of the Agreement.
* Upon completion of the investigation, both parties will review the impact of the proposed change and, if mutually agreed, a Change Authorization will be executed.
* A written Change Authorization and/or PCR must be signed by both parties to authorize implementation of the investigated changes.

**IN WITNESS WHEREOF,** the parties hereto have caused this SOW to be effective as of the day, month and year first written above.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Client Name |  |  | Company Name |
| By: |  |  | By: |  |
| Name: |  |  | Name: |  |
| Title: |  |  | Title: |  |

**Exhibit A**

NEXT STEPS

A brief overview of some of the activities that are not obvious in a raw SOW but does give insight to how this will unfold and what to expect.

* The BOD or equivalent will release a Charter on day 1 that details how your company will embrace a new standard approach designed to protect the employees and stakeholders. This is a demarcation of the fact that you have reached an official point in your maturity whereby recent events and future landscape requires more comprehensive action (a determination you will account to your risk management program).
* An assessment will begin immediately and will require due diligence around third party access and control, including the assigned Partner of Record that allows us to get insights and adoption attributes. Similarly, you will setup internal accounts with the necessary roles assigned so we can perform our work and install resources from Microsoft and other Security and Compliance providers.
* At the end of the first week, we begin to prioritize the do outs from the initial assessment.
* In subsequent week, Directives will be established, or some equivalent vehicle will establish official lines of communication that are designated as the source of truth in the organization, to include specific branding for easy identification. This enables Records Management and written policy acknowledgement.
* A number of programs will be fired up simultaneously, and we will track adoption attributes to identify programs that need attention, are doing poorly, may not be needed or can be converged with others.
* Roles and responsibilities will be identified and assigned, are where applicable there can be only 1 Owner.
* Designated individuals will have to accept responsibility for things and may not like it.
* Most of what we are doing has elements of Change Management, so we incorporate some technology to increase what we refer to as adoption rate.
* Executives in the organization will have to endure a couple of seminars. This is important because when accreditation is required, or an audit occurs, C level is interviewed by the auditors, and must pass a basic evaluation of their “readiness”. We have a cheat sheet for you as a takeaway on what they will ask and what you should say.
* There will be somewhere around 40 policy templates that can break out into as many as 110, and we have to acknowledge them all. If you do not have automation for this, we will set that up. We will incorporate as many of your existing polices as we can.
* In all practicality, we generally execute about 10 percent over and above the scope of man hours we propose. I estimate our actual clock time will be on the order of 300 hours. This is an artifact of logging in a few minutes before an activity, and due diligence post activity, which leaves a trail in the Audit Log of all our activity. In this way, when there is an audit, forensics will, among other things, clearly delineate cause and effect of activity without “noise” from regularly scheduled maintenance or work product. This also serves to make customers feel better by going above and beyond.