ATTACHMENT A

STATEMENT OF WORK

The Contractor shall provide a cloud-based Enterprise Risk Management Software-as-a-Service (the "Solution") to the New York State Office of the State Comptroller ("OSC"). The Solution must: (1) automate the collection of risk assessment data and streamline the reporting of risks to executive management; and (2) integrate with the Committee of Sponsoring Organizations of the Treadway Commission ("COSO") Internal Control – Integrated Framework (the "COSO Framework").

I. PROJECT REQUIREMENTS

A. General Contractor Requirements

The Contractor shall:

1. develop and deliver a project plan that includes roles, milestones, key dates, and regular status updates,

2. analyze and define OSC's business requirements and business rules and perform a gap analysis comparing OSC requirements with existing Solution functionality.

3. customize or configure the Solution to meet OSC's business requirements and business rules, ensuring that the Solution meets all mandatory requirements as detailed in Section III (Solution Requirements),

4. convert and migrate five years of historical data from OSC's current system into the Solution and perform migration testing to verify the successful migration,

5. conduct and facilitate testing of the Solution, and refine configuration or customization as needed based on the results of that testing,

6. provide training to OSC staff on the use of the Solution, and

7. deploy the Solution to production.

NOTE: OSC prefers that Solution implementation be completed within nine months of commencement of the Agreement, and requires an amendment to extend the Agreement if the implementation is not completed on or before the end of the first year of the Agreement.

B. Staffing

1. The Contractor shall assign one or more staff members to the following key roles:

a. **Project Manager:** The Project Manager shall serve as the Contractor's principal contact and will have day-to-day responsibility for the project and successful implementation of the Solution. Duties include communication, planning, scheduling, coordination, and resolution of issues as they arise. The Project Manager will report to OSC's Internal Control Officer ("ICO").

b. **Analyst:** The Analyst shall gather OSC requirements for the Solution, complete a gap analysis comparing OSC requirements with the Solution, create conversion and migration specifications, and draft and update all necessary documentation needed for the project.

c. **Trainer:** The Trainer shall train OSC staff on how to use the Solution.

The assigned staff members shall perform all implementation services remotely unless otherwise directed by OSC to perform them in person at 110 State Street, Albany, New York.

2. The Project Manager shall coordinate with OSC's ICO to ensure adequate project resourcing and effective communications, and coordinate OSC's review and acceptance of the deliverables.

3. An OSC staff member with functional knowledge of the current system and business processes will be available to assist with the project and answer questions regarding the current state and needs for the Solution.

C. Customer Service

The Contractor shall provide customer service and technical support to OSC Monday through Friday, except for New York State holidays. OSC prefers customer service and technical support to be available at least from 8:00 a.m. to 5:00 p.m. ET.

D. Training

1. The Contractor shall train OSC administrators on how to use the Solution.

2. OSC prefers the Contractor provide on demand training, which may include live instruction or prerecorded videos. The Contractor should provide training documentation, including step-by-step instructions on how to use the Solution.

3. OSC prefers the Trainer to be available to respond to questions within one business day of receiving a question.

II. DELIVERABLES

The Contractor will submit deliverables to OSC for review. OSC will provide the Contractor with written confirmation of its acceptance or notice of any deficiencies. OSC may provide such confirmation or notice via email. If a deliverable is not accepted by OSC, the Contractor shall address identified deficiencies and resubmit the deliverable within ten business days.

A. **Project Plan:** The Contractor shall supply a project plan within two weeks of Contract approval. The project plan must include a project schedule with the timeline, list of tasks and activities, roles, and applicable milestones necessary to implement the Solution. The Contractor shall keep the project schedule up to date throughout the implementation of the Solution.

B. **Gap Analysis:** The Contractor shall analyze and define OSC's business requirements and business rules and complete and deliver to OSC a gap analysis comparing OSC requirements with existing Solution functionality.

C. **Configured or Customized Solution:** The Contractor shall deliver to OSC a configured or customized Solution that meets all the mandatory functional requirements stated in Section III (Solution Requirements).

D. **Data Conversion and Migration:** The Contractor shall convert and migrate approximately 125 MB of historical data that is currently stored in Microsoft Excel and Access into its Solution. OSC staff will be available to test data conversion and migration prior to the Go-live Date.

E. **User Acceptance Testing:** OSC staff will perform User Acceptance Testing ("UAT") of the Solution in a test environment provided by the Contractor. The Contractor must update the UAT environment to the most current version prior to OSC initiating UAT. Approximately three OSC staff members must be trained in the use and navigation of the Solution so they can competently perform UAT. OSC staff will test the Solution to ensure it meets all the mandatory functional requirements in real-world scenarios and encompasses the full range of business processes included in the scope of this project. As such, files will be received and sent using the integration processes agreed to as part of the project. OSC staff will be available to test Solution functionality prior to the Go-live Date.

F. **Resolution of all Critical and Major Defects:** The Contractor shall perform all required effort to ensure all Solution functionality required to execute OSC's business processes works as required.

G. **<u>Training</u>:** The Contractor shall provide approximately four selected OSC staff members with up to 15 hours of training sufficient to use the Solution with respect to OSC's business rules and requirements.

H. **<u>Fully Functional and Implemented Solution</u>:** The Contractor shall provide a fully functional and implemented Solution in a production environment.

III. SOLUTION REQUIREMENTS

The Solution must meet the mandatory functionality requirements listed in this Section III (Solution Requirements). While not required, OSC has also identified preferred Solution functionality listed below (identified with a "Preferred" heading).

A. User License Types

The Solution must allow OSC to assign users at various levels of capabilities and/or license types, including the ability to set the following permissions (the Solution may use other names for these roles but must have these distinct roles):

1. Business User – can edit/update/certify for their organizational units. Business User's access must be restricted to only their organizational unit's risk data.
2. Viewer – has read-only access to all data for their organizational units or for other levels (as assigned by an Administrator).
3. Administrator – can edit/view all organizational units, add/remove users, change access rights and roles, review audit trails/data changes, set up new organizational units, and perform other tasks necessary to administer the Solution.

B. Risk Register

The Solution must provide a risk register that can manage each organizational unit's risks.

1. The risk register must allow Administrators and Business Users to:
   - **a.** describe the risk;
   - **b.** identify risk ratings (scores or risk levels) such as high, medium, low;
   - **c.** relate the OSC functions affected by the risk;
   - **d.** identify risks as being unmitigated (deficient, significant, major, etc.);
   - **e.** assign controls to risks;
   - **f.** allow creation of an action plan for unmitigated risks including steps required to be completed;
   - **g.** allow status updates to the corrective actions, including date completed; and
   - **h.** identify when a risk is no longer unmitigated and/or applicable.
2. The risk register must allow Administrators to:
   - **a.** administer risks;
   - **b.** relate risks to OSC's strategic priorities;
   - **c.** rate risks in multiple categories (e.g., IT, privacy, operational); and
   - **d.** allow for the ability to edit/update any information including creating, updating, and deleting risks.
3. The Solution must restrict Business Users' access to only their organizational unit's risk data.
4. <u>Preferred</u> - OSC prefers a Solution that can store and relate risk to OSC's organizational structure, a/k/a "org chart."

C. Risk Assessment

The Solution must:

1. Allow OSC users to:
    a. perform risk assessments using risk questionnaires distributed through the Solution to various organizational units;
    b. test organizational unit functions; and
    c. certify results;
2. Allow users to configure risk questionnaires, including the ability for users to:
    a. use boilerplate questions and announcements;
    b. develop customized questions specific to the organizational unit;
    c. restrict the format of answers (e.g., dates, dropdowns, lookup fields); and
    d. display questions based on branching logic;

(For OSC's current questionnaire format, refer to Attachment D – Sample Questionnaire)

3. Provide risk assessment functionality that allows Business Users to:
    a. designate which functions are required to be tested;
    b. identify new key controls;
    c. identify new risks;
    d. document all testing performed and the results with respect to the user's key controls;
    e. identify exceptions in their internal control testing and designate them as "major" or "minor" (e.g., significant, not significant);
    f. identify corrective action plans related to exceptions identified in their internal control testing (i.e., steps to address the exception and expected date the step will be completed); and
    g. certify the results of their risk assessment;
4. Allow Administrators to include a certification statement that Business Users can electronically sign/acknowledge upon completion of the Business Users' risk assessment. The certification statement must be able to be edited as needed by OSC. The Solution must be able to identify the user certifying and the date certified;
5. Allow Administrators to track business functionality by organizational unit. The Solution must:
    i. allow administrators to rate the business functions using OSC-identified criteria;
    ii. provide a calculated rating (such as high, medium, or low) based on the administrators' rating of the business functions;
    iii. allow administrators to override the calculation; and
    iv. allow business users to view/edit their list of functions and ratings;

    Preferred - OSC prefers the Solution allows Administrators to confirm edits made by Business Users to their list of functions and ratings.
6. Allow Administrators to notify OSC organizational units of their required risk assessments;
7. Allow Administrators to send automated reminders to business users to complete unfinished work;
8. Allow Administrators to respond to risk assessments submitted by organizational units;

9. Allow Business Users and Administrators to provide an update on corrective actions that have not been marked as completed;

10. Allow Administrators to schedule risk assessment workflows;

11. Allow Administrators to configure risk assessment workflows; and

12. Allow Administrators to determine the certification year of the testing exceptions identified by Business Users.

Preferred - OSC prefers the Solution allows Business Users to report real time and post hoc high-risk incidents.

D. Reporting

1. The Solution must include functionality that will allow OSC users to:

a. Create reports on the risk categories assigned to the risks, by organizational unit and strategic priority;

b. Produce reports identifying OSC's top risks and risk exposure based on the information provided by Business Users (e.g. heatmaps, aggregated reports, risk portfolios);

c. Share reports (e.g., by PDF export, secure link) with stakeholders outside the Solution (i.e., individuals without a user license), such as management or external auditors;

d. Identify and report on functions not tested that are required to be tested by the organizational unit;

e. Determine how long corrective actions have been outstanding; and

f. Create reports that show the organizational unit's risks, risk profiles, and outstanding corrective actions to the unit's respective head.

2. Preferred - OSC prefers the Solution:

a. Have the ability to generate internal control scorecards by organizational unit and a compilation scorecard for all organizational units (e.g., "out of the box" reports that could include how many unmitigated risks, and/or the controls efficiency);

b. Include ad-hoc reporting functionality to facilitate data analysis;

c. Include dashboard functionality so important information can be shared with stakeholders with some customization per viewer (e.g., "out of the box" dashboards that show risks of the organizational unit and/or the ability for the user to add/remove metrics);

d. Recognizes exceptions reported by Business Users across the organization that can be interrelated and use data analytics or other reporting features to create a combined risk score that differs from the sum of the individual risks at the business unit level;

e. Include advanced analytics so OSC is able to stay up to date on risks and be well informed of future issues, such determining risks that are not yet critical but could be in the near future (e.g., predictive analysis, risk analysis, quantitative impact); and

f. Include reports with relevant graphical options (e.g., bar charts, heat maps, line chart, histograms).

E. Incident Submission

1. Preferred - OSC prefers the Solution provides functionality that allow Business Users:

a. To submit risk incidents and details, including date of incident and corrective actions taken or planned to be taken; and

b. Link risk incidents to related business functions.

F. COSO Framework

The Solution must have the ability to:

1. Integrate the most recent COSO Framework within the risk assessment;
2. Demonstrate OSC's compliance with the most recent COSO Framework. (The Contractor must update the Solution to reflect any changes to the COSO Framework as adopted by, and within the implementation date specified by, COSO.); and
3. Identify those components of the COSO Framework that OSC has failed to comply, if any.

Preferred - OSC prefers the Solution has the ability to apply the COSO Framework to each organizational unit's system of internal control and identify noncompliance by organizational unit.

G. Security and Access

The Contractor shall maintain physical and electronic security sufficient to ensure that neither the Contractor nor any third party (other than cloud service providers designated by OSC) can view, read, store, or act on any OSC data.

1. The Contractor shall:

   a. Employ an external vendor to conduct annual penetration testing on the implemented Solution and promptly remediate any findings. The Contractor shall provide OSC with third-party certification of this penetration testing upon OCS's request;

   b. Ensure that all network-based information and application development, or programming, including, but not limited to, websites delivered to OSC as part of the Solution comply with State Technology Law § 103-d and Executive Law § 170-f, as each may be amended from time to time, and be consistent with New York State Enterprise IT Policy NYS-P08-005, Accessibility of Information Communication Technology, as such policy may be amended, modified or superseded (the "Accessibility Policy"). The Solution and related technology must be accessible to all users, including those with disabilities as determined by accessibility compliance testing. The Contractor must provide proof of compliance if requested by OSC.

   c. In the event of a Security Incident (as defined in Section XII.G of the Agreement), provide authorized OSC users with access to the Solution's authentication logs containing data from the previous 90 days, at a minimum;

   d. Comply with all applicable data privacy and data protection laws and regulations;

   e. Demonstrate that its systems comply with an industry- or government-accepted security framework (e.g., NIST, FedRamp, ISO 27000 series). The Contractor must provide evidence of its compliance via third-party assessment (e.g., SOC2 type 2) or certification, or provide other documentation satisfactory to OSC;

   f. Ensure that all systems and individuals that access or interact with OSC data be physically located within the contiguous United States, including the District of Columbia ("CONUS"), and that all OSC data accessed, stored, or processed by the Solution remain in the CONUS; and

   g. Ensure the Solution's non-production environments that hold or contain personal information include security and access controls equivalent to those provided in the production environment.

2. The Solution must:

   a. Encrypt communications using Hypertext Transfer Protocol Secured ("HTTPS") or an equivalent protocol;

   b. Require multi-factor authentication ("MFA") for all remote access to the Solution;

c. Use OSC's Active Directory Federated Services ("ADFS") and Security Assertion Markup Language ("SAML") to provide a single sign on;

d. Limit OSC user access to information according to user roles, permissions, and business rules; and

e. Provide an OSC employee interface for OSC functions that can be restricted to access from only the OSC IP address range, and only via authenticated access.

H. Integration

1. The Solution must:

a. Have the ability to export data to flat files in MS Excel format; and

b. Allow OSC to fully extract its data into MS Excel and/or MS SQL Database.

2. Preferred - OSC prefers the Solution be able to:

a. Export formatted information into Microsoft Excel or other Microsoft products; and

b. Integrate data stored in the Solution with third-party systems, such as Tableau.

I. Performance and Availability

The Solution must be:

a. Able to support a minimum of four Administrators, 125 Business Users, and 30 Viewers; and

b. Available 99.9% of the time outside of scheduled maintenance. Scheduled maintenance must occur outside of business hours.

J. Usability

The Solution must:

a. Have a graphical user interface that allows users to easily navigate components; and

b. Allow OSC to fully audit any data changes made by users within the Solution.

Preferred – OSC prefers the Solution be able to identify the changes and the user that performed the change.

IV. Post-Implementation

A. **As Needed**. The Contractor shall provide post-implementation services, subject to OSC approval, on an as-needed basis throughout the term of the Agreement. These post-implementation services may include supplementary training, change requests to alter customizations or configurations, analytics development, post-implementation assistance, and other consulting services. OSC anticipates up to 200 hours of post-implementation services will be needed during the term of the Agreement.

B. **Solution Support and Maintenance**. The Contractor shall provide certain post-implementation services at no additional cost to OSC. These include any Solution updates and versions, enhancements, improvements, corrections, service packs, or other modifications of or to the Solution that are released by the Contractor for general distribution to licensees, and such other support services as the Contractor provides as part of its Solution support and maintenance program. Any customization made to the Solution to meet OSC's requirements must become a supported configuration of the Solution and be maintained in future releases of the Solution at no additional cost to OSC.

C. **Location of Post-Implementation Services**. The Contractor shall perform all post-implementation as needed services remotely unless otherwise directed by OSC to perform them in person at 110 State Street, Albany, New York.