

Statement of Work
Enterprise Risk Management and
Business Impact Analysis Services
2019



CONTENTS

Introduction / Background	3
Scope	3
Deliverables & Roles/Responsibilities	3
Phase I - Enterprise Risk Management Service	3
Business Impact Analysis	3
Reports and Meetings	4
Period of Performance / Schedule	4
Invoices and Payment / Acceptance Criteria	4
ERS/Vendor-Furnished Equipment	4
Assumptions/Requirements	4
Respondent's Proposal	5
Overview of the Scope	5
Enterprise Risk Management (ERM) Services	5
Key Activities	6
Business Impact Analysis	9
Staff capabilities	13
Service capabilities	15
Pricing	16
Change Requests	16
Schedule of Events and Response Milestones	17
Guidelines	17
Q/A	17
Point of Contact	17
Response submission requirement - Submission Format	17
Confidentiality	17
Signatures / Acceptance	19

INTRODUCTION / BACKGROUND

The Employees Retirement System of Texas (ERS) is a constitutional trust fund established as mandated by Article XVI, Section 67, Texas Constitution, and further organized pursuant to Subtitle B, Title 8, Texas Government Code, as well as 34 Texas Administrative Code, Sections 61.1, et seq. ERS administers a retirement and disability pension plan for state employees, law enforcement and custodial officers, elected state officials and two classes of judges (in this context, hereinafter referred to as Members). ERS invests state and Member contributions in the retirement trust funds and administers the trust funds with a fiduciary obligation to the members and retirees of ERS who are its beneficiaries. ERS also administers the Texas Employees Group Benefits Program, which consists of health benefits, life insurance and other optional benefits, to participating individuals eligible to receive those benefits under applicable law.

SCOPE

ERS seeks the services of an experienced vendor (herein each respondent to this SOW is referred to as "Respondent" and the selected vendor is referred to as the "Vendor") to assess and update the Enterprise Risk Management (ERM) profile of the agency and to conduct a Business Impact Analysis (BIA) for the business processes of ERS.

ERS conducted an ERM study in 2013, with the goal of understanding critical and strategic risks faced by ERS, and ways to better manage risk. Several entity-level risk categories (operational, information technology, economic, etc.) were analyzed to determine the risk profile of the organization based upon the level of impact and likelihood of risk events. This analysis was used to inform organizational decisions on key programs, operations, and functions.

ERS requests the Vendor conduct a risk assessment to determine the risk profile for ERS. This study should build upon previous assessments to re-evaluate levels of risk associated with key programs, operations, and functions. This study will consider the probability of adverse events caused by either natural processes, like severe storms, fires, or floods, or adverse events caused by malicious or inadvertent human activities. The study will identify and document areas of greatest risk based upon level of impact and likelihood. Finally, the Vendor will document recommended risk management activities and recommend best practices for risk avoidance or best practices to minimize risk.

ERS uses a BIA from a previous study, and most of the critical business processes in that study have been modified, abandoned, or changed in recent years. Using the ERM research, the Vendor should update the BIA and identify business processes and prioritize their importance for continuity of operations and disaster recovery plan development.

DELIVERABLES & ROLES/RESPONSIBILITIES

Phase I - Enterprise Risk Management Service

The core functions and deliverables for the ERM service are:

- Build upon previous assessments to re-evaluate levels of risk associated with key programs, operations, and functions through interviews with ERS management and program/technical staff
- Support the development of risk management activities and documentation and recommend best practices for adherence
- Identify and document areas of greatest risk based upon level of impact and likelihood

Business Impact Analysis

The core functions and deliverables for the BIA service are:

Phase II - Update existing BIA based upon current ERM research:

- Serve as primary lead for completion of all BIA deliverables and tasks
- Develop a BIA process and tool for use with identified departments in accordance with the critical functions of ERS business
- Gather business requirements from stakeholders and translate them into the proper format to convey messaging across technical and business domains
- Conduct BIA interviews with senior leadership across the agency to update process profiles, impact assessments, and identify dependencies

- Conduct variance analysis to identify any possible gaps between business needs and functional or process recovery capabilities
- Document BIA results, training materials, and policies

Phase III: Develop recovery scenarios based on business requirements

- Develop enhanced BIA focus/deliverables on financial impact and risk management on business functions and IT services/applications
- Document and present recovery scenarios and cost implications of each to executive management

REPORTS AND MEETINGS

1. ERS and the Vendor will schedule and conduct meetings with appropriate business staff.
2. ERS will provide Vendor with full access to the relevant functional, technical, and business resources with adequate skills and knowledge.
3. ERS will assign a Project Manager, who is the contact for this service.
4. The Vendor may tour the ERS facilities at 200 E. 18th, Austin, Texas.
5. The Vendor will have staff available to answer questions regarding billing and invoices.
6. The Vendor will participate in meetings after each draft report is developed in order to determine the gaps which may remain in the final report.

PERIOD OF PERFORMANCE / SCHEDULE

The term of service for this Statement of Work is for up to one (1) year, effective upon execution of both parties.

INVOICES AND PAYMENT / ACCEPTANCE CRITERIA

ERS will pay an invoice for the services when the reports are submitted and accepted by ERS. The acceptance of reports is made by the ERS.

ERS/VENDOR-FURNISHED EQUIPMENT

The Vendor must bring all equipment, hardware and software, for the completion of the SOW.

ASSUMPTIONS/REQUIREMENTS

ERS assumes that the Respondent can provide all services described in this SOW. Any changes to the SOW are reflected in the Respondent's Proposal.

1. ERS must review and approve Vendor's standard Certificate of Insurance (COI). ERS should allow up to 10 business days if ERS requires endorsements to be added to the COI.
2. The Vendor agrees to sign a Non-Disclosure Agreement for the term of this engagement (the form of which is attached as Appendix A).
3. ERS will provide workspace and internet access for up to two (2) persons during the development of the SOW.
4. The Respondent may not access ERS member information.
5. The Respondent will provide a copy of their latest SOC II, Type II report.
6. If the selected DIR Prime vendor decides to subcontract any part of the contract in a manner that is not consistent with DIR's HUB subcontracting plan (Appendix B of the DIR Cooperative Contract), the selected DIR Prime vendor must comply and submit a revised HUB subcontracting plan to DIR before subcontracting any of the work under the SOW. No work may be performed by a subcontractor before DIR has approved a revised HSP for the Cooperative Contract.

RESPONDENT'S PROPOSAL

Overview of the Scope

At a high level, this engagement will consist of three key phases, as illustrated in the following diagram:



Additional details regarding our methodology and approach are provided below.

Enterprise Risk Management (ERM) Services

Weaver utilizes a top-down approach to enterprise risk management, focusing on the strategic, entity and process levels. Weaver identifies your most relevant internal and external risks, and considers risk types affecting major systems and controls. We focus on important risk factors such as asset protection, loss prevention, fraud occurrence and compliance with policies and procedures that may restrict the entity's ability to achieve strategic objectives and execute procedures in an efficient and effective manner.

Risk assessment is an evolving, ongoing process - not simply a template wherein attributes are entered into a static spreadsheet. As such, we customize our risk assessments to meet specific objectives at every level, as illustrated below:



Our procedures are developed to comply with the Committee of Sponsoring Organizations (COSO) Enterprise Risk Management Framework (ERM), as well as aspects of the International Organization for Standardization (ISO) 31000 Risk Management Framework.

COSO ERM is quite similar to ISO 31000, with several notable exceptions. First, COSO ERM does not specifically prescribe consideration of external elements of risk and the opportunity side of risk; therefore, we incorporate these considerations into our risk assessment process to ensure a more complete and well-rounded approach. For example, in order to maximize the benefits of strategic risk management, an organization should consider both the opportunistic and adverse sides of risk. Additionally, an organization should consider external and internal risks facing the company in establishing the risk universe.

Key Activities

Building upon previous assessments, Weaver will assist ERS with identifying and documenting relevant risks and assessing the strategic and business significance of those risks with regard to the achievement of your strategic objectives at both the enterprise and process levels. Our approach typically includes the following activities:

- Establish agreed-upon strategic business objectives
- Identify and assemble the team in risk assessment meetings, with management's participation
- Conduct brainstorming sessions with management to gain an understanding of the existing risk environment and organizational risk appetite
- Develop and administer risk identification questionnaires
- Conduct risk assessment team meetings within ERS to identify risks and develop the risk universe
- Evaluate responses and investigate outliers
- Hold forum meetings to develop consensus
- Develop risk profile and prepare risk maps
- Work with management to develop a risk response plan

Through our independent and disciplined approach, Weaver can provide a documented risk tolerance statement, a prioritized risk category and event register, a risk-rated activity and process universe, risk maps, a strategic initial risk response plan, and recommendations that can be used as a basis for full ERM and risk monitoring.

Performing the Risk Assessment

Step One: Risk Identification

Weaver will facilitate a brainstorming session with the risk assessment team to enhance our current understanding of the risk categories and events at ERS. This working session will be interactive: the team, with assistance from Weaver, will discuss and confirm the high-level risk categories and events, as well as the specific risk influencers. The group will also discuss your strategic goals and how they may be impacted or influenced by the identified risk profile.

Additionally, we will conduct one-on-one interviews with senior leadership to ensure that the identified risks are encompassing of the views of those charged with strategic direction for ERS. Upon completion of the risk identification process, we will have a complete inventory of risk categories and individual events that are specific and relevant for ERS. These risks will serve as the basis for the entity-wide risk assessment.

Step Two: Entity-level Risk Assessment

The purpose of the entity-level assessment is to identify risks from external and internal influences that impact the organization. Results are compared to internal processes in order to determine whether such risks should be mitigated through controls, accepted or eliminated. In this manner, the entity-level risks are linked to the process level risks.

The risk categories and influencers identified in the risk profile and tolerance phase will be used to develop a questionnaire that will be distributed to a select group of individuals across ERS. Participants will complete the questionnaire to provide feedback regarding the most significant risks facing the company.

Once the risk assessment results are obtained, responses are evaluated through both a quantitative and qualitative analysis:

- **Quantitative Analysis.** Results are tabulated for each respondent and summarized by department. A detailed analysis of risk responses is conducted and a composite is calculated. Aberrations (which we call outliers) are identified for further analysis.
- **Qualitative Analysis.** Comments are read to gain a better understanding of management's perspective. Outliers that were previously identified are investigated via interviews with respondents to determine:
 - Are the responses accurate? Occasionally, respondents don't understand a question. In this case, Weaver may update the questionnaire to reflect the accurate answer after discussing it with the respondent. Changed responses are identified by color-coding.
 - Do the responses identify legitimate issues that must be addressed? In some instances, the answers uncover significant issues that require attention.

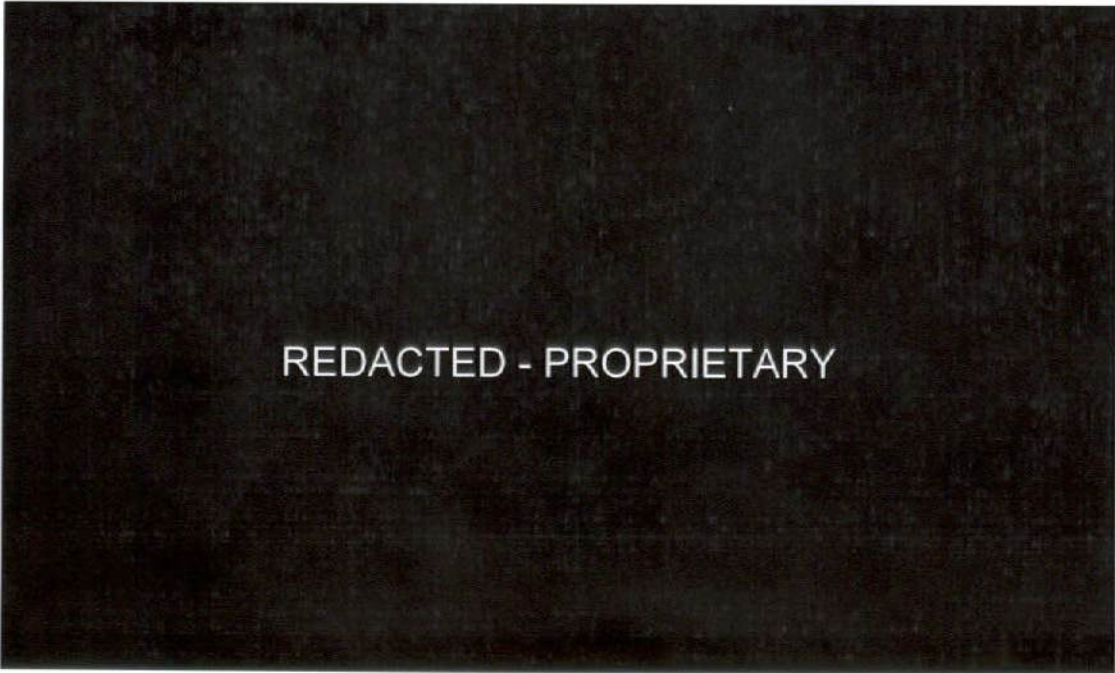
When the responses have been evaluated and ratings finalized, each identified critical risk factor will be defined using ERS-specific risk influencers and reported in order of assessed significance to develop a complete risk profile. Additionally, we will link risks to strategic objectives in accordance with the fundamental tenets of enterprise risk management.



REDACTED - PROPRIETARY

Step Three: Process-level Risk Assessment

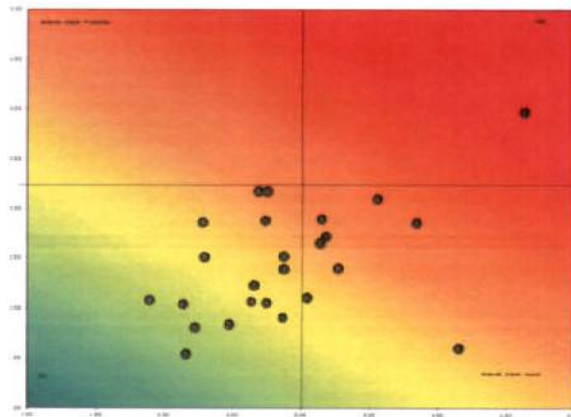
Our process-level risk assessment is prepared to risk rate the significant processes for the relevant risks. At this stage, we will obtain existing policies and procedures and other related documentation in order to develop a universe of significant activities throughout the entity. An example of a process-level risk assessment audit universe is shown below:



REDACTED - PROPRIETARY

We will review the risk universe with the risk assessment team to ensure complete coverage of all financially and operationally significant activities. We will also conduct forum meetings with select individuals from across ERS to risk-rank all identified activities and build consensus as to the inherent risk probability and impact of all critical risk factors to each significant activity.

We will then develop risk maps to provide graphical illustration of the concentration of risk, based on probability and impact.



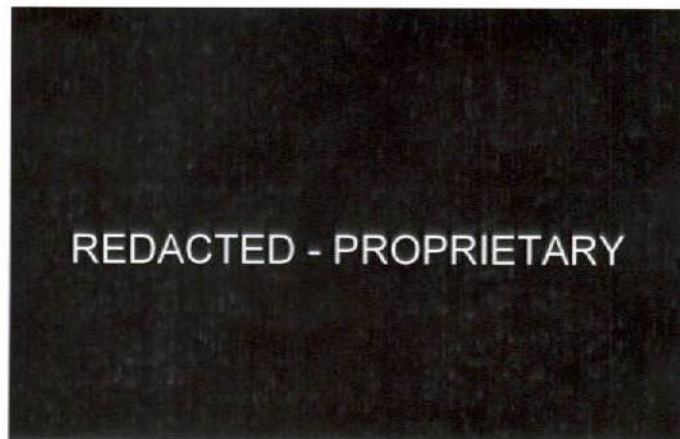
Sample Risk Map

Step Four: Update/Develop Risk Profile

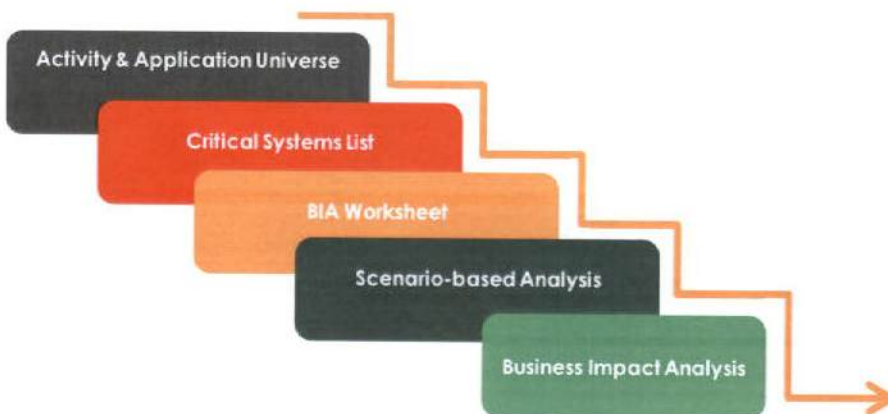
Upon completion of the Enterprise Risk Assessment, ERS will have documented and adequate information to update/develop a new risk profile statement, which depicts the sum of risk awareness and risk tolerance. This risk profile statement, in conjunction with the other deliverables resulting from the assessment, will inform our team's updates to the Business Impact Analysis in phase 2.

Business Impact Analysis

Using the information gained during the risk assessment, Weaver will work with ERS to update the existing BIA and develop recovery profiles with associated cost implications using our proven methodology.



A Business Impact Analysis (BIA) is designed to predict the consequences following the disruption of the systems supporting a business function or process so that management can develop efficient and effective recovery strategies. The BIA consists of an Application Universe, a Critical Systems List, a Scenario Analysis and a BIA Worksheet. Together, these tools assess the potential impact of a disaster, as well as help determine recovery times and objectives. Weaver has a multi-tiered and interactive approach to ensure that the BIA is customized and relevant to the organization. Details regarding this approach are provided below.



Activity and Application Universe

The first phase of the project will be to identify all critical functions and activities at each department and the associated systems and applications. Through a combination of questionnaires and interviews, we will identify the operational and financial impacts resulting from the disruption of business functions and processes. We will also identify the critical business processes and resources needed for the business to continue to function at different levels. This is done using a four-step process:

Develop

- Develop a critical activity and application survey tailored to ERS' operating environment to target the specific systems utilized by each business unit and ensure that all critical applications are identified.

Distribute

- Distribute survey to a broad cross-section of employees, including entry-level and managerial personnel
- Leverage existing electronic survey tools and methods
- Monitor response rate

Analyze

- Compile responses
- Analyze responses
- Aggregate results
- Investigate response outliers

Critical Systems List

- Prepare and present the Critical Activity & Application Universe to Management
- Discuss Universe with Management to ensure completeness

Critical Systems List

After analyzing and aggregating the survey results, we will complete the critical systems list, which:

- Addresses operational, administrative, and financial systems, including investment, group benefits and retirement programs
- Identifies primary transactions and average frequency and volume of each
- Identifies network and computing resources for each location, and where they reside
- Aligns resource needs with the disaster recovery plan and determines business resumption requirements

When we are reasonably confident that the listing of systems is complete and contains all systems critical to ERS, we will consolidate all the systems into a matrix to independently aggregate and analyze the systems.

BIA Worksheet

The BIA worksheet aggregates each system by department and outlines evaluation factors that are prioritized by management. The evaluation factors will include quantitative and qualitative factors, as well as recovery objectives.

- Qualitative and Quantitative Factors
 - Financial metrics of impact over a specified timeframe
 - Revenues
 - Expenses
 - Penalties and Fines
 - Operational metrics of impact over a specified timeframe
 - Public Image
 - Customer Service
 - Competitive Advantage
 - Legal/Regulatory
 - Safety
- Recovery Objectives
 - Recovery Time Objectives (RTO): Assesses criticality of the speed of returning the system to full functioning status.
 - *Example: An operational system that interfaces in real time will have a higher RTO ranking than a financial system used on a monthly basis.*
 - Recovery Point Objectives (RPO): Assesses the totality of the data preservation required for this system.
 - *Example: A system that requires 100% totality of data preservation whereas a maintenance system that utilizes paper documentation for all work orders in the past week does not require 100% totality of data preservation.*

REDACTED - PROPRIETARY

Scenario-Based Analysis

Once the BIA worksheet is complete, we will assess each department based on specific disaster scenarios.

- Each system identified as utilized by the business unit will be evaluated to estimate the impact to business operations for each scenario.
- Each assessment will have selected assumptions unique to each disaster scenario.
- Analysis will primarily be based on quantitative measures such as transaction volume, revenue generation, regulatory cost, etc.
- Analysis results will be used for the facilitated department meetings

Based on the analysis of each scenario, we will prepare recommendations for business resumption priorities to integrate into the Disaster Recovery Plan.

Business Impact Analysis

The completion of the BIA is executed through facilitated department sessions to obtain feedback on the criticality of the systems based on the quantitative and qualitative factors.

Participants will be selected from throughout the organization that have a specific knowledge of the systems and provide a cross section of experienced employees that can provide information from all levels and aspects of operations.

Each department-level BIA will be analyzed and evaluated to identify system criticality across all of ERS. We will identify the critical linkages between business processes that must be operationally guaranteed as a basis for the Disaster Recovery Plan and prepare recommendations for business resumption priorities for the three components of business operations: personnel, location, and information technology.

KEY BUSINESS DISRUPTION SCENARIOS

- Restricted access or physical damage to a site or building
- Damage to or breakdown of machinery, systems or equipment
- Utility outage (e.g., electrical power outage)
- Damage to, loss or corruption of information technology systems
- Terrorism
- Fire
- Natural Disaster
- Absenteeism of essential employees

KEY IMPACTS CONSIDERED

- Unfavorable investment returns
- Inability to execute investment decisions timely
- Increased expenses
- Regulatory fines
- Impaired delivery of employee benefits
- Contractual penalties
- Customer dissatisfaction
- Delay of business or strategic goals

STAFF CAPABILITIES

Weaver has extensive experience with ERS' operations and enterprise risk management (ERM) processes. In 2013, we assisted with the implementation of ERS' ERM program by performing an entity-level risk assessment to identify and assess significant risk events that impacted the agency and performing a process-level risk assessment to determine how those entity risks impacted agency operations.

The key leadership team for this engagement was selected for their hands-on experience with ERS, as well as their overall ERM and BIA skills and experience. Summary biographies for the team are provided below; detailed resumes are available upon request.



John Wauson, CPA | Partner, Risk Advisory Services

Experience with ERS: John was on the team that performed the enterprise risk assessment for ERS in 2013. As such, he is deeply familiar with the ERM program, as well as agency operations, culture and risk profiles.

John has a dozen years of public accounting and risk advisory experience. Specifically, he is experienced in identifying and assessing risk at the entity- and process- levels and developing a response plan to manage and mitigate identified risks. John assists clients with designing and implementing risk mitigation activities for a wide-range of strategic, operational, financial and compliance activities.

John is experienced in conducting strategic risk assessments at the entity and process level, performing process and internal control design evaluations, and developing risk management procedures for a variety of public sector entities, including

REDACTED



Brett Nabors, CISA | Partner, IT Advisory Services

Brett has more than 12 years of experience in advisory services, including formerly directing PwC's risk assurance practice in Austin. His career focuses on business process improvement, integrated compliance, internal control assessments, IT governance, ERP implementation, enterprise risk management and system and organization controls (SOC) reporting.

Brett is highly skilled in business process improvement, data analytics, IT control evaluations and other aspects of managing and improving IT performance, effectiveness and security. He regularly assists clients with improving controls and processes, identifying and addressing risks and aligning IT processes to overall organizational strategy. He is experienced with both the public sector and healthcare, including clients

REDACTED



Adam Jones | Senior Advisor

Experience with ERS: As a former state agency fiduciary and former member of the DIR board of directors, Adam has a fundamental understanding of both the mission and purpose of ERS and the financial and IT requirements imposed upon it by state oversight agencies and the Texas Legislature.

Adam has two decades of experience in Texas state government, including nine years serving as Deputy Commissioner and Chief Operating Officer of the Texas Education Agency. He brings broad experience as the responsible administrator for every major operational area of the TEA during his tenure there, including accounting, budget, procurement, the administration of the Foundation School Program, grants administration, HR, organizational development, and the agency's information technology environment. He chaired the agency's Fraud, Risk Assessment and Compliance Committee, the oversight body for the internal audit function. Having served on the DIR Board, Adam has deep operational and cultural insight with regard to alignment of risk profiles and recovery strategies with business needs and strategic goals. He serves as an invaluable resource for identifying organizational risks and working with management to facilitate meaningful, sustainable organizational change.

Over the past several years, Adam has served as a management, IT and organizational assessment consultant for a variety of public and private sector clients, including

REDACTED

He brings vast experience in organizational management, and is a frequent, sought-after speaker on managerial topics, as well as an experienced and effective group facilitator and trainer.



Marci Sundbeck, CIA, CISA, CCSA, CFE, CRMA | Senior Advisor

Experience with ERS: Having served as both the Director of Enterprise Risk Management and the Director of Internal Audit, Marci has a unique perspective and insight with regard to governance and the ERM program at ERS.

Marci has more than 25 years of audit and advisory experience in state government, including extensive experience developing and managing governance and enterprise risk management programs and processes in a state agency environment. In her work with Weaver, Marci's clients have included

REDACTED

A Certified Internal Auditor (CIA), Certified Information Systems Auditor (CISA) and Certified Fraud Examiner (CFE), Marci also holds a Certification in Risk Management Assurance (CRMA) and Certification in Control Self-Assessment (CCSA).



Morgan Page, CIA | Senior Manager

Morgan has ten years of public accounting and industry experience in executing business process improvement engagements, working with organizations to define and monitor critical risk attributes, and operating as a subject matter expert on multiple application implementation teams to ensure organizational risks are identified and addressed. He has experience planning and executing many different types of engagements including internal audits; reporting and tool development engagements; business impact analyses; disaster recovery/business continuity planning evaluations and engagements; and regulatory compliance. Morgan is a member of the Institute of Internal Auditors (IIA) and he graduated with a Bachelor of Science in business administration and a Master of Science in accounting from the University of Texas at Dallas).

SERVICE CAPABILITIES

Weaver's Advisory Services practice is made up of approximately 80 dedicated professionals recognized for their breadth and depth of experience in a full range of governance, risk management and compliance services.

Our **Risk Advisory Services** professionals are recognized for experience in all phases of risk management, from internal control evaluations over individual processes to complete enterprise risk management. They bring many years of experience performing risk assessments and implementing/enhancing enterprise risk management programs for a wide variety of Texas-based public and private sector clients. Core competencies and specialized skills of the auditors in our Risk Advisory Services group include:



Our **IT Advisory Services** professionals have extensive experience providing IT and business process-focused assessments and audits for a wide variety of organizations, including public entities and Fortune 500 companies alike. Our team is also well-versed in the standards and control frameworks used by leading organizations to manage compliance with a variety of technical regulations, including frameworks such as COBIT 5, NIST 800-53, NIST-CSF, TAC 202, Systems and Organization Controls (SOC) 1, 2 and 3, SOC for Cybersecurity, ISO 27001/27002, FFIEC, FISMA and ITIL. Core competencies and skillsets of the auditors in this group include:



PRICING

The pricing listed below includes all the SOW costs – add lines, if necessary, for costs which should be considered, but are not listed in the table. Finally, these are the fixed-fee, total, and complete costs to deliver the services described in the SOW.

Description	Cost
Phase I Enterprise Risk Management Service	
<ul style="list-style-type: none"> Build upon previous assessments to re-evaluate levels of risk associated with key programs, operations, and functions through interviews with ERS management and program/technical staff Support the development of risk management activities and documentation and recommend best practices for adherence Identify and document areas of greatest risk based upon level of impact and likelihood 	
Total – Phase I Enterprise Risk Management Service	\$53,000
Phase II - Business Impact Analysis - Update existing BIA based upon current ERM research:	
<ul style="list-style-type: none"> Serve as primary lead for completion of all BIA deliverables and tasks Develop a BIA process and tool for use with identified departments in accordance with the critical functions of ERS business Gather business requirements from stakeholders and translate them into the proper format to convey messaging across technical and business domains Conduct BIA interviews with senior leadership across the agency to update process profiles, impact assessments, and identify dependencies Conduct variance analysis to identify any possible gaps between business needs and functional or process recovery capabilities Document BIA results, training materials, and policies 	
Total – Phase II Business Impact Analysis	\$36,000
Phase III - Business Impact Analysis - Develop recovery scenarios based on business requirements	
<ul style="list-style-type: none"> Develop enhanced BIA focus/deliverables on financial impact and risk management on business functions and IT services/applications Document and present recovery scenarios and cost implications of each to executive management 	
Total – Phase III Business Impact Analysis	\$18,000
Total Project Cost, all phases	\$107,000
Other costs (add lines if necessary)	
	n/a
	n/a
Total – Other Costs	n/a

CHANGE REQUESTS

ERS and Vendor affirm they are fully committed to successful delivery of services. All scope changes must be reviewed by both ERS and Vendor.

1. ERS and the Vendor will discuss the change request and mutually agree on the scope of the change.
2. ERS and the Vendor's Representative will document the change.
3. The Vendor will determine the impact to the test schedule and cost impact, if any.
4. ERS and Vendor make an addendum to the ongoing service delivery documentation and other required service artifacts.
5. The Vendor and ERS will sign the change request which contains the information listed in steps 1-4 above.
6. Change Orders will be submitted to DIR for their review and approval.

7. ERS will execute the Purchase Order Change Notice (POCN) to the purchase order.
8. The duly authorized ERS representative who may approve change orders and pricing increases is the Director of Enterprise Planning.

SCHEDULE OF EVENTS AND RESPONSE MILESTONES

Item	Delivery Date
SOW Release	November 5, 2018
Respondent Q&A session (conf. call)	November 14, 2018 – 9:00 AM CST
Respondent written question deadline	November 16, 2018
Respondent Q&A/written question responses	November 21, 2018
Respondents SOW response deadlines	December 5, 2018 – 10:00 AM CST
Vendor Selection	January 9, 2019
Service Start	After execution / mutually agreed-upon date
Service Ends	After execution / mutually agreed-upon date

GUIDELINES

Q/A

ERS will schedule a conference call for Respondent Q&A; in addition, ERS will also respond to written questions submitted by the date in the Schedule of Events and Response Milestones table. ERS will also discuss the services, ask questions and receive clarification from finalists during the conference call.

POINT OF CONTACT

The contact for this SOW will be the IS Administration section; they can be contacted at isadministration@ers.texas.gov.

RESPONSE SUBMISSION REQUIREMENT - SUBMISSION FORMAT

Respondent should use the SOW form for responses. These should be returned as a final submission in PDF format.

CONFIDENTIALITY

Respondent should note which portions of the SOW are to be considered confidential by submitting a separate document which specifies everything that Respondent deems to be confidential and/or proprietary.

ERS is required to provide access to certain records in accordance with the provisions of the Public Information Act (PIA). Respondent is required to make any information pursuant to the SOW, and not otherwise excepted from disclosure under the PIA, available in a format that is accessible by the public at no additional charge to ERS.

During the evaluation process, ERS shall make reasonable efforts as allowed by law to maintain proposals in confidence and shall release proposals only to personnel involved with the evaluation of the proposals and implementation of the Contract unless otherwise required by law. However, ERS cannot prevent the disclosure of public documents and may be required by law to release documents that Respondent considers to be confidential and proprietary.

Labeling of Confidential and Proprietary Information. In order to protect and prevent inadvertent disclosure of confidential information submitted in support of its proposal, Respondent shall supply, in good faith and with legally sufficient justification, a separate schedule of all pages considered by Respondent to contain any confidential and/or proprietary information. Respondent shall also mark each page/section of its proposal as confidential/proprietary each time it submits information to ERS, whether in its initial proposal or in any supplemental information submitted to ERS. By submitting a proposal, Respondent acknowledges and agrees that all information submitted by Respondent in response to this SOW that is not clearly marked as

"Confidential" information is public information and may be fully disclosed by ERS without liability and without prior notice to or consent of Respondent or any of its subcontractors or agents.

Respondent further understands and agrees that, upon ERS' receipt of a PIA request for Respondent's information, ERS will provide the requestor the information which is not confidential and/or proprietary. If Respondent fails to submit its confidential and/or proprietary information as described herein, ERS shall consider all of the information to be public, and it will be released without notification to the Respondent upon receipt of a PIA request.

To the extent the public version of Respondent's proposal contains "Protected Materials", Respondent acknowledges that such Protected Materials may be disclosed, publically displayed, published, reproduced and/or distributed by ERS pursuant to the PIA, or as otherwise required by law. Respondent warrants and represents that it owns, or has obtained all necessary permissions with respect to the use of, the Protected Materials and hereby grants ERS an irrevocable, perpetual, non-exclusive, royalty-free license to display, publish, reproduce, distribute or otherwise use the Protected Materials solely for the purpose of compliance with applicable laws. Respondent shall indemnify and hold harmless ERS, its trustees, officers, directors, employees, and contractors, as well as any trust managed by ERS, from and against any claim of infringement of the Protected Materials resulting from ERS' use of the Protected Materials as set forth herein.

Upon receipt of a PIA request, ERS will submit the information which the Respondent considers confidential and/or proprietary to the Texas Attorney General to issue a ruling on whether the information is excepted from public disclosure.

It is Respondent's sole obligation to advocate in good faith and with legally sufficient justification the confidential or proprietary nature of any information it provides to ERS. Respondent acknowledges and agrees that ERS shall have no obligation or duty to advocate the confidentiality of Respondent's material to the Texas Attorney General, to a court, or to any other person or entity. Respondent acknowledges and understands that the Texas Attorney General may nonetheless determine that all or part of the claimed confidential or proprietary information shall be publicly disclosed.

In addition, Respondent specifically agrees that ERS may release Respondent's information, including alleged confidential or proprietary information, upon request from individual Members, agencies or committees of the Texas Legislature where needed for legislative purposes, for their own information, as provided for in the PIA, or to any other person or entity as otherwise required by law.

MANDATORY TERMS

Notwithstanding anything to the contrary in this SOW or any subsequent agreement between ERS and Respondent (collectively the "Agreement"), the parties hereby agree as follows: (a) the obligations of the parties shall be subject to the Texas Public Information Act (Tex. Gov't Code ch. 552) and state of Texas record retention laws and regulations, and Respondent is required to make any information pursuant to this Agreement, and not otherwise excepted from disclosure under the PIA, available in a format that is accessible by the public at no additional charge to ERS; (b) ERS hereby reserves and does not waive its sovereign immunity; (c) ERS does not agree to indemnify Respondent for any liability or costs incurred by Respondent for any reason; (d) the laws of the state of Texas shall apply without regard to the principles of conflicts of laws; (e) without waiving its sovereign immunity, any disputes will be heard exclusively in a Texas state court in Travis County, Texas; (f) ERS does not agree to engage in arbitration and does not waive its right to jury trial; (g) ERS is tax-exempt, and any fees to be paid under this Agreement: (i) do not include any taxes and (ii) have not been increased because of ERS' tax-exempt status; (h) Respondent represents and warrants that there are no facts or circumstances that could give rise to a conflict of interest or the appearance thereof; (i) Respondent may not assign this Agreement, including by merger or similar transactions, without the prior written consent of ERS; (j) Respondent is eligible

to enter into this Agreement and receive payments under Tex. Gov't Code §§ 403.055, 2155.004, and 2155.006 and Tex. Fam. Code § 231.006; (k) Respondent agrees to comply with all applicable laws and regulations of the state of Texas relating to contracting with state agencies; and (l) this paragraph shall survive the termination or expiration of the Agreement. ERS and Respondent agree that this paragraph shall control to the extent of any conflict with any other portion of the Agreement.

SIGNATURES / ACCEPTANCE

Accepted by:

Weaver and Tidwell, L.L.P.

Signature:



Print Name: John Wauson

Title: Partner

Date: 11/30/18

DIR Contract #: DIR-TSO-3877

Accepted by:

Employees Retirement System of Texas

Signature:



Print Name: Porter Wilson

Title: Executive Director

Date: 02/01/2019

DIR SOW ID# ERS-000015

DocuSigned by:



Hershel Becker

Chief Procurement Officer

Texas Department of Information Resources

Date: 2/5/2019 | 3:40 PM CST