Statement of Work
Identity Access Management Service

Information Security
June, 2019

Deloitte Consulting LLP response to
Employees Retirement System (ERS) of Texas
Identity Access Management Service (IAM)
Statement of Work (SOW)
Revision Date: 01-29-2020

DIR Contract # DIR-TSO-4031 ("DBITS")

Table of Contents

1. Introduction

The Employees Retirement System of Texas is a trust fund established by the Texas Constitution and is described in Article XVI, Section 67, Texas Constitution. ERS is also organized pursuant to Subtitle B, Title 8, Texas Government Code, as well as Title 34 of the Texas Administrative Code, Sections 61.1, *et seq*. ERS invests and administers trust funds as a fiduciary for the exclusive benefit of the members and annuitants of the system. 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. Participants are those persons eligible to participate in these programs per the Texas Employees Group Benefits Act as set forth in Chapter 1551 of the Texas Insurance Code.

This deliverables-based service is to assess the security requirements, including authentication, authorization, and auditing for ERS applications and deliver improved and unified security platforms which are easily maintained by agency personnel. The successful Respondent(s) shall assess, develop, or configure, test, stage, and release application security modules using Agile methodology on a frequent release cycle. This project will be done in phases and ERS intends to award to either one (or multiple) vendors for this entire project. The initial award will be for Phase I only and subsequent phases will be awarded to the same vendor or multiple vendors through a change order and corresponding amendment to this Statement of Work (SOW).

Deloitte's Response

Deloitte Consulting LLP ("Deloitte") is pleased to submit this proposal ("Response") to the Employee Retirement System of Texas (the "State" or "ERS"), in response to its SOW for IAM Assessment (the "SOW") under the State of Texas Deliverables-Based Information Technology Services contract with DIR Contract No. DIR-TSO-4031("DBITS").

2. Background

ERS currently maintains application islands associated including Cisco, Oracle, Active Directory, Clarity, PeopleSoft, Linux/Unix, AIX, RSA, and SFTP. The agency would be well-served with a role-based, unified security model for all applications which has fewer points of failure and a more iterative and documented process for applying security rules.

3. Scope

The goal of this SOW is to develop and implement a unified data security model (UDSM) for ERS based on the Information Technology Infrastructure Library (ITIL) methodology. The scope may include, but is not limited to, the following activities:

- Analysis of the current security methodology. This should include, but not be limited to, a detailed analysis of Active Directory user groups.
- Analysis of application discovery to determine if additional applications benefit from the new model.
- Identify project risks, actions, issues and decisions using a risk register or RAID project register.
- Design future state to enable (where appropriate):
    - Single sign on
    - Role based authentication
    - Same sign on
    - Multi-Factor authentication

- Develop and document auditable controls and procedures including:
    - Roles and responsibilities for IS Operations, IS Security Office, business units, and authorized agency security teams
    - Criteria for determining appropriate role-based security constraints
    - Workflow for security requests
    - Workflow for security exception requests
    - Quality control assessments

- Recommend deliverables and plans for future sprints.
    - Future sprints to implement activities recommended in the project design phase of the SOW will be determined as change orders or amendments to this SOW. See Appendix C Software List.

The successful Respondent will work in a team-based Agile environment. The successful Respondent will create and maintain system roadmaps, project plans, and security service releases that will be the basis for the successful Respondent's work. The ERS project manager will specify high-level requirements to the Agile team. As in typical scrum-based Agile processes, ERS project manager will work together with the team to develop and estimate user stories and establish acceptance criteria. These acceptance criteria will specify expected functionality for a user story, as well as any non-functional requirements that must be met in the development of the storyline. The ERS project manager, supported by SMEs and business analysts, will determine whether acceptance criteria have been satisfied.

4. Project Management and Deliverables

4.1 Project Design Phase Deliverables

- The successful Respondent shall deliver project plans for the future project sprints from work done during this project design phase. This should include the following high-level deliverables:
    - Analysis of the current application security methodologies including identification of points of failure.
    - Analysis of application discovery to determine if additional applications benefit from the new model.
    - Provide governance methodology for determination and recommendations for in-scope/out-of-scope applications and UDSM.
    - Recommend policy and governance documentation.
    - Develop design for SSO, Multi-Factor, and other future state authentication models
    - Define sprints for future implementation.
    - Estimate costs for each sprint.
    - Review licensing and cost implications for new UDSM.
- For each future sprint the successful Respondent should determine:
    - Buy/Build recommendation.
    - System clean-up and redesign (AD, Linux, etc.) to fit into new UDSM.
    - Process/Procedure documentation and training.
    - Retirement schedule of systems and processes replaced by new design.
- The product of each sprint must be in accordance with TAC, Title 1, Part 10, Chapter 202, Sub Chapter B, Information Security Standards for State Agencies and comply with, but is not limited to, the following security requirements:
    - U.S. Department of Commerce National Institute of Standards and Technology (NIST) 800-53 R, and
    - Texas Department of Information Resources (DIR) Texas Cyber Security Framework requirements for asset management, access control, continuous security monitoring, data security, detection processes, information protection, protective technologies, and training.

- The product of each sprint must conform to State Accessibility requirements for Electronic and Information Resources specified in 1 TAC Chapters 206 and 213 and the Web Content Accessibility Guidelines (WCAG) 2.0 (as applicable).

4.2 Project Design Phase Deliverables Estimated Due Dates

Deloitte's Response

The estimated due dates for deliverable submission are as provided in the table below. These dates assume a project start date of 9/30/2019 2/12/2020. At the start of the project, Deloitte will work with ERS to put together a detailed project plan. The project plan will help track the key activities, dependencies and milestones including the submission of deliverables listed below.

Deliverable	Deliverable Description	Estimated Due Date
1	Analysis of the current security methodology	3/06/2020
2	Analysis of application discovery to determine if additional applications benefit from the new model	4/03/2020
3	Determine in-scope/out-of-scope applications and security models	4/03/2020
4	Develop design for SSO (single or same sign on), two-factor and other future state authentication models	4/03/2020
5	Develop sprints for future implementation	4/17/2020
6	Estimate costs for sprints, including current licensing review and cost implications for new models	4/17/2020
7	Develop project plans (if not covered by sprint activity)	4/17/2020
8	Policy and governance development	4/17/2020
9	Develop or configure, test, stage, and release new security models on a frequent release cycle using Agile project management methodology for each future sprint	4/17/2020

5. Project Management

5.1 Reports and Meetings

Meetings and deliverables:

- A kickoff meeting will be held at a location and time selected by ERS where the successful Respondent and its staff will be introduced to ERS project team.
- Deliverables must be provided on the dates specified by the ERS project manager. Any changes to the delivery date must have prior approval (in writing) by the ERS project manager and the ERS contract manager or designee.
- All deliverables must be submitted in a manner approved by the ERS project manager.
- If any deliverable cannot be provided within the scheduled timeframe, the successful Respondent is required to contact the ERS project manager in writing with a reason for

the delay and the proposed revised schedule. The request for a revised schedule must include the impact on related tasks and the overall project.

- A request for a revised schedule must be reviewed and approved by both the ERS contract manager and the ERS project manager before placed in effect. Contract Terms and Conditions may dictate remedies, costs, and other actions based on the facts related to the request for a revised schedule.
- ERS will complete a review of each submitted deliverable within ten (10) specified working days from the date of receipt (this may change depending on the complexity of the effort and the deliverable).

Progress Reports:

- The progress reports shall cover all work performed and completed during the week for which the progress report is provided and shall present the work to be performed during the subsequent week. The reports will be required to be delivered at a time negotiated with the ERS project manager and the successful Respondent.

- The progress report shall identify any problems encountered or still outstanding with an explanation of the cause, resolution of the problem, and when the problem will be resolved.

- The successful Respondent will be responsible for conducting weekly scrum status meetings with the ERS project manager. The meetings will be held at a time and place designated by the ERS project manager. The meetings can be in person or over the phone at the discretion of the ERS project manager.

6. Service Level Agreements

The successful Respondent will complete, at least, the deliverables associated with the project as specified in sections 4.1 and 4.2. The ability to work on the subsequent sprints in the SOW is dependent on the following:

- Ability to meet budget goals within 5% of original sprint estimate (+/- 5%).
- Ability to meet budget goals within 5% of project design phase (+/- 5%).
- Deliverables must be finalized within three rewrites and approved by the ERS project manager.
- Ability to meet sprint or design phase delivery goals by original due dates (within two weeks).
- Systems are implemented as designed and available for production work at previously agreed delivery date.
- There is no loss of data or lack of security when moving from the current-state security model to a future-state security model.

7. Invoices

- ERS will pay an invoice for the services at the end of each phase when the work is accepted by ERS. The acceptance of a phase is made by the ERS Chief Information Officer or his designee. Invoices will not be processed and will be considered incomplete unless ERS has accepted the work for each phase.
- The successful Respondent must have an accounting point of contact available to ERS to answer any questions during the invoice reconciliation process.
- Provided ERS can reconcile the invoice to supporting detail within five (5) working days, ERS issues payment in accordance with the Texas Private Prompt Payment Act and in accordance with Appendix A of the DIR contract. ERS does not accelerate payments in advance of due dates.

- Any disputes regarding payment will be resolved in accordance with Contract terms and TGC Ch. 2251, pertaining to dispute of invoices.
- The successful Respondent must submit invoices to ERS by mail: P.O. Box 13207, Austin, Texas 78711-3207, or by email: ap@ers.texas.gov.

8. Additional ERS Terms and Conditions

- ERS will provide a work area for successful Respondent use during on-site activities that include Internet and public phone access.
- ERS will provide virtual machines and Wyse connectivity to the virtual machines. These will include Microsoft Windows and Microsoft Office as standard software for the engagement. All other software must be provided by the successful Respondent and must undergo a software security and license review by ERS.
- ERS will provide parking passes and adequate parking for the successful Respondent project team.
- Standard hours of operation are 8 a.m. to 5 p.m. Central Time, Monday through Friday. It is understood that due to the nature of the industry and work performed, after-hours and weekend availability is often required. In the event successful Respondent resources are required to perform work outside of the standard hours of operation, agreed-upon work windows will be discussed and subsequently documented via email. It is also required that the ERS project manager or a technical contact be on-site during the agreed-upon weekend/after-hours work window(s).
- ERS will participate in all design and planning sessions.
- ERS delays in providing successful Respondent with the necessary information to accomplish each task may result in timeline changes.
- Before project work begins, ERS must review and approve successful Respondent's standard Certificate of Insurance (COI). ERS should allow up to 10 business days if ERS requires endorsements to be added to the COI.
- Subject to the terms and conditions of the underlying DIR Contract, the successful Respondent agrees that all work done under this SOW is a Work for Hire. The successful Respondent retains no rights to inventions, copyrights, or any other intellectual property developed solely for ERS during the course of this engagement. The successful Respondent retains rights to prior work used to develop ERS materials but grants ERS a royalty-free perpetual license to the work products required or resulting from all sprints contained within this SOW.
- The successful Respondent has no rights to ERS data and may not keep or use ERS data or reports in future engagements.
- All ERS data and work products must be erased from successful Respondent equipment at the end of the engagement and verified by the ERS Information Security Office
- The successful Respondent agrees to sign a Non-Disclosure Agreement -- the software lists and security platform information contained in Appendix C are confidential; therefore, Respondent must execute a Non-Disclosure Agreement to obtain the information in these appendices prior to returning the SOW. The Non-Disclosure Agreement is located at Appendix B, and Respondent shall email its properly executed Non-Disclosure Agreement to ERS at isadministration@ers.texas.gov.
- Upon receipt by ERS of Respondent's executed Non-Disclosure Agreement ERS will provide access to Appendix C Software List.
- The successful Respondent is required to provide copies of completed FBI criminal background checks of all assigned staff prior to the start of the project.
- The successful Respondent agrees to sign an ERS HIPAA Business Associate Agreement upon request by ERS.
- 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 (HSP) (Appendix B of the DIR Cooperative Contract), the selected DIR Prime Vendor must comply and

submit a revised HUB subcontracting plan to DIR prior to 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 and notifies the ERS contract manager.

9. Vendor Response

The following information shall be provided in the successful Respondent's response in the sections below:

9.1 Staff Capabilities

Respondent shall list staff capabilities specific to this SOW -- include key personnel resumes illustrating the qualifications of each to perform the services described in this SOW. List the percentage of the time that the Respondent staff member will be assigned full-time to the project.

Deloitte's Response

The cornerstone of our client service approach is our commitment to providing the desired experience and team to our clients. Deloitte has a large pool of IAM professionals, complemented [redacted] Our professionals bring a wealth of experience of providing cyber security services to commercial and government organizations, including services provided to various local, state, and federal agencies. Our deep understanding of IAM industry standards and leading practices enables us to assess current state and provide strategy for further enhancements.

[redacted]

With careful thought, Deloitte has put together an experienced team that possess the capabilities and skills required to plan and deliver the IAM assessment for ERS, as described below.

9.1.1 Our Team

[redacted] Our team draws on relevant domain knowledge and experience to hit the ground running and provide value to the State from the start of the engagement.

[redacted]

9.1.2 Staff Resumes

Key Personnel

As illustrated in the bios below, our key staff was chosen for their experience, along with their ability to provide the broad range of skills required to meet your requirements described in the RFP. The key staff has previously worked together on IAM implementation projects. This further reduces the project risk since the team leads have developed an effective and collaborative working style that helps keep the project on-track. A professional summary for the representative team members for this engagement is as follows:

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

9.2 Service Capabilities

Respondent shall provide evidence of its services capabilities, including but not limited to:

- Description of three (3) projects of similar size and scope that Respondent has conducted within the past five (5) years;
- Description of experience providing similar deliverables in public sector, specifically state and local government; and
- Detailed outline of its capability to deliver the required services, including process, functional and technical expertise.

Deloitte's Response

[redacted]

In this section below, we have included four select project references with similar size and scope as ERS IAM assessment.

9.2.1 Selected Project Experiences

Project Experience 1

[redacted]

[redacted]

Project Experience 2

[redacted]

[redacted]

Project Experience 3

Client	A Large Federal Civilian Agency
Project Name	Profess ona Support Serv ces for Ident ty, Credent a , and Access Management (ICAM)
Project Descr pt on	De o tte was engaged by the c ent to he p n estab sh ng, assess ng, and evo v ng ts ICAM program from one based on d sparate commod ty too s nto a comprehens ve y funct ona ICAM program w th mproved operat ona eff c ency and ower operat ng costs. As such, the c ent requested that De o tte perform n depth assessments of the peop e, processes, and techno og es support ng the ICAM program w th the goa of deve op ng an enterpr se ICAM strategy and roadmap to remed ate ssues found n the assessments. The cu m nat on of th s task ed to an ongo ng mu t year remed at on and opt m zat on efforts across c ent's ICAM program, dur ng wh ch De o tte worked c ose y w th the c ent's IAM Serv ces Area Manager and Execut ve Leadersh p to execute the ICAM strategy and roadmap. De o tte cont nues to prov de IAM Serv ces w th a ways on secure Operat ons and Ma ntenance (O&M, Eng neer ng Serv ce and broad Program Management Off ce) support. [redacted]

[redacted]

Project Experience 4

[redacted]

[redacted]

9.2.2 Our Cyber Risk and IAM Experience

Our Cyber Risk Services practice helps complex organizations more confidently pursue their strategic growth, innovation and performance objectives through proactive management of the associated cyber risks. With deep experience across a broad range of industries, our Cyber Risk Services practitioners provide advisory and implementation services to help transform legacy IT security programs into proactive programs that better align security investments with business risk priorities, establish improved threat awareness, and strengthen the ability to thrive in the face of cyber incidents.

Our Demonstrated IAM Experience

Deloitte brings over 20 years of IAM experience, a demonstrated approach, and knowledge of IAM technology to the ERS project. Deloitte has collaborated with several states, federal agencies and commercial organizations to implement and operate IAM solutions. The following figure illustrates our recent experiences in implementing and operating IAM solutions for state government agencies.

[redacted]

Our Deep Public Sector Experience

Deloitte has deep experience working with multiple state, local and federal agencies across the US. We understand the business processes, IT systems, and security requirements from compliance drivers. We have a deep understanding and effective track record of providing similar services to various states. In addition, Deloitte is not only a leader in cyber risk consulting services in the public sector but also actively involved in leading the conversation and shaping the future from a security perspective. For example, the Deloitte-NASCIO Cybersecurity Study, published biennially, highlights the challenges states face in the cybersecurity arena.

Deloitte is also an active participant as a member and contributor on the council and multiple subcommittees in the National Governors Association's (NGA) Policy Council for State Cybersecurity, established to inform and assist governors in securing their organizations against cyber threats. Deloitte will bring security insights to ERS that not only meet today's requirements, but also prepare it to face the challenges of tomorrow. The following figure illustrates our public-sector experience delivering cyber risk projects.

[redacted]

Our State of Texas Experience

The State of Texas ("State") has been, and continues to be, a very important client to Deloitte for the last four decades. Over the past several years, Deloitte has collaborated with the State to drive many transformational technology engagements including IAM system design and implementation projects for various State of Texas agencies. Deloitte understands the State's working environment and supports it across a wide spectrum of advisory services. As a strategic partner, the State's ability to achieve its goals is a significant measure of our accomplishments and continues to strengthen the relationship between Deloitte and the State.

[redacted]

Figure 4. Deloitte's demonstrated experience of working collaboratively with State of Texas for over 40 years

Our IAM Capability

Deloitte has one of the largest IAM practices in the world, and we have been recognized by leading IT research firms as one of the leaders in IAM based on our thought leadership, client service, and vendor relationships. Deloitte brings a dedicated practice with deep experience and knowledge gained from 20 years of delivering strategy, architecture, design, and implementation of enterprise IAM for clients in both the public and private sectors. [redacted], including for Fortune 500 companies, government agencies, and higher education institutions.

[redacted]

Figure 6: Our IAM Capability

By working with major vendors on our implementation projects we have developed a deep understanding of how these products work. We have also observed how these products perform once they are deployed and operating under real world conditions. This allows us to define solution architectures upfront that will withstand the test of real-world performance loads and decrease the chance of having to rework an IAM environment after it has been deployed to meet performance expectations. When we develop ERS's IAM architecture we will reference past architectures that we have developed. Deloitte's solution architectures are not based on how products theoretically will perform, but instead are based on our observations of how products perform in real world environments.

[redacted]

[redacted]

Analyst Recognition

We are the only organization with the breadth, depth, and insight to help complex organizations become Secure, Vigilant, and Resilient. Our Cyber Risk Services practice is consistently ranked a leader amongst its peers by industry analysts such as Gartner, Forrester and ALM Intelligence. Selected analyst recognition is provided in the following figure.

We are ranked #1 globally in:

- CRM & Customer Experience Services by Gartner (2018)
- HR Operations Consulting by ALM Intelligence (2018)
- Innovation Strategy Consulting by ALM Intelligence (2018)
- Business Consulting Services by IDC (2017)
- Business Transformation Consulting by Forrester (2017)
- Analytics IT Consulting by ALM Intelligence (2017)
- Risk Consulting by IDC (2017)
- Crisis Advisory in Financial Services by ALM Intelligence (2017)
- IT Operations Consulting by ALM Intelligence (2017)
- Customer Strategy & Experience Consulting by ALM Intelligence (2017)

In terms of capabilities, we were named a global leader in:

- Data Analytics Services by Gartner (2018)
- Customer Service Consulting by ALM Intelligence (2018)
- Workforce Management Consulting by ALM Intelligence (2018)
- Health & Wellness Consulting by ALM Intelligence (2018)
- Retirement Benefits Consulting by ALM Intelligence (2018)
- Communications & Change Management Consulting by ALM Intelligence (2018)
- Compensation Consulting by ALM Intelligence (2018)
- Strategic Risk Consulting by ALM Intelligence (2018)
- Product Development Operations Consulting by ALM Intelligence (2018)
- Finance Operations Consulting by ALM Intelligence (2018)
- Cloud Professional Services by IDC (2018)
- Public Cloud Infrastructure Managed Services by Gartner (2018)
- SAP Application Services by Gartner (2018)
- Oracle Application Services by Gartner (2018)
- Information Security Consulting Services by Forrester (2017)
- Digital Experience Services by Forrester (2017)
- Application Management & Digital Operations Services by Forrester (2017)

Figure 5. Deloitte's recent analyst recognition and accolades

Strategic Vendor Relationships

As highlighted in the above section, one of the distinguishing factors of our IAM practice is our strategic alliances with industry-leading IAM product vendors. Our alliances and relationships provide our practitioners rare access to vendor product engineering teams and gives us the ability to escalate issues. We are a product agnostic systems integrator who brings leading options to meet client needs. We have strong relationships and alliances with leading product vendors, service providers and the ecosystem, as illustrated by the accompanying figure. These strategic alliances and partnerships allow us to better serve ERS through advances in capabilities and joint solution development.

[redacted]

IAM Tools and Accelerators

Deloitte has developed an extensive set of accelerators for IAM assessment and implementation that incorporate best practices and learnings from working with various clients. Our accelerators have been successfully applied in various industry sectors where the enterprise is managing multiple and emerging risk and compliance programs.

Method or Tool Name	Method or Tool Description

[redacted]

9.3 Project Work Plan

The successful Respondent shall provide a draft high-level project work plan addressing the tasks specified in the SOW, which shall include:

- A description of key activities and milestones.
- A description of the successful Respondent's approach to analyze, assess, validate, document and complete each sprint/iteration.
- A description of the resources necessary from ERS to support the project, including estimates of time needed from ERS' subject matter experts and high-level analysis of data gathering requirements.
- Any assumptions, risks, constraints, and dependencies of the project.

Deloitte's Response

9.3.1 Execution Approach

Our work plan approach expands on our demonstrated experience in delivering IAM projects effectively at several public sector agencies. Our understanding of the changing cyber risk landscape of the public sector industry, emerging trends in IAM, and deep experience in implementing cutting edge IAM solutions allows us to achieve ERS objectives. As illustrated in the service capability section, we bring our demonstrated IAM Toolkit that containing tools and accelerators to expedite analysis, deployment of IAM solution and integration of applications.

We understand that ERS is looking to create an IAM strategy and roadmap, to establish an effective IAM platform. To achieve the end goals of the project, it is important that we proceed in a logical, sequential manner, with a business benefit focus, while driving toward the overall IAM program objectives. Our approach will align the areas with the business benefit helping the program get good

momentum from inception. We use our industry knowledge and your priorities to tailor our assessment scope and methodology to meet your requirements. The below figure represents our assessment approach.

[redacted]

[redacted]

[redacted]

[redacted]

Our approach, based on our demonstrated IAM methodology, leverages tools and frameworks and not only assists with the fulfillment of the identified requirements related to IAM, but also provides with a futuristic view and assist in effectively architecting an Identity Governance and Administration solution. Based on the RFP requirements and your Q&A responses, we will be leveraging the applicable portions of our IAM framework to assess your Access Management, Identity Administration and Password Management.

[redacted]

We will work with you to develop an understanding of how your organization works, define the target state IAM program, determine an evaluation criterion for which IAM products aligns with your circumstances, as part of the overall strategy.

9.3.2 Key activities and milestones

In this section, Deloitte has defined the key activities and work products from our proposed IAM assessment approach.

Step 1: Planning & Current State Assessment

SOW Reference: Section 3 (Scope)

The scope may include, but is not limited to, the following activities:

- Analysis of the current security methodology. This should include, but not be limited to, a detailed analysis of Active Directory user groups.
- Analysis of application discovery to determine if additional applications benefit from the new model.

[redacted]

[redacted]

Step 2: Develop IAM Strategy

SOW Reference: Section 3 (Scope)

The scope may include, but is not limited to, the following activities:

- Design future state to enable (where appropriate):
  - Single sign on
  - Role based authentication
  - Same sign on
  - Multi-Factor authentication

[redacted]

[redacted]

Step 3: Develop Roadmap and Cost Estimates

SOW Reference: Section 3 (Scope)

The scope may include, but is not limited to, the following activities:

- Develop and document auditable controls and procedures including:
  - Roles and responsibilities for IS Operations, IS Security Office, business units, and authorized agency security teams
  - Criteria for determining appropriate role-based security constraints
  - Workflow for security requests
  - Workflow for security exception requests
  - Quality control assessments

- Recommend deliverables and plans for future sprints.

[redacted]

[redacted]

9.3.3 Project and Risk Management

SOW Reference: Section 3 (Scope)

The scope may include, but is not limited to, the following activities:

- Identify project risks, actions, issues and decisions using a risk register or RAID project register.

[redacted]

Based on our experience working on similar project within State of Texas and with various other clients, we propose to perform project management and communications in two distinct activities. The first step involves the establishment of the project management and communications framework whereas the second step incorporates the ongoing planning, reporting and communications activities necessary to facilitate the ongoing management of the project.

Some of the benefits ERS can gain from our project management approach include:

[redacted]

Deloitte's project management approach adheres to the standards of the Project Management Book of Knowledge® (PMBOK) and constitutes of following high-level steps:

- Initiation. Define, analyze, and decide
- Planning. Work breakdown structure, Resource Plan, project schedule, project budget, Performance Plan, and Project Plan is developed, and project processes and procedures are assessed
- Execution and Control. Defined activities for security assessment are conducted
- Close Out. Knowledge transfer is conducted; lessons learned are collected, close out financial accounts.

We have tailored our project management and communications approach in two distinct sets of activities, depicted by the table below:

Activity	Steps	Description
Establish Project Management and Communications Framework	Develop Project Plan (Work/Task Plan)	During the first week of the project, we will develop the project's task plan detailing the assessment activities. The project plan will contain Work Breakdown Structure (WBS), resource assignments, task owners and account for changes to the start date, holiday schedules, and constraints on stakeholder availability.
	Establish Baseline Project Management (EPMM)	Tailor EPMM documents as required and check into ERS-identified repository.

	Artifacts in ERS Accessible Repository.	
	Establish Issues and Risk tracking process (Issue Identification Report)	Establish issues and risk tracking format including vulnerabilities and risks, as well as the tracking details of the issues and risks to resolution.
Ongoing Project Management and Communications Activities	Weekly Status Reports	These status reports, delivered in the standard ERS format (if available), affords ERS project management the ability to assess the health of the project and review status items, issues, and risks. Deloitte will produce and circulate the status reports on a weekly basis and will save the status reports to the designated project document repository.
	Weekly Status Meetings	Given the duration of the project, we believe that weekly status meetings are essential to maintaining a healthy level of communication amongst project stakeholders. We will work with ERS to establish the participants and schedule the project team meeting. We will also assume responsibility for circulating meeting agendas and meeting minutes as well as saving the meeting records to the project's document repository.
	Updates to the Project Plan and Issues List	It is important that project management artifacts be kept in alignment with ongoing project activities. We will periodically update artifacts such as the project plan and issues list so that they can be used as effective communications vehicles regarding project progress, risks, and issues. In addition, Deloitte's project manager will notify the ERS project manager/CISO and obtain approval prior to making changes to the Deloitte project team members.

Agile Delivery

SOW Reference: Section 3 (Scope)

The scope may include, but is not limited to, the following activities:

The successful Respondent will work in a team-based Agile environment.

The successful Respondent will create and maintain system roadmaps, project plans, and security service releases that will be the basis for the successful Respondent's work.

Deloitte's comprehensive methodology is flexible to fit project objectives and provide a mature, transparent operational framework, which allows the team to quickly jump-start the project and efficiently drive the successive Agile/SDLC phases and deliverables. Deloitte supports early communication and close collaboration throughout the development life cycle with client stakeholders and other external partners to reduce risk and improve buy-in of the new system. Our approach encourages a sustainable system based on effective knowledge transfer and detailed documentation that supports ERS during design and implementation phases.

[redacted]

[redacted]

9.3.4 Work plan

Our approach is structured to drive value in a realistic timeframe using an experienced team and supporting accelerators. We anticipate a duration of up to [redacted], depending on the availability of ERS stakeholders, and the time taken to review the deliverables. As outlined in the diagram below, [redacted] and the conclusion of each step is a milestone for the project.

[redacted]

During the initial step of the project, we will develop a customized project plan listing specific tasks/activity for the project. The following diagram is a sample snapshot of the project plan which will be used to govern this project. This project plan, once created, will be updated in Week 1 after project kick-off and meeting with the ERS project manager and/or sponsor.

[redacted]

Please refer to Attachment A "Sample Project Plan" for reference work plan of IAM assessment.

9.3.5 ERS Responsibilities

During project execution, responsibilities will be shared between Deloitte and ERS. We have suggested the following roles, responsibilities and time commitment expectations of the ERS team (for the course of the assessment) in the below table:

[redacted]

9.3.6 Assumptions

We have relied on below list in agreeing to perform the Services and upon which it is based (the "Assumptions"). A deviation from these Assumptions may cause changes to our schedule, level of effort or otherwise impact our performance of the Services, and the parties will enter a Change Order as described herein to reflect any adjustments to the Services and/or pricing for the Services as a result thereof.

[redacted]

[redacted]

[redacted]

9.4 Pricing

The Respondent must provide a separate cost for each deliverable (or sprint as applicable) in this SOW. Respondent must provide a summary of any assumptions and exclusions. Respondent shall provide fixed pricing for the project design phase in the table below.

9.4.1 Project Design Phase Deliverables Pricing

Deloitte's Response

[redacted]

Total Cost	$92,500

Upon completion of the design phase, ERS and the successful Respondent shall mutually agree upon the Respondent's team capacity/capability. The final quantity of sprints to be completed by the successful Respondent will be determined by capacity and capability of the successful Respondent, as well as the continued ability to provide work in accordance with SLAs listed in Section 6. Change Orders or amendments to this SOW will be created for future sprints. Final decision to proceed with this SOW and future sprints will be determined by ERS.

Deloitte's Response

Our SOW is based on DBITS terms and conditions and offers a fixed fee pricing for the design phase. Our cost summary assumes that the project is executed per the scope and timeline outlined in our response. In the event the ERS requires additional support, ERS and Deloitte will follow the change management process which will include cost and schedule impact analysis for changes requested by ERS.

10. Schedule of Events and Response Guidelines

The following dates represent ERS's desired schedule of events associated with this Statement of Work. ERS reserves the right to modify these dates at any time, with appropriate notice to prospective Respondents.

Item	Delivery Date

SOW Release	June 19, 2019
Respondent Q&A session (conf. call)	June 25, 2019
Respondent written question deadline	June 27, 2019
Respondent Q&A/written question returns	July 1, 2019
Respondent SOW response deadline	July 23, 2019
Vendor Selection	September 25, 2019

11. Period of Performance / Schedule

The term of service for the contract between ERS and the successful Respondent in connection with this Statement of Work is for up to one (1) year, effective upon execution of both parties. Change orders and corresponding amendments may extend the term of service.

12. Points of Contact

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

By submission of a response, Respondent acknowledges that the applicable response and official answer may be shared with other vendors; and therefore, Respondents will not include any confidential or proprietary information in such responses. ERS will not identify the Respondent that submitted any particular response.

Other contract-related communications for this SOW must be directed through ERS Contract Manager:

Thomas Williams
200 E. 18th Street, Austin, Texas 78701
(512) 867-7347
tommy.williams@ers.texas.gov

Project issues must be coordinated with the ERS Project Manager:

Mark Xavier
200 E. 18th Street, Austin, Texas 78701
512-867-7154
Mark.Xavier@ers.texas.gov

Upon issuance of this SOW, employees and representatives of ERS other than the point of contacts identified in this section will not discuss the contents of this SOW with any Respondent, vendor, potential vendor, or their representatives. **Failure of a Respondent and any of its representatives to observe this restriction may result in disqualification of any related response.** This restriction does not preclude discussions between affected parties for the purpose of conducting business unrelated to this procurement.

13. 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, 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 vendor responses in confidence and shall release vendor responses only to personnel involved with the evaluation of the vendor responses 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 response, 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 response or in any supplemental information submitted to ERS. By submitting a response, 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, publicly 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 Office of the 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 Office of the Attorney General, to a court, or to any other person or entity.
Respondent acknowledges and understands that the Texas Office of the 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.

14. Mandatory Terms

The contract resulting from this SOW shall be governed by all of Terms and Conditions (T&Cs) of the Texas Department of Information Resources (DIR) Master Contract. The T&C's of the Master DIR Contract shall prevail and control over any terms and conditions of the selected Respondent and ERS. Selected Respondent shall not include any additional T&C's as an amendment or attachment to the T&C's of the DIR Master Contract. Additional ERS terms and conditions apply to this SOW (see also Section 8).

Notwithstanding anything to the contrary in this SOW or any subsequent agreement between ERS and the successful 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.

Deloitte Response

[redacted]

[redacted]

15. Change Requests

ERS and the successful Respondent affirm they are fully committed to successful delivery of services. All scope changes must be reviewed by both ERS and the successful Respondent. Change requests shall be executed as follows:

1. ERS and the successful Respondent will discuss the change request and mutually agree on the scope of the change.
2. ERS and the successful Respondent's representative will document the change.
3. The successful Respondent will determine the impact to (1) the test and implementation schedule and (2) cost, if any.
4. ERS and the successful Respondent negotiate an addendum to the ongoing service delivery documentation and other required service artifacts.
5. The successful Respondent and ERS will sign the change request which contains the information listed in steps 1-4 above.
6. Change Orders and corresponding amendments will be submitted to DIR for their review and approval. An amendment to the SOW will hold the highest order of precedence in the SOW.
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 ERS Chief Information Officer or his designee.

Signatures/Acceptance

Accepted by:

Deloitte Consulting LLP

Signature:

Print Name: Eric Reeder

Title: Managing Director, Deloitte Consulting LLP

Date: January 29, 2020

Accepted by:

Employees Retirement System of Texas

Signature:

Print Name: Porter Wilson

Title: Executive Director

Date: 6-3-2020

DIR Contract Number: DIR-TSO-4031("DBITS")

Texas Department of Information Resources

SOW ID# ERS-000019

DocuSigned by:
Hershel Becker
7F04C0B913D547B...

Hershel Becker

Chief Procurement Officer

6/12/2020 | 12:58 AM CDT

Appendix A – External Reference

Reference the Texas Private Prompt Payment Act and Appendix A of the DIR contract

Appendix B – Non-Disclosure Agreement

Reference the attached Non-Disclosure Agreement in the email solicitation

Appendix C – Software List

Sign and return attached Nondisclosure Agreement to obtain a copy of the Software List.