RFP 18-010
Service Organization Controls 1 Reporting Services
Questions from Vendors

Question #1
Has the RSA/PEEHIP ever had a SOC 1 Type 1 or Type 2 audit performed previously? If so, (a) when was the last audit performed, and who performed it; and (b) can the RSA/PEEHIP provide us with a copy of the most recent SOC 1 audit report?

Answer #1
Yes. RSA’s most recent SOC audit covered fiscal year 2017. PEEHIP is in the middle of its first SOC examination. The report for fiscal year 2018 will be issued later this year. We will not provide a copy of the most recent SOC 1 audit report.

Question #2
What is the impetus for the RSA/PEEHIP to request a SOC 1 Type 2 audit (ie: is there a specific need, requirement, or event causing this audit to be requested)?

Answer #2
GASB issued pronouncements (No. 67, 68, 74, and 75) that significantly changed the way in which public employee benefit plans and their participating employers must report the related liabilities and note disclosures.

Question #3
Who would be the report user to which the RSA/PEEHIP expects to provide the completed audit report each year?

Answer #3
Employers participating in RSA’s pension plans and/or the Public Education Employees’ Health Insurance Plan (PEEHIP) and their independent auditors.

Question #4
Reference Page 15, section M. Minimum Qualifications. The RFP requests references for 3 “clients for whom the firm has completed SOC 1 Type 2 reports”. We have completed a number of SOC 1 Type 2 audits/reports (including reports using the previous designations of SAS 70 and SSAE 16 audits) for different systems/areas for various large divisions of a much larger state entity. Would the RSA/PEEHIP accept each of the large divisions as separate clients (given that each division has separate management, and each audit was unique)?

Answer #4
Yes.

Question #5

Reference Page 16-17, section B. Technical Proposal. This section requests that the technical proposal "Describe the approach you anticipate following for each asset category and each area of operating revenues and expenditures. Be specific indicating expected use of confirmation, examination, analytical review, comparative analysis, etc. Specifically discuss your methodology utilizing a readiness approach, timing of the engagement, estimated number of hours, and estimated client involvement."

- a. A SOC 1 Type 2 Audit assesses the fairness of presentation, adequacy of design, and effectiveness of controls to achieve the stated control objectives. Therefore, we would have expected that the RSA/PEEHIP would desire that specified control objectives and the related controls to achieve the objectives would be the focus of the SOC 1 audit. Can the RSA clarify its expectations related to "asset categories" and "areas of operating revenues and expenditures"?
- b. If the RSA/PEEHIP has not previously had a SOC 1 audit performed, has the RSA/PEEHIP already defined and documented its control objectives and related controls to achieve the objectives that would be the subject matter for the audit; or is the expectation that the selected vendor will assist the RSA/PEEHIP in defining and documenting these?
- c. If the RSA/PEEHIP has already defined and documented its control objectives and related controls to achieve the objectives, can the RSA/PEEHIP provide them to us to allow us to scope the expected level of effort and cost to perform the requested services?
    - d. Related to "utilizing a readiness approach", does the RSA/PEEHIP desire that the selected vendor approach this engagement with an initial readiness assessment, followed by the actual audit for the first year?

Answer #5

5a – The successful proposer should have a thorough understanding of defined benefit pension plans and health insurance plans so that when the successful proposer reviews the internal control documents they should be able to determine what needs to be tested.
5b – RSA and PEEHIP have defined and documented their respective control objectives and the related controls to achieve those objectives.
5c – No.
5d – No.

Question #6

Two reports are requested, one for RSA and one for PEEHIP. Based on the description provided in section I B can you confirm the breakdown of the each of the reports as follows:

- a. RSA Report
    - i. Includes the TRS, the ERS, and the JRF and RSA administrative and support functions
- b. PEEHIP Report
    - i. Includes the PEEHIP, the PRT, and the RSA-1 and RSA administrative and support functions

Answer #6

The RSA report will include TRS, ERS, and JRF. The PEEHIP report will include PEEHIP and PRT. Both reports will include administrative and support functions that are provided to all of the plans. RSA-1 is not included in the scope of either report. The description of RSA-1 in the RFP was for informational purposes only

Question #7

Are the enrollment, contributions, distributions, valuation, and investment management controls different for the PEEHIP as compared to TRS, ERS and JRF?

Answer #7

No.

Question #8
Under minimum qualifications, you site that an audit Manager/Partner must possess a CISA certification. Can it be either the Audit Manager or the Audit Partner if the organization plans to have both roles on the engagement team?

Answer #8
Yes.

Question #9
Is there an established budget for this project you can share?

Answer #9
We are not disclosing this information as a part of the RFP.

Question #10
What did you pay your prior auditor for the SOC 1 Examination fees?

Answer #10
We are not disclosing this information as a part of the RFP.

Question #11
Does the RSA and/or PEEHIP host the data locally or is it outsourced to a third party data center?

Answer #11
Data is hosted locally.

Question #12
Does the RSA and/or PEEHIP utilize any third parties to assist in delivering the services identified in the scope of the SOC report? SSAE 18 would define these as, "subservice organizations." If yes, please describe their function and whether they are reported under the carve out or the inclusive method.

Answer #12
PEEHIP utilizes the following third-party administrators which are reported under the carve out method:

- BlueCross BlueShield of Alabama – claims administrator for the hospital/medical, supplemental medical, and flexible spending accounts.
- MedImpact – claims administrator for the prescription drug plan.
- Southland – claims administrator for the optional benefit plans: vision, indemnity, cancer, and dental.
- Artemetrx – benefits consultant related to pharmacy drug management.

Subservice Organizations related to investments which are reported under the carve out method:

- Bloomberg – processes trades and corporate actions.
- Eze Software Group – trade order management system.
- Omgeo – automates trade lifecycle events.
- State Street Bank – investment custodian.
- SimCorp – investment accounting and portfolio management.
- TradeWeb Markets, LLC – fixed income trading network.

Question #13
Section I, General Information for the Bidder, Paragraph D, Proposal Timetable, there is a statement that says "We also request a redacted physical copy and in electronic format". Earlier in that paragraph, it indicates that 6 hard copies of the proposal are required, and 1 electronic copy. What is meant by the additional redacted physical copy and in electronic format?

Answer #13
In addition to the 6 hard copies and 1 electronic copy that are not redacted, we want one redacted physical copy and one redacted electronic copy.

Question #14
Section II, Information Required from Bidders, Paragraph C, Cost Proposal, states that the pricing model must include the investment transactions and cycle, member contribution reporting, member retirement/withdrawal disbursements and participant data. Are each of these items applicable to both RSA and PEEHIP? Are we to assume in the pricing that the associated information technology controls are included in each of these areas?

Answer #14
Yes.

Question #15
If the RSA and PEEHIP have been audited in the past, what were the audit fees and how many auditors were in the field for how long?

Answer #15
We are not disclosing this information as a part of the RFP.

Question #16
Where is the actual location that work will be performed? Are all personnel at this location and controls performed at this location?

Answer #16
Yes, the actual location is the RSA Systems Building at 201 South Union Street in Montgomery, Alabama.

Question #17
How many employees would be considered in-scope for RSA?

Answer #17
Approximately 297 employees.

Question #18
How many employees would be considered in-scope for PEEHIP?

Answer #18
Approximately 261 employees.

Question #19
What are the primary applications used in delivering services related to RSA and PEEHIP, and please note if these applications are developed internally or by a third party?

Answer #19
Primary applications developed by a third party:

- Deloitte Pension Administration System which includes Library Manager, Work Manager, and Customer Relationship Management modules
- SimCorp Dimension
- My.statestreet.com and Corporate Action Tracking and Interactive Network – State Street Bank
- Eze OMS
- Bloomberg
- Omgeo – ALERT, OASYS Workstation, OASYS TradeMatch, Central Trade Manager, TradeSuite ID, and TradeSuite ID Confirm Archive
- TradeWeb
- TaxPort
- State of Alabama Accounting & Resource System (STAARS)
- Microsoft Dynamics Great Plains Receivables Management System

Primary applications developed internally:

- RSA Workbench System
- Contribution Reporting Application
- PEEHIP Benefits Administration System

Question #20
Is a formal risk assessment prepared for RSA and PEEHIP by the organizations themselves or any other oversight bodies? If so, would a copy of this risk assessment be made available to the selected bidder prior to fieldwork?

Answer #20
Yes.

Question #21
We retrieved a copy of the SOC 1 Type 2 report with period ending September 30, 2016 from the RSA website. Is this the most recent report? If not, can the most recent report be provided?

Answer #21
No.

Question #22
The RFP states that the engagement should begin no later than February 1, 2019. Can you provide the reporting period (i.e., October 1 – September 30) and when you expect fieldwork to be performed outside of the February date?

Answer #22
The reporting period is 10/1 – 9/30 with the report being issued no later than November 30 immediately following. We expect fieldwork to be performed in the spring and September.

Question #23
Will any additional services other than those in the previous report be covered in the proposed SOC examinations?

Answer #23
Yes.

Question #24
Are Cost Proposals to be provided separately (and excluded) from the proposal response? If so, how many copies of the Cost Proposal should be provided?

Answer #24
Yes. 6 copies.

Question #25
Is there a dedicated Project Manager at the State assigned to oversee the audits?

Answer #25
There is one point of contact to which all information requests should be sent.