



ADDENDUM NO. 4

REQUEST FOR PROPOSALS INFORMATION TECHNOLOGY CONSULTING AND AUDITING SERVICES RFP No. 2018-01-AUD

Addendum No. 4 is being issued to provide the questions submitted as of Thursday, October 4, 2018, and the related answers. Past questions are repeated.

1. Question: Do you have an estimate for the number of vendors you plan to award a contract to?
Answer: No, the number of contracts awarded depends solely on the RFP review.

2. Question: Is there an incumbent(s) or is this a new requirement?
Answer: This is a new contract; therefore, there is not an incumbent.

3. Question: Since you are awarding to multiple vendors do you expect each vendor to respond to all areas? For example, the key audit areas are below. Could we respond to 7 out of the 8 areas? Or are we required to respond to all areas?
 - Identifying IT assets managed internally and outsourced including, but not limited to, physical and virtual devices, operating systems and software;
 - IT Risk Assessments;
 - IT General & Application Controls Reviews;
 - Information Security Audits & Assessments;
 - Network and Cyber Security Audits & Assessments;
 - IT Policies and Procedures Review & Assessment;
 - Health Insurance Portability and Accountability Act (HIPAA) Compliance Reviews; and,
 - Payment Card Industry (PCI) Data Security Standard (DSS) Compliance Reviews.Answer: A vendor can chose to respond to any or all of the specific areas mentioned in the RFP as well as other related areas the responding firm believes they have expertise in.

4. Question: Can you provide the following:

- Number of locations?
- Number of IT Assets?
- Number of employees?
- Number of internal IPs?
- Number of external IPs?
- Number of Web Applications?

Answer: As noted in Section 2.3 of the RFP, "...the Comptroller's Office will not be able to answer any specific questions as to the current systems in place or anticipated. In addition, this section also notes that one of the anticipated services could be, "Identifying IT assets managed internally and outsourced including, but not limited to, physical and virtual devices, operating systems and software."

5. Question: Reference section 2.3 (last bullet). Does the County require that the PCI DSS reviews be performed by a certified assessor?

Answer: Yes.

6. Question: Reference section 3, item A. Does the Audit Division use an electronic working paper application (such as TeamMate or Engagement); and, if so, what application (and version of the application) is being used?

Answer: Yes. We are in the process of implementing AutoAudit, Version 6.5.

7. Question: What is the County's merchant level for PCI compliance (i.e.: Level 1, 2, 3 or 4)?

Answer: We do not know the answer to this question. As noted in Section 2.3 of the RFP, "...the Comptroller's Office will not be able to answer any specific questions as to the current systems in place or anticipated.

8. Question: Is this a year-round type of work to support all types of audit at the County's office? For example, financial statement audit, state specific required audit (what's the schedule), etc.?

Answer: Work under this contract will be awarded on a task/project basis.

Section 3.1 of the RFP:

It is anticipated that for each project, the County Audit Division, in coordination with the Comptroller, will work with one of the selected firm(s) to develop a specific scope with a good faith intention to use that firm to perform the project. After a specific project scope has been identified, the firm will be required to provide an estimate of hours needed to satisfy the scope with the hourly rates negotiated in the Contract and an estimated timeline for completion.

The number of audits and scope/tasks to be performed is not known and will change from year-to-year.

9. Question: How much weight is given to the rates? (pricing)

Answer: Price is not one of the criteria that will be used when evaluating proposals. See Section 4.2 of the RFP

10. Question: Is there a format to submit pricing?

Answer: Price is not one of the criteria that will be used when evaluating proposals. See Section 4.2 of the RFP

11. Question: Does the Comptroller have a budget in mind that can be shared?

Answer: In anticipation of issuing this RFP, the contractual services account was increased from \$100,000 to \$200,000 for Fiscal year 2018-19. This amount is not a guarantee of work. In addition, if needed, budget amendments can be requested.

12. Question: Does a vendor have the ability to work from their office location or only onsite at the Comptroller?

Answer: Work under this contract will be awarded on a task/project basis. The scope of each individual project will dictate the location of the work. It is anticipated that most work will be performed on County property

13. Question: Are rates by position required in the proposal?

Answer: Price is not one of the criteria that will be used when evaluating proposals. See Section 4.2 of the RFP

14. Question: Can you provide the most recent County Risk Assessment?

Answer: As noted in Section 2.3 of the RFP the anticipated services include, "Identifying IT assets managed internally and outsourced including, but not limited to, physical and virtual devices, operating systems and software" and "IT Risk Assessments."

Services such as this, if requested, would be considered a billable task.

15. Question: Section 2.3 Description of Requested Services. If internal network penetration testing will be performed, can it be done remotely if we provide a device?

Answer: If internal network penetration testing is a requested scope of service, the testing methodology will need to be coordinated with and approved by the appropriate Information Security personnel as well as County Audit

ADDENDUM NO. 4
RFP No. 2018-01-AUD

16. Question: Section 2.3 Description of Requested Services. How many locations will be part of the in-scope?
Answer: As noted in Section 2.3 of the RFP the anticipated services include, "Identifying IT assets managed internally and outsourced including, but not limited to, physical and virtual devices, operating systems and software". All locations are within Orange County, FL
17. Question: Section 2.3 Description of Requested Services. PCI – Has the Comptroller conducted approved security vendor (ASV) vulnerability scans?
Answer: The County Audit Division of the Comptroller's Offices has not performed such testing. It is not known whether any of IT Departments of the Board of County Commissioners or various Constitutional Offices have ever contracted for such services.
18. Question: Section 2.3 Description of Requested Service. PCI – will the Comptroller need to conduct a formal Report on Compliance (ROC) or support the Comptroller for conducting self-assessment questionnaires?
Answer: The type and extent of the PCI testing required for the Board of County Commissioners and various Constitutional Offices will not be known until a risk assessment is done of each entity's current PCI compliance status.
19. Question: Section 2.3 Description of Requested Services. Has the Comptroller ever experienced a breach?
Answer: The County Audit Division of the Comptroller's Offices is not aware of any breaches.
20. Question: Section 2.3 Description of Requested Services. Has the Comptroller undergone a Penetration Test in the past?
Answer: The County Audit Division of the Comptroller's Offices has not performed such testing. It is not known whether any of IT Departments of the Board of County Commissioners or various Constitutional Offices have ever contracted for such services.
21. Question: Section 3.1 (b) Deliverables. For PCI, will the PCI Templates be authorized to use for deliverables for the PCI reviews?
Answer: The type and extent of the PCI testing required for the Board of County Commissioners and various Constitutional Offices will not be known until a risk assessment is done of each entities current PCI compliance status.

22. Question: How many different vendors does the Orange County Comptroller expect to partner with to complete the planned audits in any given year? Or will one vendor be selected to assist with all IT Audit needs?

Answer: The number of firms selected will depend largely on the number of proposals received and the qualifications of the proposing firms. It is anticipated that the number of selected firms will not exceed two.

23. Question: Will these audits be under one contract, or will there be individual contracts required per audit?

Answer: A contract will be awarded to each selected firm. However, Work under this contract will be awarded on a task/project basis. As noted in Section 3.1 of the RFP,

It is anticipated that for each project, the County Audit Division, in coordination with the Comptroller, will work with one of the selected firm(s) to develop a specific scope with a good faith intention to use that firm to perform the project. After a specific project scope has been identified, the firm will be required to provide an estimate of hours needed to satisfy the scope with the hourly rates negotiated in the Contract and an estimated timeline for completion.

24. Question: How many audits does the Orange County Comptroller expect to complete this year, and in any given year thereafter?

Answer: The number of projects assigned each year will depend on a combination of the scope of selected projects, availability of firm resources, availability of County Audit resources and available funding. The Division is hopeful that a project will be ongoing at all times. It is not anticipated to be a sporadic investment of time and resources, but a continual process.

25. Question: What is the approximate/average number of hours each audit year will require?

Answer: The number of hours will depend on the scope of each selected project as well as a number of the factors noted above.

26. Question: What is the level of effort of scoping each project? Is it an option to include scoping as part of the audit execution itself?

Answer: Developing and contracting for a specific project scope is not considered billable hours and the level of effort necessary to develop a project/task scope, estimated hours, and time to complete would depend on many factors.

27. Question: If work papers are provided, who would organize and maintain them, and on what system will they reside, if any

Answer: In the event copies of work papers are requested, it is assumed they will be provided in an organized manner. How and where the work papers are maintained by County Audit will depend on the format the work papers are provided. If a working paper contains information that is exempt from public disclosure under provision of Florida laws, appropriate safeguards will be followed. .

28. Question: Under what circumstance(s) would work papers be required to be provided to the Orange County Comptroller?

Answer: As noted in Section 3.1 A. of the RFP, "All documentation obtained and created by a firm during the course of a project will be provided to the County Audit Division, if requested. It is anticipated that the Division will request copies of data and ask to review supporting information for conclusions reached."

It is likely that there will be instances where the Division requests evidence to support conclusions reached in certain circumstances. The support requested could be reformatted into any agreeable format as the specific working paper is not necessarily needed.

29. Question: How many example reports should be provided by each firm as part of the bidding process, and on what topics should they be related to specifically?

Answer: As noted in Section 4.1 of the RFP, "Sample reports including the deliverables stated in Section 3.B. can be provided with the proposal [Emphasis added]."

There is no requirement to submit any reports, but the number submitted is at the discretion of the responder. We would request that no more than five reports be provided.

30. Question: Is there a time of year that the Orange County Comptroller expects IT audit work to generally occur, or are the audits spaced evenly throughout the calendar year?

Answer: The timing of projects assigned each year will depend on a combination of the scope of selected projects as well as the availability of the firm's and County Audit's resources.

ADDENDUM NO. 4
RFP No. 2018-01-AUD

31. Question: Would any PCI Gap Assessment work result in either a Report on Compliance or a Self-Assessment Questionnaire being issued by the selected firm? What is the Orange County Comptroller's current PCI compliance reporting date?

Answer: The type and extent of the PCI testing required for the Board of County Commissioners and various Constitutional Offices will not be known until a risk assessment is done of each entities current PCI compliance status.

32. Question: How will proposed rates from each firm factor into the bidding process?

Answer: Price is not one of the criteria that will be used when evaluating proposals. See Section 4.2 of the RFP