Question	Agency	Question	Answer
1	RSM US LLP	On page 1 in the introduction, what does, "design and built" mean? a. Is V3 being implemented "out of the box" or truly built for San Mateo.	The V3 product is being designed, configured, and customized to meet the SamCERA requirements. The V3 product is configurable for customer needs, and customizable for customer-specific requirements. The SamCERA implementation of V3 is a mix of base-product and customer customizations.
2	RSM US LLP	How much customization to the product will there be?	We estimate that less than 20% of the SamCERA implementation relies on custom software code.
3	RSM US LLP	Did SamCERA do any initial mapping of legacy system data fields to V3 data fields? a. Were any significant changes or functional gaps identified?	It has been a part of the data conversion process throughout the project. There were no significant changes or functional gaps identified.
4	RSM US LLP	Have all the business processes been defined which will compliment or be a part of V3? Including the manual controls or human touches? a. Example - is the incoming mail opened by one person keeping the data secure? i. Is the paper scanned into V3 then shredded?	All of the business processes have been defined, including the manual controls and human touches. Incoming mail is opened by limited staff keeping the data secure, and the paper is scanned into V3 then shredded.
5	RSM US LLP	On page 2, when discussing materiality, who determines that amount? Us or SamCERA?	We expect the Contractor to indicate the severity of any deficiencies identified, using criteria agreed to by SamCERA.
6	RSM US LLP	On page 2, under security: during the implementation did you use the existing or built-in access control rules for segregation of duties? a. If not, how did you determine access? (who has access to what fields)	Existing, with some modifications. Access control by role was defined during the system design sessions.
7	RSM US LLP	On page 2, under process integrity: have all the calculations, algorithms, percentages, etc. been documented and is it the responsibility of the contractor to test these for accuracy and completeness? a. Example – who has access to what fields?	They have been documented, and it is the responsibility of the contractor to selectively test these for accuracy and completeness on a sample basis. We do not understand your reference to "fields". Contractor will be given necessary information for testing.

Question	Agency	Question	Answer
8	RSM US LLP	Is V3 vendor hosted or is it on premise? a. If on premise, do you intend to issue a SOC 1 or SOC 2 report for 2017?	Production is hosted and the test and Disaster Recovery environments are onsite. We anticipate that the Contractor will issue a SOC 2 report. Proposers are encouraged to provide separate cost estimates for SOC 2 reports for both hosted and onsite environments.
9	RSM US LLP	Some of the requirements are not internal control related. a. Some requirements are asked to determine if the system is performing as required or needed. For example, the ability to print a report i. Is verifying a report printed sufficient, "testing" ii. Could these items be given to SamCERA to reduce time and costs?	The Contractor is expected to identify the subset of requirements that are related to internal controls. Verifying a report printed will be considered sufficient "testing". These items may be given to SamCERA to reduce time and costs (specifically, as part of the planned user acceptance testing).
10	RSM US LLP	Is experience with Vitech's systems a prerequisite?	No.
11	MOSS ADAMS LLP	Has management conducted a risk assessment over the deployment of PASS and if so will you please provide?	SamCERA has been operating a risk management process throughout the project. SamCERA intends to perform a risk review specifically focused on deployment in the near future, and will provide the revised risk register to the Contractor when available.
12	MOSS ADAMS LLP	What operating system and database will PASS utilize?	Linux, Java, and Oracle.
13	MOSS ADAMS LLP	Are controls over the operating system and database in scope for this project?	Yes.
14	MOSS ADAMS LLP	Are controls over physical security in scope for this project? If so, are all physical resources located in San Mateo?	Yes. The hosted production environment is in New York. The on site location is in San Mateo County.
15	MOSS ADAMS LLP	Is an assessment over system segregation of duties needed as part of the access controls evaluation?	Yes.

Question	Agency	Question	Answer
16	MOSS ADAMS LLP	Will PASS have other system interfaces? If so, will controls over these interfaces be in scope?	There are no direct integrations with other systems, but there are portals for both member and employer self-service, self-service apps for iOS and Android, and other file-based interfaces (import and export).
17	MOSS ADAMS LLP	Will SamCERA resources only be available Monday-Thursday while the project in process?	Yes.
18	MOSS ADAMS LLP	Is there a limit on file size for the Company's email server?	Yes (36 MB).
19	PricewaterhouseCoopers LLP	Who are the final recipient(s) of this report? How is the report going to be used by SamCERA? Further, will the report be made public (ie) put on your website?	SamCERA management, Vitech project management, and the Board of Retirement. The report will be used to address material internal control deficiencies identified prior to V3 deployment. The report will be a public record and may be on the website.
20	PricewaterhouseCoopers LLP	Has SamCERA adopted a Controls Framework? a. If yes, please share the framework name and further also share the list of controls against which we shall evaluate your new PASS system. b. If no, would the scope of work include identifying a set of criteria and controls for each principal (Security, Availability, Processing Integrity and Confidentiality) as part of 19Phase 1 of our work? c. Does the scope of work also requires us to review your Project Management and IT General Controls (Change Management, Access Controls, Computer Operations and System Development Life Cycle including Data Conversion from old system to PASS system) as part of Phase 1?	No. Not applicable. The scope of work would include identifying a set of criteria and controls for each principle. The scope of work also requires reviewing the Project Management and IT General Controls.

Question	Agency	Question	Answer
21	PricewaterhouseCoopers LLP	SamCERA has provided us with the functional requirements (appx 1850) as part of Attachment A. Please confirm that the scope of work for both phases shall only include working with SamCERA to identify controls (as not all 1850 items are controls) and reviewing them for gap (in Phase 1) and design effectiveness (Phase 2).	Confirmed. The Contractor will review Attachment A to identify the controls, and review them for suitability of design (Phase 1) and operating effectiveness (Phase 2).
22	PricewaterhouseCoopers LLP	Does the scope of our work for Phase 1 include comparing your Functional Requirements provided against Solution Design Documents? If yes, please confirm that the expectation of our review would include review of available documents prepared as part of the project to identify gaps based on general best practices.	Yes. Confirmed.
23	PricewaterhouseCoopers LLP	On Page 1, Para 4 discusses that the audit objective should ensure Compliance with legal and regulatory requirements. Please share the list of legal and regulatory requirements for us to scope our work.	SamCERA operates under authority granted by the County Employees Retirement Law of 1937, also known as the '37 Act (Government Code section 31450 et seq.), California Public Employees' Pension Reform Act of 2013 (PEPRA) (Government Code Section 7522-7522.74, the regulations (on our website), under Board/Governance procedures and policies adopted by the SamCERA Board of Retirement (on our website under Board/ Governance), the Board of Supervisors may also adopt resolutions and ordinances which may affect the benefits of certain groups of SamCERA members (SamCERA will provide if deemed needed) and finally, IRS Codes and regulations applicable to SamCERA (which are reflected in Article VIII of the Board of retirement regulations). SamCERA will give specific direction in regards to the statutes applicable for the audit to the selected Contractor. It is not anticipated that there will be a lot of sections.
24	PricewaterhouseCoopers LLP	Can you elaborate further what is expected around "efficiency" in Page 2 Para 3 of the RFP?	We do not expect efficiency to be the focus of this audit. However, we want Contractors to take efficiency into account when making any recommendations.

Question	Agency	Question	Answer
25	PricewaterhouseCoopers LLP	Is PASS on Premise or cloud-based system? Will Vitech share a copy of their SOC 2 report if this is a Cloud based implementation?	See response to Question 8. We will request a copy of any applicable Vitech-issued SOC reports.
26	PricewaterhouseCoopers LLP	Does execution of the work require specific clearances (security), permits or licenses? If yes, please share further details on this requirement so we can staff the engagement appropriately.	No.
27	PricewaterhouseCoopers LLP	Have you done any prior audits of this implementation? If yes, share high level details and outcomes of such an audit.	No.
28	PricewaterhouseCoopers LLP	For delivering high quality work in an efficient and effective way, we do get our Global Shared Services (that might be located outside of United States) to support our audits, is that acceptable as part of the contract?	Yes.
29	PricewaterhouseCoopers LLP	Is SamCERA considering a AICPA SOC 2 Type 2 report for the PASS system in the future?	See response to Question 8.
30	PricewaterhouseCoopers LLP	Based on our reading of the RFP we are seeing that there may be two tracks (a) IT audit of the PASS system around Security, Availability etc (b) review of Functional and Technical requirements to validate the system has the 1850 (appx) functionalities built into it. As you will appreciate the scope of work and our associated professional fees for the above review is completely different. So if you could please clarify if one or both tracks are in scope that would be much appreciated.	See response to Question 21.

Question	Agency	Question	Answer
31	Macias Gini & O'Connell LLP	The audit objectives include: a) ensuring compliance with legal and regulatory requirements, as well as, b) the confidentiality, integrity, and availability of the information maintained in or generated from the PASS system. a. Did SamCERA receive a detailed plan from its vendor prior to implementation to ensure the above can be achieved? b. Is this plan available for review? c. Please provide the specific legal and regulatory requirements you would like compliance with.	SamCERA did not receive a separate detailed plan from its vendor prior to implementation. This is in the System Design Documents. The System Design Documents will be available for the selected contractor's review. The specific legal and regulatory requirements are addressed in the response to Question 23.
32	Macias Gini & O'Connell LLP	Did SamCERA monitor and evaluate the functional requirements during the implementation phase of the project? If yes, can you provide the details of your monitoring procedures?	Yes. The functional requirements were confirmed during the first phase of the project, and at that time, were allocated to numerous design sprint sessions. At the end of each sprint, verification sessions were conducted to evaluate whether the requirements allocated to that sprint were met. Four validations were also conducted to re-test the integrated work performed during sprints, again, validating that requirements were met. We will identify undelivered or untested requirements prior to the start of user acceptance testing.
33	Macias Gini & O'Connell LLP	In both Phase 1 and Phase 2, you have described 4 out of 5 Trust Services Principles. Are you requesting an examination, in essence a SOC 2 opinion, or just a review?	See response to Question 8.
34	Macias Gini & O'Connell LLP	Have you prepared your system description and identified specific controls related to the criteria associated with the trust services principles?	No.
35	Macias Gini & O'Connell LLP	Has SamCERA obtained a SOC 2 report from its new vendor, V3, for the PASS system? a. If so, what is the reporting period of the SOC 2 report? b. Is the SOC 2 report available for review by us?	See response to Question 25.

Question	Agency	Question	Answer
36	Macias Gini & O'Connell LLP	Why did SamCERA change software? Was it functionality? Please provide additional information regarding the need to change software.	The following is the stated mission from the PASS RFP: "The current pension administration system is fifteen years old and no longer fully meets the SamCERA business needs. SamCERA would like to take its current pension administration business processes (both human and electronic), and improve and/or integrate those processes into PASS. SamCERA would like to ensure that the data used in PASS is of the highest quality. SamCERA would like to integrate PASS with Enterprise Content Management (ECM) to improve access to member, staff and board documents and to improve SamCERA's ability to continue business in the case of a disaster." Please note, ECM is now unified within PASS, so there is actually no integration required.
37	Macias Gini & O'Connell LLP	When will your selection process be completed and successful bidder notified?	We anticipate that the selection will be made the week of July 25th.