**Scoping Questionnaire**

**SOC 1/SOC 2/SOC 3/SOC4Cyber /ISAE 3000/3402**

**Administrative / Business Process/ Entity wide reports**

|  |  |  |
| --- | --- | --- |
| **No.** | **Question** | **Response** |
|  | What is the legal name of your organization? |  |
|  | What are the name, title, and address of the person whom the engagement letter should be addressed to? |  |
|  | Has consideration been given to the fact if the report will be a SOC1 / SOC2 / ISAE 3000/3402? |  |
|  | Do you currently hold any security process certifications such as ISO 27001/2, NIST 800-53 etc. |  |
|  | Would you need a readiness / pre-assessment before doing the report? |  |
|  | A Type I report is only as of a point in time and a Type II report covers a period of time. Will this be a Type I or a Type II report? If Type II what is the proposed period coverage of the report? |  |
|  | Are there any other compliance initiatives that your company wishes to address at this time such as \_\_\_\_\_\_\_\_ |  |
|  | Are there any commitments to your clients to provide the report by a particular date? |  |
|  | What is the scope of the services your organization provides? If you have any material that describes your services in detail please provide that as well. |  |
|  | Are there any specific industries or clients that the business focuses on? |  |
|  | How many personnel are within your organization that performs the services noted above? |  |
|  | Are there / will there be any anticipated new services or changes to existing services during the proposed review period? |  |
|  | Is this a general distribution report or meant for only one specific client? |  |
|  | If SSAE 18- SOC / ISAE , has the company established a preliminary list of control objectives? |  |
|  | If SOC 2 report which of the following principles would be applicable based on your customer/s’ requirements?   * Security * Availability * Confidentiality * Privacy * Processing Integrity   **(Normally it is opted for Security, Availability & Confidentiality)** |  |
|  | Where are the location(s) of the personnel under the scope of the audit? |  |
|  | Where are the locations where the IT Systems / Infrastructure under the scope of the audit exist? |  |
|  | Are there any parts of the processes or controls that are outsourced to a third-party vendor (also referred to as a sub-service organization in SSAE 16 / SOC 2 /ISAE 3402 terminology) that should be included within the scope of this review? If, yes, please provide a brief description of the services the subservice organization/s provide? |  |
|  | Where is the subservice organization located? |  |
|  | Does the subservice organization have an SSAE 16 or any other independent third-party examinations of their controls performed? |  |

**Technical**

|  |  |  |
| --- | --- | --- |
| **No.** | **Question** | **Response** |
|  | What is the IT Infrastructure used to deliver your services? Please specify details in no of nodes etc.   * 1. Network   2. Operating System   3. Database   4. Applications |  |
|  | Are there any anticipated significant changes to the applications or IT systems including new implementation or significant upgrades to applications / IT systems? |  |
|  | Do you perform programming and development efforts of the production applications? If yes, please provide a high level overview of tools used for software development / maintenance and any supporting systems to track the SDLC / Change Controls process. |  |

**Cloud Offering Specific Questions (this is only applicable if you are taking into consideration cloud services)**

|  |  |  |
| --- | --- | --- |
| **No.** | **Question** | **Response** |
|  | Which of the following characteristics does your cloud offering provide for?   1. On-demand self-service 2. Broad network access 3. Resource pooling 4. Rapid elasticity 5. Measured service |  |
|  | Which of the following service models do you offer?   1. Software as a Service (SaaS) 2. Platform as a Service (PaaS) 3. Infrastructure as a Service (IaaS) |  |
|  | Which of the following deployment models do you offer?   1. Private cloud 2. Community cloud 3. Public cloud 4. Hybrid cloud |  |
|  | Are there any specific industries or clients that the cloud offering focuses on? |  |
|  | Are there situations within your cloud environment where data is processed or stored trans-nationally? |  |
|  | How many personnel are within your organization are dedicated to your cloud services offering? |  |