

Response to Request for Clarification ITN:
2022 Governance, Risk and Compliance (GRC) Assessment

| | Question | Answer |
|----|---|--|
| 1 | Is this funded by a federal grant or under a prime federal grant? | No |
| 2 | Do you have a budget for this work and, if yes, what has been allocated (either dollars or hours)? | The prior GRC assessment vendor signed the contract in August 2017 and the report was issued in January 2018. We expect this assessment to be completed within the same time frame of 5-6 months. The fee structure is dependent on the methodology of the responding vendor and their resources needed to perform that methodology. |
| 3 | Does the SBA anticipate leveraging the awarded vendor for any recommended corrective actions? | Potentially |
| 4 | We are not publicly traded; however, we do have a peer review in replacement of financial statements. Will SBA accept the peer review letter? | Yes |
| 5 | What encryption technology is approved by SBA? | Current National Institute of Standards and Technology (NIST) recommended encryption algorithms and protocols are approved for use by SBA. Others will be considered on a case-by-case basis. |
| 6 | Has the SBA had a GRC Assessment performed in the past? If so, | Yes |
| | a. Who conducted the most recent GRC Assessment? | Funston Advisory Services |
| | b. When was the most recent GRC Assessment performed? | Report was issued in January 2018; contract was signed August 2017 |
| | c. What were the fees and hours expended for the most recent GRC Assessment? | <i>Repeat question - see #2 above regarding budget.</i> |
| | d. May we receive a copy of the most recent GRC Assessment report? | The vendor selected for the project will be provided with the report issued in January 2018. |
| 7 | Would the Consultant be able to complete the work remotely, or would the Consultant need to be onsite at the SBA? | Preference is for the consultant to be onsite, however depending on the environment at the time, remote work may be acceptable. |
| 8 | What is the SBA looking for in a Consultant? | The elements are indicated in the ITN for what we are looking for in a consultant for this project. |
| 9 | <i>What is the SBA's cost estimate for the requested services?</i> | <i>Repeat question - see #2 above regarding budget.</i> |
| 10 | Does SBA have a strategic plan and does it address GRC? | Yes |
| 11 | Does the scope include relationships and reporting to the Board and its direction, oversight and control? | Yes - see Scope of Services, Section 2.1 |
| 12 | Has SBA been tracking the implementation of the recommendations of the prior GRC review? | Yes |

Response to Request for Clarification ITN:
2022 Governance, Risk and Compliance (GRC) Assessment

| | | |
|----|--|--|
| 13 | Would SBA like an assessment of progress relative to prior GRC recommendations? | Yes |
| 14 | To what extent, are there existing GRC process documents or process maps from which a current state assessment can be performed? | We have the process maps prepared during the previous GRC Assessment that can be used as a starting point in performing this assessment. These process maps will need to be updated to reflect any changes to the process since the previous assessment. |
| 15 | If there are existing GRC process documents, maps, or flowcharts, is there a standard that has been deployed across all major GRC processes? | They are in the format as provided by the consultant during the previous assessment |