The Santa Fe Group

SIG Web Application –Definition and Design Phase

Request For Proposal

Issue Date: May 11, 2017

Proposal Due Date: June 9, 2017

1. Summary and Background

Summary

The Santa Fe Group (SFG) is seeking proposals for the 'Definition and Design' Phase of a new web application. The purpose of this web application is to provide users with the ability to scope and respond to the Standardized Information Gathering (SIG) questionnaire. With over 1300 questions, the SIG is used to perform an initial vendor assessment and is critical to the third party (vendor) risk management lifecycle. By using the SIG, a company can obtain the information necessary to conduct an initial assessment of a service provider's cybersecurity, IT, privacy, data security and business resiliency controls. The SIG is reviewed annually, with updates and revisions made based on referenced industry regulations, guidelines and standards, including NIST, FFIEC, ISO, HIPAA and PCI. Currently, the SIG and a comparison spreadsheet called the SIG Management Tool (SMT), are MS Excel files provided to our clients.

Because of the complexity of the macros in the Excel sheet, it is easily broken, and not flexible or secure. The SIG web application will take the current MS Excel user experience online, providing a robust, secure, intuitive web experience. In addition, it will provide functionality for collaboration, communications, and analytics such as tracking SIG usage.

This Request for Proposal (RFP) is focused solely on creating custom visual concepts, the user experience design, the functional requirements, and the planning for the technical development for this web application. Although there is no technical development associated with this RFP, SFG intends to contract with the same vendor for the development, testing, and release phases of this project once this Definition and Design Phase is complete. SFG will evaluate bidders on both their design and development offerings and experience.

Background

The Santa Fe Group (santa-fe-group.com) provides custom strategic advisory services in the areas of cybersecurity, fraud, payments risk, and emerging technologies to create solutions for a more secure economy. SFG is the creator, thought leader, and manager of the Shared Assessments Program (sharedassessments.org), the trusted source for third party risk management. Shared Assessments (SA) provides a framework and certification, and creates tools and best practices to effectively manage the critical elements of the vendor risk management risk lifecycle.

We are not a software product company and do not plan to become one. We need help in designing an intuitive, flexible, secure, and effective web application that can grow in functionality over time.

2. Proposal Guidelines

2.1 This RFP represents the requirements for an open and competitive process. Proposals will be accepted until 5pm EDT on June 9, 2017. Any proposals received after this date and time will not be considered.

2.2 Proposals must be emailed to RFP@santa-fe-group.com. Please provide all documents in .PDF format.

2.3 Proposals must be signed by an official agent or representative of the company submitting the proposal.

2.4 Costs included in proposals must be all-inclusive and include any outsourced or contracted work. Any proposals which call for outsourcing or sub-contracting work must include the name, location, and description of the work to be provided. All terms and conditions of any contract with SFG are binding for all sub-contractors.

2.5 The top three bidders will be asked to present their proposal to the SFG team via teleconference prior to award. SFG may visit the offices of the top two bidders where the work is to be performed. The purpose of the visit is to tour the office and meet office leadership and project team, if available.

2.6 Although SFG intends to award a contract, SFG is not required to award a contract. There will be one (1) award for this RFP, if an award is made.

2.7 Contract terms and conditions will be negotiated upon selection of the winning bidder. All contractual terms and conditions will be subject to review by the SFG legal department.

2.8 All Proposals submitted will remain valid for sixty (60) days from the date on which proposals are due, unless the period is extended by agreement between SFG and the affected bidders.

2.9 SFG is not responsible for any of the costs of preparing, presenting, or submitting a proposal.

2.10 Oral communication between SFG staff and prospective bidders is unofficial and non-binding. Bidders may rely only on written information issued by the designated SFG staff member who is managing the RFP process. The designated staff member's name and email address will be sent out once a bidder's Intention to Respond is received by the due date.

2.11 All questions should be submitted via email to RFP@santa-fe-group.com. Telephone calls will not be returned during this RFP process.

2.12 Ownership of the design and all content (including source files) will be transferred to SFG upon completion of the project.

3. Success Criteria

The following criteria must be met to achieve a successful project:

3.1 The design is user-friendly, intuitive, and easy to navigate.

3.2 Current users of the MS Excel spreadsheet can transition easily to the online application.

3.3 The design is clean, simple, and visually consistent with SFG/SA brand guidelines and is ADA compliant.

3.4 The process for updating and maintaining website content is straight-forward for SFG administrators and content creators.

3.5 The web application design and planned architecture is based upon proven and accepted secure website development standards while maintaining flexibility to grow and add new functionality over time with minimal cost.

3.6 The web application is designed to capture appropriate analytical data informing future improvements and other aspects of SFG/SA work.

4. Project Scope and Deliverables**

Targeted Users

This is a high-level description of the user types involved in the assessment process to provide bidders with context. It is not meant to be exhaustive or a complete picture. It is a general description of how different user roles could interact with the SIG application. A demonstration of the SIG, the SIG and SMT Excel files, and the functional requirements captured to date, which will be provided to bidders once the signed NDA is received, will also provide additional insight into SIG user types and functionality.

4.1 **Outsourcer**

An Outsourcer is a company that uses the SIG to obtain all the information necessary to conduct an initial assessment of a third party's cybersecurity, IT, privacy, data security and business resiliency controls. The number of questions within the SIG can vary depending on whether the Outsourcer uses the SIG LITE or the FULL SIG. In the next MS Excel version to be released at the end of 2017, and on the web application, an Outsourcer will have the ability to filter the questions depending on the specific type of service being outsourced to the third party. An Outsourcer company may have several role types:

4.1.1 **Assessor:** A risk professional who needs to assess the risk levels of potential third party service providers, or 'Assessees'. The first step for the Assessor is to create a Master SIG. A Master SIG file represents the ideal answers to the SIG that align with the level and types of risk controls an Assessee should have in place.

4.1.2 **Procurement (Sourcing) Professional:** A procurement staff member who may send the SIG to a new third party for them to complete as part of an organization's RFP process, but is not involved in assessing the risk levels (SIG answers) of third party service providers.

Once an Assessee's SIG is completed and returned to the Outsourcer, the Assessor will use the SIG Management Tool (SMT) to compare the Assessee SIG to the Master SIG, analyzing gaps and following up with the Assessee for more information and support documentation, as needed. Ideally, in the web application, the SIG questions identified by the Assessor as needing follow-up can be extracted from the returned SIG and tracked as open issues through an issue management function in the application.

4.1.3 **Outsourcer-SME:** If an answer or section from an Assessee's SIG is flagged in the SMT review, the Assessor may need to send it to a Subject Matter Expert (SME) within their own company to assist in determining if the answer or section is acceptable for a targeted product or service or if follow up is needed. The SME will provide comments back to the Assessor, who will follow up with Assessee as needed.

4.2 **Assessee**

An Assessee completes the SIG by answering the binary questionnaire and by providing additional information and documentation if a question requires more explanation. An Assessee company may have several role types:

4.2.1 **Assessment Manager:** An Assessment Manager is responsible for answering or compiling the SIG answers for a company. He/She answers the questionnaire and provides added description or documentation if a question requires more explanation. This process is currently done with excel files via email with the Outsourcer. If an Assessee provides one service, they can complete one SIG questionnaire, which can then be shared with multiple clients. If an Assessee provides more than one service, they may be required to fill out a SIG per service provided. Also, if an Assessee provides the same service from multiple locations, an assessment may be required for each physical location from where the service or product is provided.

4.2.2 **Assessee-SME:** As with Outsourcers, an Assessee may need to consult SMEs within their own company to assist in answering questions and may assign sections to other users, then compile answers into a final SIG for submittal to an Outsourcer.

4.3 **Administrator**

An Administrator manages user permissions for the SIG within the Outsourcer or Assessee company. For example, an Assessor may have permission to add custom questions to the SIG, but a Procurement Professional may not have that permission.

4.4 **Self-Assessor**

A company will use the SIG to assess the risk controls within their own company. The user may assign sections of the SIG to their own SMEs to answer, then combine sections and analyze the results. This will likely lead to a report or plan for improvements.

4.5 **SFG Administrator**

SFG staff member(s) administrator who updates SIG questions and related content through a CMS and creates analytics reports. SFG Staff will also be responsible for user support functions.

4.6 **Content Licensee**

Downloads an XML file of the latest version of the SIG to use the content in their own proprietary system.

Definition and Design Phase Scope Description

Please note: The SIG questions, their organization, and their relationship mapping with risk controls and regulations already exists and will be vetted and updated by SFG and SA. The bidder will not need to revisit the validity of this content as part of the scope of this project.

Project Scope Overview:

4.7 **Consistent Website Design** – Website design must remain consistent throughout all pages to maximize usability. The bidder will provide the design for the user interface, including infrastructure, visual elements, interactive elements, and color schemes of the application based on the functional requirements and current brand guidelines.

4.8 **Design Overview** – Usability, simplicity, security, and flexibility are paramount to the application design. The web application must be built using a flexible framework that can adapt to the ongoing advances in technology, can easily be updated and added to on a rolling basis, and can integrate with SFG's existing platforms, if applicable.

4.9 **ADA Compliant** - Website templates must be ADA / 508 standards compliance.

4.10 **Design Process** – SFG expects to work iteratively with the vendor, having interim and final design review sessions and final signoff in all aspects of the design and functionality.

4.11 **Well considered Functional and Technical Requirements** – The vendor to provide the technical requirements and framework for building the site given the technical goals of project. The vendor will update, validate, and formalize the functional requirements started by SFG. The existing functional requirements will be provided to all bidders once the Intention to Respond and the signed Non-Disclosure Agreement are received by the designated due date.

Suggested Deliverables**:

4.12 **Competitive Insights** - A summary of competitor sites which includes the strengths and weaknesses of the design, interaction, functionality, and pricing model. This is not meant to be an in-depth competitive analysis. It is meant to provide quick insights and impressions to help distinguish our product and inform the design team of the competitive landscape.

4.13 **Two (2) to three (3) visual design concepts rendered on three (3) main pages** – SFG will down select to one concept for the final design. That final design selection will be mocked up on several pages for review before final sign-off.

4.14 **Wireframes –** Low-fidelity wireframes for all identified page types.

4.15 **Content Design Strategy and Requirements** – Identify and provide the content required, other than the existing SIG questions and content already in the SIG. Provide the organization, layout, and templates for the content. Also, recommend a content management system (CMS) and a CMS implementation plan. The CMS must be flexible, easy to use, and not compromise the integrity of the web application's design. The exact CMS functional and system requirements will be determined as part of this project.

4.16 **Information Architecture** – Describes how the user interacts with the site to find and use the information they need to complete all aspects of the SIG assessment process.

4.17 **Functional Requirements** - Collaboratively update, edit, and finalize the existing list of functional requirements provided by SFG.

4.18 **Technical Framework** - Document the technical architecture of the web application that satisfies the finalized business and functional requirements. It should include the technical requirements, process of development, specifications, and proposed guidelines.

- 4.18.1 Technical Framework should also include a plan and recommendations for:
  - 4.18.1.1 Browser Support/Cross Browser Compatibility/Legacy Browser Support
  - 4.18.1.2 Security protocols including Encryption
  - 4.18.1.3 Hosting Services
  - 4.18.1.4 CMS
  - 4.18.1.5 Analytics
  - 4.18.1.6 Any other product recommendations and the potential additional costs associated with building and supporting the application (i.e., CMS, cloud-based software).

4.19 **Usability Testing and Summary Report** - Test interaction and identify issues with visual design, navigation, and layout using low fidelity methods. SFG will be responsible for identifying current SIG users for testing. SFG envisions no more than 8 to 10 users from varying companies and service verticals. This testing may need to be remote as users are spread across the U.S. Keeping overall budget in mind, provide a description of the type of testing and any additional costs associated with testing in your proposal, if applicable.

***SFG is open to alternative deliverables as suggested by the bidder in accordance with their methodology and expertise. The final deliverables of this phase must provide a clear understanding of the visual and interaction design, the user experience, the functional and technical requirements, and the technical architecture. The intention of the deliverables of this project is to provide enough information to allow developers to immediately start building the site. Please provide thorough definitions of all deliverables in your response.*

5. Request for Proposal Timeline

Request for Proposal Timeline:

5.1 Email RFP@santa-fe-group.com with your Intention to Respond by 5pm EDT on May 18, 2017. Please include the signed NDA (Attachment A), company name, primary contact person's name, email address, and phone number in the body of the email. The expression of intent is not binding but will greatly assist us in planning for the SIG demonstration and proposal evaluation process.

5.2 SFG staff will have a demonstration of the functionality of the existing SIG tools via WebEx on May 23, 2017 at 2pm EDT. Invitations to join the demonstration, the current version of the SIG and SMT, and the draft functional requirements will be sent to the primary contact stated in the Intention to Response email once a signed NDA is received.

5.3 All inquiries regarding this RFP including requests for additional information or clarification, must be submitted in writing to RFP@santa-fe-group.com. Inquiries must be received no later than 5pm EDT on June 2, 2017. All questions and answers will be posted to http://conta.cc/2prAq8J during the period of May 12, 2017 to June 5, 2017.

5.4 **All proposals in response to this RFP are due no later than 5pm EDT on June 9, 2017**.

5.5 Evaluation of proposals will be conducted from June 10, 2017 through July 12, 2017. If additional information, questions, or discussions are needed with any bidders during this time, the bidder's primary contact will be notified.

5.6 The winning bidder will be notified no later than 5pm EDT on July 13, 2017. Notifications to bidders who were not selected will also be completed no later than 5pm EDT on July 13, 2017.

5.7 Upon notification, the contract negotiation with the winning bidder will begin immediately. If the terms and conditions of a contract cannot be successfully established within a reasonable amount of time (as determined by SFG), then contract discussions will be terminated and contract discussions with the next highest ranking bidder will commence.

5.8 Work is expected to begin within one (1) week of contract signature. The entire project team is expected to be available on project start date.

5.9 RFP Schedule Summary*:

RFP Schedule	Dates
Intention to Respond and signed NDA Due	5/18/17
SIG Demonstration Teleconference	5/23/17
Questions Period Begins	5/12/17
Questions Period Ends	6/2/17
Bidder Responses Due	6/9/17
Notification of Award	7/13/17

*schedule is subject to change

6. Phase/Project Timeline

SFG intends to begin this phase of the project no later than the first week of August 2017. SFG plans to launch this web application in December 2017.

7. Pricing & Project Plan

7.1 All Proposals must include proposed costs to complete the deliverables described in the project scope. Costs should be stated as one-time or non-recurring costs. Proposal should also include requested payment

schedule (e.g., *X% at start of project, X% upon sign-off of X deliverable*). All assumptions and dependencies must be clearly stated in the response.

7.2 Proposals must include a tentative project plan which includes timeline, tasks, milestones, and delivery dates. Bidder will have an opportunity to update the project plan after award. The contract will include a detailed project plan with specified delivery dates.

7.3 Proposals must include a list of the project team roles and percentage of time to be spent on the project (e.g., Interaction Designer, 50%).

8. Bidder Qualifications

Bidders should provide the following items as part of their proposal:

8.1 One sample of bidder's work for each of the proposed deliverables.

8.2 Organization description, including services offered, number of full-time employees, number of sub-contractors, location(s) where work is to be performed, and years in business.

8.3 Although this RFP does not include development of the application, bidder should include a description of their experience and expertise in developing web applications, including methodologies used, years of experience, and the Development and QA Testing team's organizational structure or hierarchy.

8.4 Description of experience with content management systems implementation, cloud-based services implementation, and analytics software implementation.

8.5 Proof of financial stability.

8.6 Organization security policies including type of background checks done on employees and contractors (if any), client data handling, and SSDLC.

8.7 Bidders must list and summarize all pending or threatened litigation, administrative or regulatory proceedings or similar matters. Bidders shall have a continuing obligation to disclose any such actions during the period of this RFP.

8.8 Examples of two (2) or more web applications designed and developed by your organization within the last three (3) years.

8.9 A minimum of two (2) references from past clients for whom you have provided similar work in the last five (5) years.

8.10 A description of your project management methodology.

8.11 A copy of your Masters Services Agreement (MSA) template, if available. If a template is not available, include suggested terms and conditions that will apply to the MSA and the statement of work (SOW).

9. Proposal Evaluation Criteria

9.1 Expertise in website design best practices and experience with designing complex interactions.

9.2 Methodology proposed including how SFG will be involved in the process.

9.3 Satisfaction of previous clients with communications, quality of design, quality of code, website performance, project risk mitigation, overall attitude and culture, and likelihood of continued business.

9.4 Internal privacy and security policies and implementation as it relates to SSDLC, client data handling, and employees and contractors.

9.5 Overall proposal suitability: proposed solution(s) must meet the scope and needs included herein and be presented in a clear and organized manner.

9.6 Cost of the solution based on the work to be performed in accordance with the scope of this project.

9.7 Because SFG intends to contract with the bidder on the development, testing, and release phases of this project, bidder will be evaluated on their development and testing capabilities, experience, and methodologies.

10. Good Faith Statement

All information offered by The Santa Fe Group is offered in good faith. Specific items are subject to change at any time based on business circumstances. The Santa Fe Group does not guarantee that any item is without error. The Santa Fe Group will not be held responsible or liable for use of the information or for any claims asserted therefrom.

Attachment A – Non-Disclosure Agreement

Please sign and return to RFP@santa-fe-group.com as an attachment to your Intention to Respond email due no later than May 18, 2017 5pm EDT.

MUTUAL STATEMENT OF NON-DISCLOSURE

_____ _____, hereafter referred to as "(Client)," and Santa Fe Strategy Center Ltd. d/b/a **Santa Fe Group**, hereafter referred to as "Santa Fe Group," agree to hold in confidence and not use, other than for the purposes described herein, all confidential information provided by either or the other, and not to publish or disclose such information to any third party without the other's written permission except as provided herein. By Confidential Information, Santa Fe Group and (Client). mean all materials, documents, data, technology, customers, processes, and other information, regardless of form, which may reasonably be designated as proprietary and confidential and/or is identified or marked as confidential at the time of its disclosure. This includes, but is not limited to, all proprietary financial data, policy and business plan information, strategic information and plans, business process information, and any customer or third party information either party is obligated to keep confidential. Notwithstanding the foregoing, Confidential Information of (Client) and Santa Fe Group and their respective customers shall not be deemed to include any information (including inventions, innovations, or information) that is (1) already within either (Client) or Santa Fe Group respective general knowledge, skills, and experience, (2) already known by either (Client) or Santa Fe Group or is readily ascertainable (without use of "improper means" as defined in California Civil Code section 3426 et seq.) from third parties, whether or not generally known by the public, (3) already within the public domain, or (4) becomes part of the public knowledge or literature no as a result of a breach of this agreement or is independently developed without reference to Confidential Information.

(Client) and Santa Fe Group agree that any Confidential Information may not be copied, transcribed, recorded, memorized or otherwise used in any manner except as may be necessary to consider entering into a business relationship and if such relationship is established to allow the development of mutually agreed upon services. (Client). and Santa Fe Group further agree that only those employees, officers, subcontractors, members (as described below) and agents with a specific need to know such information in order to perform their duties shall have access to any such information. These employees, officers, subcontractors, members and agents shall be instructed by (Client) and Santa Fe Group not to sell, assign, transfer, reveal, or otherwise use any such information for any purpose other than those set forth herein without the other's prior written consent.

Company_____	**Santa Fe Strategy Center Ltd.**
Signature_____	**Signature_____**
Name_____	**Name_____**
Title_____	**Title_____**
Date_____	**Date_____**