Central Bank of The Bahamas
Response to Bidder Questions Regarding
RFP CSRG20250101:

1. Though you have commented on scalability of the tool, you have not specified how many core users will actually require access to the application. Core users are the members of the 4 units that will require access.

   Answer: With regard to the number of core users (members of the four units that will require access), the Bank expects a range of up to 40 "core" users from the business units managing Enterprise Risk, Business Continuity, Onsite Examination, Information Security and Internal Audit areas. However, the Bank expects to require additional 80 "stakeholder" users to either update or report on relevant activity.

2. I understand that Business Licenses are applicable in The Bahamas. Is it permissible to provide the equivalent document for our country if not in The Bahamas?

   Answer: For clarity, the Bank desires a bidder that complies with the laws of the Commonwealth of The Bahamas for taxation purposes. In addition, it also requires a bidder to possess a valid business license compliant with its host country.

3. On page 8, you have indicated the information that should be on the cover page. You have stated "Bank". Can you elaborate on what is meant by this?

   Answer: The Bank desires to receive the bidder's bank instructions within the proposal. Upon award of the contract, the Bank would seek to remit the mobilization deposit as specified in section 3.15.9.

4. Projects of this nature do not usually include a Change Management element. On page 11 you have asked for us to describe change management methodology. Change Management is usually the responsibility of the entity. Are you indicating that you would like us to also incorporate Change Management as a part of the project?

Answer: All projects are subjected to change, e.g., missed requirements, additions required, etc., which the Bank manages through a project change management framework.

5. On page 13, you have referred to risk management resources to advise during the analysis, design, implementation and support phases of the project. Is there an expected Risk Management implementation element required? That is, design of a methodology for the central bank, instead of actually assisting the bank in implementing, in the tool, a risk management methodology that already exists?

   Answer: The Bank desires to establish its existing Enterprise Risk Management framework and methodologies into the solution and ensure that these frameworks and methodologies align with industry standards and best practice guidelines for enterprise risk management. Therefore, the Bank is open to discussion on enhancing existing frameworks and methodologies prior to deployment of the solution.

6. Can you elaborate on the expectation where "Project Documentation" is mentioned at section 4.1.2?

   Answer: "Project Documentation" refers to most general documentation relative to the use of the solution. The documentation includes but are not limited to (and can exist within one document):

   a. General User guide

   b. Training Manual

   c. System Rules

   d. Service Manual

7. How many Core User licenses will the organization need for your IT Compliance solution?

   Core users are people with creating and testing access. Stakeholders are just responding to tasks such as risk assessments and document requests. Stakeholder licenses are unlimited at no charge.

   Answer: The Bank expects 5 core users for Information Security purposes.

8. How many Core User licenses will the organization need for your Enterprise Risk Management solution?

   Answer: The Bank expects 4 users for Enterprise Risk Management (inclusive of Compliance, Risk management and Business Continuity) with 1 of these users having access to each of those components.

9. What does your audit lifecycle look like?

   Are you managing only IT-compliance-related audits and are they performed on a project basis?

   Answer: This differs between Internal Audit, Onsite Examination and Information Security Unit. The audit cycle for Internal Audit goes from risk assessment to annual audit plan development, execution and follow-up. The annual audit plan covers the entire audit universe inclusive of operational and compliance audits which are identified as projects. Technology audits are also included in the audit plan, the scope of which is process focused.

   Onsite Examination goes from planning to fieldwork, reporting and follow up.

   For Information Security, there are various security reviews that take place during the course of the year. The vast majority can be classified as projects. However, there are instances where observations may arise during the course of monitoring which may serve as a catalyst for a remediation task to be assigned.

10. Does your organization have a budget range in mind? We tailor our pricing to meet each organization's needs.

    Answer: The Bank conducted a benchmarking exercise within the past 3 years on a number of GRC solutions in the market. The Bank has prepared a budget based on that prior information and is willing to take appropriate steps to acquire the solution that best meets the Bank's needs based on the requirements outlined in the RFP.

11. What IT frameworks is your organization currently complying with?

    Answer: The Bank makes specific reference to ISO27001, NIST, CIS along with other proprietary frameworks.

12. Please state the preferred type of hosting infrastructure required.

    Available options are: On Prem/ Cloud (With options of hosting servers available in EMA or Canada)

    Answer: The Bank would prefer an On Prem infrastructure as priority but is open to Cloud infrastructures that can be hosted in jurisdictions with similar data sovereignty and privacy laws as that of The Bahamas.

13. For the Legacy GRC system in place, what data types have to be migrated?

    Please provide an indication of the types and volume of the data

    Answer: The Bank does not possess an existing GRC. Most data are captured via spreadsheet and word documents.

14. How many systems are to be integrated into the proposed solution? What are types of data that will require integration?

    Answer: The Bank will share this in detail with the selected bidder.

15. What is the expected number of users to be given access? User counts are generally on role-based accesses such as:

    - Users with unlimited access (Read & write access to all components of the solution)
    - Users with limited access (Read & write access to only 1 sub-component of the solution)
    - Low level users (Read Only access to all components of the solution)

    Answer: With regard to access type, all "core" users (up to 40) would require Read and Write access to their (1) component of the solution. Stakeholder users (80) would only require access suitable to update information requests as required.

16. With reference to point C-12 that states 'The solution must include the ability to create and manage business continuity plan documents.

    Please detail this process. Do you require the ability to the perform an end-to-end Business Continuity function? Alternatively, are you looking for the system to manage and store the documents?

    Answer: With regard to point C-12, the Bank seeks a solution that permits a user of a business unit to generate a business continuity plan (with subsequent approval by the appropriate supervisor) within the application for the purposes of maintenance (continuous updates), version control (approved by responsible party) and as secondary storage (in addition to dedicated internal storages that plans are stored). In the case of alternative solutions that only upload documents and store them, functionality to monitor their life expectancy (plans require periodic review) would be mandatory at minimum for consideration.

17. With reference to point C-21 that states 'The solution must include the ability to perform party risk audits for security risk assessment purposes.

Do you require the ability to the perform an end to end Third Party Risk Management function? Alternatively having a repository of third parties with the ability to have a security risk assessment questionnaire sent out to third parties?

Answer: Yes, end to end third party risk management for Information Security Management.

18. Would the Central Bank of Bahamas prefer on-premise or cloud solution?

    Answer: The Bank would prefer an On Prem infrastructure as priority but is open to Cloud infrastructures that can be hosted in jurisdictions with similar data sovereignty and privacy laws of that of The Bahamas.

19. Does the Central Bank of Bahamas currently having a GRC solution in place (to address other areas than demanded in the RfP)? If yes:

    a. what is the solution name and scope?

    b. Shall we assume to either integrate with or incorporate existing solution?

    Answer: The Bank does not have an existing GRC solution in place.

20. What solution(s) is currently Central bank using for Internal audit, business continuity management, and risk management (incl. RCSA)?

    Answer: The Internal Audit team utilizes an audit management solution that interfaces with a data analysis tool. Other operations are currently performed via manual methods.

21. Would central bank consider also combination of 2 software solutions (i.e., one covering Internal audit and second one GRC - business continuity management requirements)?

    Answer: The Bank is open to a combination of 2 software solutions that meets the requirements specified in this RFP, under the condition that:

    - they are offered by the same bidder

- the submitted proposal include both solutions as a part of their suite to meet the requirements specified in this RFP.

22. Is Central Bank of Bahamas considering integration towards 3rd party / internal banks' system or a database(s)?

    Answer: Not presently.

23. Would you consider adjusting or modifying your processes or methodology to better utilize solution benefits and native features in line with best practices delivered with out-of-the-box (OOTB) solution, or would you rather expect to customize the solution to fully reflect existing approaches?

    Answer: The Bank envisages, in most cases, to implement its existing frameworks and methodologies into the solution to reflect existing approaches. However, the Bank is open to discuss modifications with the selected bidder so that the solution meets expected requirements.

24. Is the indicative timeline in the RFP shared for overall implementation of needed modules, i.e., does Central bank expect to run implementation of modules in parallel?

    Answer: The Bank envisages the implementation of modules to be ran in parallel across multiple business units. However, this can be developed and agreed with the selected bidder as indicated in section 4.2 (Solution Delivery).

25. Is there any internal / external deadline until when the Central Bank would like to have the solution deployed in Production?

    Answer: The Bank envisages the deployment of the solution within a 16 to 20 week as stated in section 4.2 (Solution Delivery) but is open to further developing and agreeing achievable timelines with its selected bidder.

26. Are the provided numbers of users combining the needs for all needed modules?

    Answer:

27. Would any data migration activity be considered as part of the project?

    Answer: Yes. At a minimum, the population of audit deficiencies within the existing Audit Management Solution.

28. Apart from post-implementation support, shall we propose business-roll out programme in our proposal to help with end user adoption of the solution?

    Answer: The Bank sees user adoption as a part of the post-implementation process and encourages bidders to make considerations to support user adoption.

29. How many users would need to have a role allowing them to create and delegate task to other users and how many would be fulfilling the assigned tasks only?

    Answer: The Bank envisages its core users (up to 40) requiring a role to delegate tasks to other stakeholder users. Those stakeholder users fulfilling the assigned tasks are expected to be up to 80 users across both Audit and GRC solutions.

30. With respect to the potential contract, would Central Bank consider having 2 separate contracts – one with implementation & advisory partner and second one with GRC solution provider?

    Answer: The Bank only seeks the services of a GRC and AMS solution provider at this time.

31. Considering broader scope of implementation, is Central Bank having data model in place, is there methodological alignment between departments and alignment in terms and naming

conventions?

Answer: It is not expected that the Onsite Examination and Information Security Units will follow the naming conventions for Enterprise Risk and Internal Audit for their operations.

32. "The solution must include further insights based on observed trends or some aspect of data analytics to add value to generated reports." Can you please provide an example of expected output?

    Answer: Exception reports, trend analysis, variance analysis, charts and illustrations.

33. Will the Central Bank of The Bahamas consider having a discussion session to further discuss key clarifications where any with respondents prior to proposal submission?

    Answer: The Bank is open to clarifying any additional queries that remain via the same channel used for proposal inquiries (section 3.1).

34. Will the Central Bank of The Bahamas need any support on content and/or process buildouts?

    Answer: The Bank will not require any additional contracts for those services at this time.

35. I recently submitted our response to your GRC RFP and in doing so I priced it based on the number of users specified in my meetings with the Audit group last year (5 - 10). The RFP document asks for capabilities in terms of number of concurrent users to be "no less than 50" but I assumed that number is a reference to performance limits and not the actual number of users required. Can you confirm this please? If I am wrong in my assumption, can I ask you to please confirm the required number of users and further that I be allowed to correct our bid and resubmit?

    Answer: Your assumption is correct that this spoke to performance and not the actual number of users required. The actual number of required “core” users is 40, as stated in our other responses. The Bank will allow bidders to modify any bids previously submitted.

36. Can you provide detailed pain points with the current GRC and Audit Management system? What specific functionalities are missing or problematic?

    Answer: The Bank does not currently possess a GRC and existing processes are performed manually. Additionally, the Bank does not have any issues with the audit management system. Our interest was to improve our data analytics capabilities.

37. Can you provide examples of the most complex or time-consuming GRC processes today that the new system should streamline?

    Answer: Amending existing templates for risk assessments with pre-defined cells with formulas.

38. Are there any manual processes currently being used that the new system must automate?

    Answer: Yes. Risk assessment at a minimum.

39. What are the top three priorities in selecting the new solution (e.g., automation, security, integration, reporting)?

    Answer: Security, Ease of use and Automation.

40. Are there existing process flowcharts or system architecture diagrams that detail how GRC and audit management workflows function today?

    Answer: No.

41. Are there any regulatory findings or audit deficiencies that the new system must address?

    Answer: There are no current regulatory findings or audit deficiencies that is sought to be addressed by a GRC solution. The Bank mainly seeks to streamline existing processes through a solution to enhance the efficiency of the aforementioned business units.

42. Does the organization currently use a SIEM (Security Information and Event Management) system? If so, which one (Microsoft Sentinel, Splunk, QRadar, etc.), and is integration required?

    Answer: A SIEM is used and it supports industry standard protocols for event collection. The Bank does not disclose specifics about the security tools that it uses for security reasons.

43. Are there specific audit trails or logging requirements beyond what is listed in the RFP? (e.g., how long must logs be retained, and must they be immutable?)

    Answer: System and audit logs should be retained for at least (1) year.

44. What are the data residency requirements? Must data remain on-premises, within specific geographic locations, or can it be cloud-hosted (Azure, AWS)?

    Answer: The Bank would prefer an On Prem infrastructure as priority but is open to Cloud infrastructures that can be hosted in jurisdictions with similar data sovereignty and privacy laws of that of The Bahamas.

45. Are there any specific security certifications or compliance mandates the solution must adhere to beyond ISO 31000, NIST, or SOC 2?

    Answer: Yes, ISO27001, CIS and other proprietary frameworks that the Bank will share with the selected bidder.

46. What level of data segregation and access controls are required between different business units or legal entities?

    Answer: Stakeholder users should be only able to view information/data relative to their own business unit/ legal entity, granted a view privilege was authorized.

47. What legacy systems are currently in place for risk and audit management? Will historical data need to be migrated?

    Answer: The existing audit management solution will require data migration for historic audit data for Internal Audit. All other operations are manual.

48. Should the system support Single Sign-On (SSO) using an existing identity provider (Microsoft Entra ID, Okta, Duo, etc.)?

    Answer: Yes. The preference is Okta/Auth0 and/or DUO.

49. What are the key risk and control data sources (spreadsheets, databases, systems) that will need to be migrated into the new platform?

    Answer: The existing audit management solution will require data migration for historic audit data for Internal Audit. All other operations are manual (spreadsheets).

50. What key reports does the bank currently generate manually that should be automated?

    Answer: The Bank produces a number of key risk related reports (including assessments and audits) that would be automated.

51. Will the system need to export data to external analytics tools such as Power BI, Tableau, or other data warehouses?

    Answer: The Bank does not currently envision data in the GRC or AMS being exported to an external analytics tool.

52. Should the system predict compliance risk trends using AI or machine learning models?

    Answer: Yes. Compliance risk trends from the business units.

53. Should the solution automatically flag high-risk incidents based on predefined risk thresholds?

    Answer: Yes, based on the risk appetite established in the Enterprise Risk Management framework.

54. What are the most critical GRC metrics and KPIs that need to be tracked and visualized in the platform?

    Answer: The Bank desires a number of key metrics to be tracked and visualized in the platform across the risk related enterprises (not limited to Inherent and Expected Risk, breaches of risk appetite, RTO and RPO, etc.).

55. Is there a specific data warehouse or business intelligence platform that the new system must integrate with for advanced analytics?

    Answer: IBM Cognos Analytics

56. A12: Does the Central Bank currently have policy limitations on the regions that both the Primary and Disaster recovery instances are established (Where a cloud base solution is proposed)?

    Answer: The Bank prefers jurisdictions with similar data sovereignty and privacy laws of that of The Bahamas.

57. B24: Can the Central Bank share if already known, estimates or objective values for these recovery metrics?

    Answer: The Bank intends to share this information with the awarded bidder during the implementation stage.

58. F3: What would be an example of an integration at the cloud provider level that an application is expected to provide?

    Answer: Further clarification is required to respond to this question.

59. G2: Will the Central Bank require annual Disaster recovery tests be performed as part of the application service program?

    Answer: Yes, but not as one of the Bank's critical applications.

60. In addition to what has already been specified in 1.2 Background, could you elaborate on how the requirements specified in the RFP are being conducted today – are their multiple different software solutions in place, or is it currently being managed through manual methods throughout the responsible business units?

    Answer: Internal Audit has an audit management solution and a data analytics tool which are currently used. All other processes are being handled through manual methods.

61. Our software can be deployed both on premise and through a cloud-based solution. Does the bank have any preference as to the deployment method, either relating to the procurement object itself or an overarching IT-strategy?

    Answer: The Bank would prefer an On Prem infrastructure as priority but is open to Cloud infrastructures that can be hosted in jurisdictions with similar data sovereignty and privacy laws as that of The Bahamas.

62. Relating to the above question on preferred deployment method, does the Bank stipulate specific data residency requirements? Is hosting in the European Union permissible to the Bank?

    Answer: The Bank prefers jurisdictions with similar data sovereignty and privacy laws of that of The Bahamas.

63. We cannot find specific Contract Terms & Conditions included in the RFP. Is it a correct interpretation that the bidder should provide our suggested contract terms & conditions, including SLA, as per item 3.15.9 Contract Payment Details? Alternatively, will the Bank provide T&Cs for review as part of the RFP process?

    Answer: The Bank expects the bidder to provide its suggested contract terms and conditions, including SLA as outlined in the RFP document. The RFP outlines the Bank's initial terms and conditions with respect to the acquisition of GRC and AMS solutions but reserves the right to add additional terms during contract negotiations based on the text outlined in section 7.3.

64. Question A11 stipulates that the solution must be interoperable with existing multiple hardware, operating systems and database management systems. Can the bank indicate what those existing hardware, OS and database management systems are?

    Answer: Due to security reasons, detailed information will be shared with the selected bidder.

65. Question C11 stipulates that the solution must possess the ability to correlate and integrate risk relationships and to map risk interdependencies within the enterprise and visualize these relationships in reports. Could you please elaborate on the use case and are there existing examples of such reporting that you could provide to outline your expectations?

    Answer: The intent is to have the ability to assess risks identified by internal audit, external assessments and those self-identified by business units, so that the Bank can obtain a holistic view of the areas that require further action/remediation. Any report or visualization that can highlight key risks that drive changes in other risks would be useful. The use case relates to being able to understand the relationship between risks within the risk register, risk incidents, risks identified by internal or external assessors, in order to understand the key risk drivers.

66. In relation to question C13, has the Bank done a prioritization of business activities and subsequent BIA work, and if so, how many prioritized business services do you have today?

    Answer: The Bank has undertaken prior business impact assessments via manual methods to prioritize business activities across the enterprise and has determined the number of services considered "critical" for The Bank.

67. Further in relation to question C13, is resource data for the existing business impact analysis stored in a system today, and if so, are you expecting this to come through integrations, or be managed by the solution?

    Answer: The existing business impact assessment data is currently not stored in a system. The Bank is open to not importing past data to avoid conflicts due to template differences.

68. Question C22 stipulates that the solution should have the ability to conduct analysis of: the risk register; interdependent risks; transversal risks; risk incidents, etc. Could the Bank expand on what type of analysis is required?

    Answer: The Bank wishes to generate automated reports and/or dashboards that speaks to, at minimum, breaches in risk appetite, status implementation of corrective action plans, key performance indicators (KPIs/KRIs), top key risks and the adequacy of the Bank's control environment as well as risk incidents (looking at trends, control breakdowns etc.).

69. Question C26 stipulates that the solution should provide functionality to monitor internal and regulatory changes (from respective organizational bodies: federal and international) and send respective automated alerts of such changes (i.e., FATF, CATF). Do you have accounts or arrangements with these bodies today for data feeds that the solution can connect to?

Answer: The Bank does not currently have any accounts or arrangements in place for these data feeds.

70. Question C28 - do you have a learning management system in use today?

    Answer: The Bank does not currently have a learning management system in use.

71. Question D5 stipulates that the solution should be able to be configured to specific reports currently generated by the Bank. Can you give examples of these specific reports and key data points required to be extracted into the reports?

    Answer: The Bank will provide this information to the selected bidder as part of the envisaged solutions requirements workshop stage of the project.

72. Question D7 stipulates that the solution must support collaboration among staff resources, allowing for simultaneous work on documents between team members. Could you please elaborate on the use case for this requirement, as our understanding would be that audits take place in the software solution rather than in documents.

    Answer: For the Onsite Examination team specifically, the Report of Examination comprises of contributions from a number of team members, to complete the report. Existing manual methods are unable to have more than one person access the report and update with their contribution. The Bank envisages that the solution would allow these team members to submit their contributions to reduce the time required to create the report.