



Acquisition and Implementation of a Next Generation Security Incident and Event Monitoring Solution

Request for Proposal

Version 2.0
November 10, 2021

TABLE OF CONTENTS

1.	Purpose and Background	5
1.1	Purpose.....	5
1.2	Background.....	5
1.3	Types of Proposals	5
1.4	Contract Terms	5
1.5	Contract Award.....	6
2.	Schedule of Events and Definition of Terms	6
2.1	Schedule of Events.....	6
2.2	Definition of Terms.....	6
3.	Proposal Instructions, Content, and Format.....	8
3.1	Proposal Inquiries	8
3.2	Delivery of Proposal.....	8
3.3	Required Review	8
3.4	Errors and Omissions	9
3.5	Addenda	9
3.6	Amendments to Proposals	9
3.7	Right of Rejection	9
3.8	Subcontractors	10
3.9	Conflict of Interest	10
3.10	Bidders Certification	11
3.11	Non-collusion.....	11
3.12	Disclosure of Proposal Content	11
3.13	System Demonstrations.....	11
3.14	Proposal Format	12
3.15	Proposal Content	12
3.15.1	Cover Page.....	12
3.15.2	Transmittal Letter	13
3.15.3	Table of Contents	13
3.15.4	Executive Summary	13
3.15.5	Introduction, Company Background, Experience and References	14
3.15.6	Proposed Solution	14
3.15.7	Implementation Approach and Work Plan	14
3.15.8	Cost Proposal.....	15
3.15.9	Contract Payment Details.....	16

4.	Scope of Work.....	16
4.1	Solution Scope	16
4.2	Current Environment Overview	17
4.3	Solution Requirements and Specifications	17
4.3.1	Minimum Solution Specifications.....	18
4.3.2	Detailed Solution Specifications	19
4.3.3	Documentation	23
4.3.4	Acceptance Test Procedure	24
5.	Evaluation Criteria and Vendor Selection	24
5.1	Proposal Evaluation Weightings	24
5.2	Rating and Scoring	25
5.3	Planned Evaluation Steps	25
5.3.1	Initial Screening	26
5.3.2	Evaluation of Written Proposals.....	26
5.3.3	Final Evaluation	26
5.4	Proposal Evaluation	26
5.4.1	Converting Costs to Points	27
6.	Standard Proposal Information	27
6.1	Assignment	28
6.2	Disputes	28
6.3	Severability	28
6.4	Supplemental Terms and Conditions.....	28
6.5	Clarification of Offers.....	28
6.6	Discussion with Bidders	29
6.7	F.O.B. Point.....	29
6.8	Contract Negotiation	29
6.9	Failure to Negotiate.....	30
6.10	Notice of Intent to Award.....	30
7.	Standard Contract Information.....	30
7.1	Contract Approval.....	30
7.2	Proposals as Part of the Contract	30
7.3	Additional Terms and Conditions	31
7.4	Proposed Payment Procedures	31
7.5	Retainer	31
7.6	Contract Payment.....	31
7.7	Contract Personnel	31

Central Bank of The Bahamas' Acquisition and Implementation of a Next Generation Security Incident and Event Monitoring Solution Request for Proposal

7.8	Inspection and Modification	31
7.9	Termination for Default	32
7.10	Schedule Delay Penalty.....	32
7.11	Contract Changes – Unanticipated Amendments.....	32
7.12	Contract Invalidation	33
8.	Appendix A: Supplemental Information	33
9.	Appendix B: Pricing Worksheet	34

1. Purpose and Background

1.1 Purpose

The Central Bank of The Bahamas (the Bank) is requesting proposals from interested and qualified firms to supply and implement a Next Generation Security Incident and Event Management solution to aid in providing the Bank with a holistic and real-time view of its information security landscape. This Request for Proposal (RFP) states the overall scope of the initiative, current technology used, outcomes desired, as well as, desired vendor qualifications, bid criteria and evaluation process.

Any decision to award a proposing firm shall be based on the demonstrated ability to understand and deliver the services desired by the Bank. Other factors that shall contribute to the selection of a proposing firm include, but are not limited to, price, accessibility and a proven record of accomplishment in delivering the requested solution.

1.2 Background

The Bank is responsible, in its role as regulator of banks and trust companies licensed in The Bahamas, for ensuring monetary stability and ensuring a sound and stable financial system for The Bahamas.

1.3 Types of Proposals

Bidders are limited to one proposal as the prime bidder. Bidders shall be allowed to collaborate with others and may be included as subcontractors on multiple proposals. The result will be one contract between the Bank and the prime bidder. The prime bidder shall be wholly responsible for meeting the requirements of the RFP, for submission of the proposal, and for performance of the entire contract. The Bank will consider the prime bidder to be the sole point of contact with regard to all contractual matters, including payment of all charges resulting from any contracts.

1.4 Contract Terms

The terms of service requested is anticipated to commence within two to four weeks of contract agreement.

1.5 Contract Award

A contract awarded by the Bank will be based upon criteria, standards, and weighting identified in this RFP as applied to the total solution proposal. Each bidder's proposal will be considered as a whole solution, without limitation, including all hardware, software and services proposed, qualifications of the bidder as well as that of any subcontractors and cost.

2. Schedule of Events and Definition of Terms

2.1 Schedule of Events

The following table provides the Schedule of Events for this RFP through contract execution. The contract term and work schedule set out herein represents the Bank's best estimate of the schedule that will be followed. If a component of this schedule (such as the proposal submission deadline) is delayed, then the rest of the schedule will be adjusted as needed.

Table 3-1-1: Schedule of Events

EVENT	DATE	TIME (EDT)
Request for Proposal Issue Date	November 12, 2021	
Deadline for Submitting Questions	November 17, 2021	5:00 pm
Deadline for Question Responses	November 23, 2021	
Proposal Submission Deadline	November 29, 2021	5:00 pm
Vendor Demonstrations	December 6-7, 2021	
Notice of Intent to Award	On or about December 17, 2021	

2.2 Definition of Terms

This RFP uses the following terminology:

- "Bidder" refers to any recipient of this RFP who submits a Proposal. All references that would normally use the words Bidder, Offer, or Bidder and Respondent, have been changed to Bidder for consistency.
- "The Central Bank" or "CBOB" or "the Bank" refers to the Central Bank of The Bahamas and includes the related entities who are seeking the services described in this RFP, the Bank's employees, and Independent Consultants and Contractors retained by the Bank for this Project.

- “Commercially available” means the material or goods must be available from a company that provides ongoing support, maintenance, and licensing. Shareware and public domain software are not considered commercially available.
- “Contract” or “Agreement” refers to a signed agreement for consulting services between the successful Bidder and the Bank.
- “Contractor” refers to the vendor selected as the prime bidder as a result of this RFP.
- “Disaster Recovery” refers to the ability to recover from the loss of a complete system or site, whether due to natural disaster, system failure or malicious intent. Disaster recovery strategies include replication and backup/restoration.
- “Must”, “mandatory” or “required” means a requirement that must be met in substantially unaltered form, for the proposal to receive consideration.
- “Project” refers to the objective of the contract, as a whole, the sum total of all elements of the contract.
- “Proposal” refers to the submission from a bidder in response to the RFP for the design, development, implementation, licensing and software maintenance of the requested Surveillance Solution.
- “RFP” refers to this Request for Proposal.
- “NG-SIEM” refers to Next Generation Security Incident and Event Management
- “VDI” refers to Virtual Desktop Infrastructure
- “Services” refer to labor, resources and materials provided by the Contractor, as required to execute the Agreement.
- “Should” or “desirable” means a requirement having a significant degree of importance to the objectives of the Request for Proposal.
- “Solicitation” refers to the invitation by the Bank or proponents to submit formal quotations, bids, tenders, proposals or statements of qualifications in direct response to the invitation.
- “Subcontractor” refers to the party contracted with the prime bidder to deliver part of all of the solution and has no direct contractual relationship with the Bank.
- “Successful” or “winning bidder” means the successful proponent to this Request for Proposal who enters into a written contract with the Bank.
- “Supplier” refers to an individual, firm, consultant, or group awarded an agreement under a Bank solicitation invitation.
- “COTS” refers to commercial off-the-shelf”
- “SIEM-as-a-service” refers to the outsourcing of SIEM. This could include hardware, software, monitoring and incident response.

3. Proposal Instructions, Content, and Format

3.1 Proposal Inquiries

All inquiries, interpretations, or clarifications, either administrative or technical, regarding this RFP, must be requested by email no later than the date indicated in the Schedule of Events. All non-proprietary written questions will be answered in writing and conveyed to all Bidders. Oral statements concerning the meaning or intent of the contents of this RFP by any person are not considered binding. Questions regarding any aspect of this RFP should be sent electronically to:

Tenders' Committee

Central Bank of The Bahamas

Subject Line: **ISU20211004 - Acquisition and Implementation of a Next Generation Security Incident and Event Management (NG-SIEM) solution Request For Proposals**

Via E-Mail: tenders@centralbankbahamas.com

3.2 Delivery of Proposal

Electronic copies of the proposal must be received on November 29, 2021, at or before 5:00 pm EDT. Faxed, hardcopy or oral proposals will not be accepted and could result in disqualification.

A bidder's failure to submit its proposal within the submission timeline will disqualify the proposal. Late proposals or amendments will not be accepted for evaluation.

All proposals submitted in response to this RFP must consist of a single electronic version of the proposal, including all required attachments (i.e. separate electronic documents, but clearly identified), and be accompanied by a scanned and signed transmittal letter described in [Section 3.15.2: Transmittal Letter](#). The Cost Proposal ([Section 3.15.7](#)) must be submitted as a separate electronic document.

3.3 Required Review

Bidders should carefully review this solicitation for defects and questionable or objectionable material. The Bank must receive comments concerning defects and objectionable material at least five (5) days before the proposal opening. This will allow issuance of any necessary amendments. It will also help to prevent the opening of a defective solicitation and exposure of bidders' proposals upon which award could not be made. Protests based on any omission or error, or on the content of the solicitation, will be disallowed if these faults have not been brought to the attention of the Bank in writing, at least five (5) days before the time set for bid opening.

3.4 Errors and Omissions

If prior to the date fixed for submission of Proposal a Bidder discovers any ambiguity, conflict, discrepancy, omission or other error in the RFP or any of its exhibits and/or appendices, the Bidder shall immediately notify the Bank of such error in writing and request modification or clarification of the document. Modifications may be made by addenda prior to the RFP response deadline. Clarifications will be given by written notice to all active Bidders, without divulging the source of the request for it.

3.5 Addenda

The Bank may modify this RFP, any of its key action dates, or any of its attachments, prior to the date fixed for submission by issuance of a written addendum posted to its website. Addenda will be numbered consecutively as a suffix of the RFP Reference Number.

3.6 Amendments to Proposals

Amendments to or withdrawals of proposals will only be allowed if acceptable requests are received prior to the deadline that is set for receipt of proposals. No amendments or withdrawals will be accepted after the deadline, unless they are in response to the Bank's request.

3.7 Right of Rejection

Bidders must comply with all of the terms of the RFP and all applicable laws governing the Commonwealth of The Bahamas.

The Bank may reject any proposal that does not comply with all of the material and substantial terms, conditions, and performance requirements of the RFP.

The Bank may waive minor informalities that:

- do not affect responsiveness;
- are merely a matter of form or format;
- do not change the relative standing or otherwise prejudice other offers;
- do not change the meaning or scope of the RFP;
- are trivial, negligible, or immaterial in nature;
- do not reflect a material change in the work;
- do not constitute a substantial reservation against a requirement or provision.

The Bank reserves the right to refrain from making an award if it determines that to be in its best interest.

3.8 Subcontractors

Subcontractors may be used to performing work under this contract. If a bidder intends to use subcontractors, the bidder must identify the following in the proposal:

- a. Complete name of the subcontractor;
- b. Complete address of the subcontractor;
- c. Type of work the subcontractor will be performing;
- d. Percentage of work the subcontractor will be providing;
- e. A written statement signed by each proposed subcontractor, that clearly verifies that the subcontractor agrees to the terms of this RFP and is committed to rendering the services required by the contract.

N.B. The subcontractor must also comply with Section 3.10: Bidders Certification as outlined in this document.

The substitution of one subcontractor for another may be made only at the discretion and prior written approval of the Bank. If subcontractors are used, the prime bidder retains all responsibility for full delivery of all requirements of this RFP.

3.9 Conflict of Interest

Each proposal shall include a statement in the transmittal letter indicating whether or not the firm or any individuals working on the contract has a possible conflict of interest (e.g., employed by the Bank) and, if so, the nature of that conflict.

The Bank reserves the right to cancel the award if any interest disclosed from any source could either give the appearance of a conflict or cause speculation as to the integrity of the solution by the bidder. The Bank's determination regarding any questions of conflict of interest shall be final.

3.10 Bidders Certification

By signature on the proposal, bidders certify that they comply with:

- a. the laws of the Commonwealth of The Bahamas (including N.I.B. certificate, V.A.T. compliance and a valid Business License);
- b. all terms and conditions set out in this RFP;
- c. a condition that the proposal submitted was independently arrived at, without collusion, under penalty of perjury;
- d. the requirement that the offers will remain open and valid for at least 60 days.

If a bidder fails to comply with [a] through [d] of this paragraph, the Bank reserves the

right to disregard the proposal, terminate the contract, or consider the contractor in default.

3.11 Non-collusion

The bidder's signature on a proposal submitted in response to this RFP guarantees that the prices, terms and conditions, as well as services quoted have been established without collusion with other bidders and without effort to preclude the Bank from obtaining the best possible competitive proposal.

3.12 Disclosure of Proposal Content

All proposals and other material submitted become the property of the Bank and may be returned only at its option. All proposal information, including detailed price and cost information, will be held in confidence during the evaluation process and prior to the time a Notice of Intent to Award is issued.

Trade secrets and other proprietary data contained in proposals may be held confidentially, if the bidder requests it in writing that the Bank does so and if the Bank officer agrees in writing to do so. Material considered confidential by the bidder must be clearly identified and the bidder must include a brief statement that sets out the reasons for confidentiality.

3.13 System Demonstrations

The Bank reserves the right to require a bidder to make system demonstrations of their proposed solutions onsite at its main office in Nassau, The Bahamas. All costs associated with a demonstration shall be borne entirely by the bidder.

3.14 Proposal Format

Vendors must organize their proposals in the following format:

- Cover Page
- Transmittal Letter
- Table of Contents
- Executive Summary (concise overview of solution proposed)
- Introduction, Company Background, Experience and References
- General System Design, Functional Specifications, and Implementation Approach (including responses to questions in [Section 4.3 General Requirements and Specifications](#))
- Cost Proposal
- Draft contract with the proposal based on information in the RFP
- Copy of valid Tax Compliance Certificate

- Copy of current Business License
- Attachments

The bidder must provide a point by point technical response stating compliance or taking exception to any or all sections of this RFP and provide sufficient information to allow the Bank to evaluate the proposal. Any deviations or exceptions to the Bank's requirements should be noted. Incomplete proposals or proposals that do not comply with the Bank's stated requirements may be eliminated from the selection process at the Bank's discretion.

3.15 Proposal Content

Proposals **must** contain the following:

3.15.1 Cover Page

The first page of the bidder's proposal must be a cover page containing the following text:

**CENTRAL BANK OF THE BAHAMAS
INFORMATION SECURITY UNIT
RESPONSE TO RFP No. ISU20211004
Acquisition and Implementation of Next Generation NG-SIEM Solution**

The cover page must also include the bidder's name, contact person, contact telephone number, address, city, state, country, zip code, fax number, and e-mail address.

3.15.2 Transmittal Letter

The bidder must submit a signed transmittal letter with its response that includes the items below.

- a. Bidder's legal name and any other name under which the bidder does business; mailing address; street address (for courier mail services); name and title of the individual who will sign the contract; name and title of the company contact person (if different); and for each key person; direct telephone number, and e-mail address; a statement that the individual who signs the transmittal letter is authorized to commit the company;
- b. A statement that the proposal is effective for a period of **sixty (60) days**;
- c. A guarantee that prices quoted in the proposal were established without collusion with other bidders and without effort to preclude the Bank from obtaining the best possible competitive price;
- d. Acknowledgement that the bidder has read this RFP and subsequent

amendments;

- e. A statement indicating whether or not the bidder or any individual working on the contract has a possible conflict of interest;
- f. A statement identifying all subcontractors and joint venture partners.

3.15.3 Table of Contents

The bidder must provide a table of contents with corresponding page numbers related to its proposal.

3.15.4 Executive Summary

The Executive Summary, which must not exceed five (5) pages, must provide a concise overview of the bidder's proposed solution and services, but must exclude pricing information. Bidders are encouraged to highlight those factors that they believe distinguish their proposals from their competitors.

3.15.5 Introduction, Company Background, Experience and References

The bidder must provide an introduction, the background of the company and details of the organization's experience with deploying similar solutions. As the Bank will evaluate qualifications of key staff proposed by the bidder, this section should include:

- a. Proposed team organization and the designation and identification of key staff;
- b. Qualification of the candidate for project manager;
- c. Qualifications of candidates for bidder key staff roles i.e. solution design engineer, project manager and security analyst, etc.; and
- d. References: last three implementations with similar scope to this RFP.

3.15.6 Proposed Solution

The bidder must identify the proposed solution up to and including the following:

- a. Provide a brief solution overview of the various solution components, their release history, current release being proposed, and number of operational installations for the proposed software solution;
- b. Describe and illustrate the general system design and integration modelling of the proposed solution;
- c. Identify any additional features, functionality, recommended solution components or services that were not outlined in [Section 4: Scope of Work](#), but that the Bidder recommends that the Bank consider. Include a description of the features and functions of each additional proposed module;
- d. Describe the policy enforcement and compliance features of the solutions;

- e. Describe alternative service delivery models (i.e. On-premise, Cloud, Hybrid-cloud, etc.) available to the Bank and indicate how these might impact the proposed solution; and
- f. Confirm ability to conform to the requirements in [Section 4.3: Solution Requirements and Specifications](#) or clearly articulate proposed alternatives.

3.15.7 Implementation Approach and Work Plan

Bidders are required to describe their proposed implementation approach, clearly identifying each phase, the timeline proposed, roles and responsibilities to be performed by the Bidder and those to be performed by the Bank. The Bidder should clearly indicate the Bank's resource requirements needed to meet the Bidder's proposed schedule and;

- a. Describe your implementation and project management methodology and approach to ensure a successful implementation;
- b. Provide a project organization chart highlighting the key staff who will be assigned to the project. Provide names and résumés for the project manager and other key assigned resources;
- c. Provide a detailed work plan that identifies major activities, tasks, deliverables, timelines and resources. The work plan should assume that the project will kick-off within no more than 3 weeks following the approval of the contract by the Bank;
- d. Describe the roles and responsibilities of Bank staff during implementation. Include the minimal and optimal number of Bank staff members (with job category), skillset, the expected role and level of effort during each phase of the project;
- e. Describe the roles and responsibilities of the Bank staff required to maintain and update the system. Include the minimal and optimal number of Bank Staff members (with job category), the expected role and level of effort on an on-going basis;
- f. Describe your change management and risk management methodology and the activities that will be performed during the implementation;
- g. Describe your user acceptance methodology and the responsibilities of Bank staff during testing;
- h. Describe your knowledge transfer methodology and approach; and
- i. Describe how the use of any alternative service delivery models would impact the proposed implementation approach, work plan, and Bank staff level of effort.

3.15.8 Cost Proposal

As indicated in [Section 3.2: Delivery of Proposal](#), the Cost Proposal must be separated from the remainder of the RFP response documents. The Bank seeks

a clear and comprehensive understanding of all costs associated with the acquisition, implementation, ongoing maintenance and licensing of the proposed solution. In this section, Bidders must itemize all costs, inclusive of all shipping, taxes (e.g. Value Added Taxes and duties). In addition to a detailed cost breakdown, a three- year Total Cost of Ownership worksheet must be completed as part of the cost proposal. A sample of the worksheet can be found in [Section 9](#).

3.15.9 Contract Payment Details

This section should outline, among other things specific to your firm, the following terms and conditions:

- Total contract sum
- Mobilization deposit
- Stage payments
- Final payment
- Retention terms

4. Scope of Work

4.1 Solution Scope

The Bank is seeking a modern, feature rich and comprehensive Next-Generation Security Incident and Event Management (NG-SIEM) solution, capable of supporting log management across a wide range of systems and devices, including custom developed applications and providing relevant contextual detail. The solution must support flexible deployment options, should scale rapidly and significantly enhance the Bank's ability to proactively identify and auto respond to suspicious activity—which should be further aided by its ability to consume threat intelligence data from external sources. Critical to the Bank, is the solution's ability to support compliance and controls implementation as guided by the Bank's Corporate Information Security Policy and internationally recognized information security management system frameworks. The core of the solution must provide support for encryption of log data, both at rest and in-transit, integrity checking should be enforced, no single points of failure must exist and high availability should be supported.

The Bank seeks a qualified vendor with the demonstrated technical and financial capacity to deliver the solution. This should be substantiated through references and profiles highlighting relevant experience and qualifications to implement a robust information security platform that must include **Log Management, Host Forensics, User and Entity Behaviour Analytics (UEBA), Network Detection and Response (NDR), File Integrity Monitoring, Security Analytics, Big Data Analytics, Security Automation and Orchestration** engine (including, but not limited to Incident Management and Response), **Advanced Correlation** within the same platform with

no additional 3rd party solution.

The proposal must list all hardware, software, licenses and professional services required to meet the Bank's needs.

The key business requirements of the project are articulated below:

1: Compliance

- The solution must support the Bank's organizational and regulatory compliance frameworks.

2: Deployment and Licensing

- The solution should support the following deployment models;
 - Self-hosted, self-managed
 - Self-hosted, hybrid-managed
 - Cloud NG-SIEM, self-managed
 - SIEM-as-a-service (full outsource)
- The solution should provide flexible licensing options that can quickly scale and support effective cost management and budgeting.

3: Support and Training

- The solution should provide flexible support arrangements covering both standard business hours and options for 24 by7; with options for escalation.
- The solution should have a diverse set of training options applicable to administrators and analysts. Delivery formats should include web-based, instructor-led, on-demand and custom. It should also have a content rich knowledge base and active forums that are user friendly and easy to navigate.

4: SLA and Professional Services

- The solution should have defined SLA's for service desk support and professional services.
- The solution should offer professional services covering project planning & management, interface development and managed services.

5: Documentation

- The solution should provide a full range of documentation for system administrators, analyst and end-users. These should include details for technical specifications and API integration.
- The solution documentation should be available for download via the web and should be augmented with a content rich knowledge base and active customer forums.

6: Product Roadmap

- The solution should have a clear and documented roadmap for product development and lifecycle. There should be a communication strategy to ensure

customers are kept abreast of product changes.

- The solution should include a process for customer feature request.

The key technology requirements of the project are articulated below:

1: File Integrity Monitoring

- The proposed solution must provide integrated built-in File Integrity Monitoring (FIM), not through a third party software and it must be managed and monitored by same NG-SIEM platform interface.
- The proposed solution FIM capability must capture the user identity for the generated FIM events.
- The proposed solution must include support for Windows, Linux distros and OS/400.

2: User Entity and Behaviour Analytics (UEBA)

- The UEBA must be fully integrated within the proposed solution – not through any separate integrated software.
- The UEBA must support an unlimited number of users
- The pre-packaged “out of the box” use cases must be listed.
- The UEBA must be able to detect and respond to insider threats, compromised accounts and privileged account abuse.
- The UEBA must collect machine data from across the environment and complete forensic gaps with endpoint and network monitoring.

3: Security Orchestration, Automation & Response (SOAR)

- The vendor must document the SOAR ecosystem identifying all vendors that have a bi-directional integration out of the box.
- The proposed solution must offer the SOAR as an embedded function not through an integration with any third party platform.

4: Data Aggregation

- The solution must aggregate data from network, security, servers, databases, applications, and other security systems like firewalls, anti-virus and Intrusion Detection Systems (IDS).

5: Correlation

- The solution should link events and related data to construct a real security incident, threat, vulnerability or forensic finding.

6: Threat Intelligence

- The solution should combine internal data with threat intelligence data to form a more comprehensive security outlook.

7: Analytics Retention

- The solution should use statistical modelling and machine learning to identify

relationships between data sources, and anomalies when compared to historical patterns, and link them to potential security concerns.

8: Threat Hunting

- The solution should allow SOC analysts to execute queries against collected data, filter and pivot the data, to proactively uncover threats or vulnerabilities.

9: Incident Response

- The solution should provide case management, collaboration and knowledge sharing around security incidents, providing a centralized portal for SOC analysts to manage, track and coordinate the threat response.

10: SOC Automation

- The solution should integrate with other security solutions using APIs, enabling execution automated playbooks and workflows based on defined responses to security incidents.

4.2 Current Environment Overview

The Bank consists primarily of two sites, which will be in scope for this initiative and both are located on the island of New Providence. The technology footprint comprises a virtualized server farm hosting Windows and Linux servers, in addition to supporting a windows-based virtual desktop infrastructure (VDI). There are two AS/400 platforms, which host the Bank's enterprise resource management solution. The Bank supports an array of endpoint devices comprising of IP phones along with Windows, Apple and Android-based computing and mobile technology. Additionally, IoT devices include smart TV's, presentation gateways and media display control devices.

The network comprises industry leading; perimeter, distribution and access layer technology, all conforming to industry standards for communication and log collection. In addition to commercial off-the-shelf (COTS) software, the Bank also maintains custom purpose built applications that support critical business functions. The Bank also subscribes to a few cloud based services which should be factored into the solution.

4.3 Solution Requirements and Specifications

The solution being proposed must meet the requirements detailed below and the response should clearly indicate how these requirements would be satisfied.

4.3.1 NG-SIEM Functional and Technical Requirements

The Bank has established the following minimum specifications. Each bid must meet or exceed the specifications listed below in order to be considered. Bidders must clearly indicate whether the solution conforms to the defined criteria by documenting

“yes”, “no” or “partially”. If the solution does not comply, describe why. If partially compliant, provide remarks.

Functional and Technical Requirements

- The NG-SIEM solution **MUST** have a remote collection mechanism to limit the impact on the WAN bandwidth.
- **MUST** support on premise, cloud and hybrid architectures.
- The solution **MUST** support auto-discovery of assets that are being protected or monitored. Describe how your solution meets this requirement.
- The solution **MUST** be software based and capable of being deployed in virtualized environments, like VMware.
- The solution **MUST** support both agent-based and agent-less log collection. The logs must be able to be compressed to support efficient collection over low bandwidth networks.
- The solution **MUST** support log compression of both data in transit and at rest. Describe the performance and productivity impact of your solution on host nodes when collecting logs.
- The solution **MUST** track hosts over time in a dynamic IP (DHCP) environment.
- The vendor **MUST** provide a detailed implementation methodology/plan that includes, at a minimum, a workshop at the start of implementation.
- The solution **MUST** be able to collect logs in real-time and start processing as soon as possible.
- The solution **MUST** have built-in ticketing/incident workflow management and also have the capability to integrate with an external ticketing system.
- The solution **MUST** have built-in evidence locker capability to preserve forensic data and support proper chain-of-custody.
- The proposed solution **MUST** have predefined use cases out of the box.
- The solution **MUST** allow the admin to visualize the attack through a simple diagram showing the connection from the source to the destination.
- The solution being offered **MUST** include full packet capture and network forensics capabilities and session replay.
- The proposed solution **MUST** support structured AND unstructured search (Google type search).
- The solution **MUST** support incident management and response.
- The solution **MUST** support user activity monitoring.
- Solution **MUST** integrate with a LDAP or AD solution for access provisioning to the NG-SIEM system.
- The solution **MUST** support integration with other security solutions; Patch & Vulnerability Management tools, Firewalls, IPS's, Antivirus, Database Activity

Monitoring, etc.

- The solution MUST provide comprehensive reporting with built-in and customized reporting capabilities. It should contain existing and customizable templates for various roles e.g. senior executive, mid-level management and various administrator levels.
- The solution MUST support exporting and/or downloading reports in multiple file formats including pdf and csv.
- The solution MUST have the ability to categorize event/alerts into various levels such as critical, high, medium and low, etc.
- The solution MUST report on devices that are no longer actively sending logs to the NG-SIEM solution.
- The solution must support role-based access control (RBAC) for the provisioning of user accounts.
- Include a copy of your solution's SLA terms and conditions giving details of the various levels of support up to professional services, including managed services.
- Provide brief a roadmap of upcoming features for your solution.
- The solution MUST provide both technical design and administration documentation for administrator, analyst and managers.
- Provide details on the proposed solution licensing structure.
- The solution MUST not drop any events if the EPS exceeds the purchased license volume.
- Data MUST be encrypted in transit, in storage and integrity checking should be enforced by the system.
- The proposed solution MUST include storage requirements.
- The solution MUST support high availability and disaster recovery from an architectural perspective as well as during collection, indexing, and management.
- The solution MUST offer highly efficient and scalable collection of log data from ALL enterprise IP devices.
- The solution MUST allow custom parsers for custom applications.
- The solution MUST categorize log data into a human-readable format to eliminate the need-to-know vendor-specific event IDs.
- The solution MUST offer a large compression ratio, typically anything from 10:1 to allow for more retention and to minimize the cost of storage.
- The solution MUST support Information Lifecycle Management, i.e. CPF Financial Services to archive old logs out of the system into an active archive/online archive solution where they can be used for future compliance needs and free up space on the appliance/solution itself. Explain how this is achieved.
- The solution MUST be able to sort, categorize and prioritize incoming incidents. It must also be able to report on the status of incidents by notifications on SMS and

emails.

- The solution MUST provide a wide set of content-rich correlation rules that define the conditions under which an alert or notification should be automatically triggered.
- Cross-device correlation based on normalized/categorized data.
- The solution MUST be capable of gathering, documenting and preserving detailed event information, allow for the analysis of evidence and maintain a complete audit trail of the investigation process.
- The system MUST give event data additional context by combining log data with vulnerability scan and configuration management systems. Alert administrators when vulnerabilities appear on critical systems and prioritize security alerts, based upon the value of the asset being attacked and its vulnerabilities.
- The solution MUST be capable of detecting high-risk administrative actions/activities on critical assets, like out-of-policy configuration changes to high-risk assets, or unusual privilege delegation.
- The solution MUST be capable of detecting suspicious user activity.
- The solution MUST be capable of detecting unusual authentication or access control issues, like multiple failed logons, or unauthorized system accesses.
- The solution MUST be capable of detecting new high-risk vulnerabilities on critical assets, or likely attacks on vulnerable hosts.
- The solution MUST be capable of detecting unusual deviations in network behavior, or network activity that violates policy.
- The solution MUST be capable of detecting critical errors on high-priority systems that might result in a system outage.
- The solution MUST support role-based access with predefined and customizable options.
- The solution MUST support multi-factor authentication.

Implementation and Ongoing support

The successful bidder shall perform the Project Management for the entire project from commencement to final hand over for production use. This should include:

- A comprehensive Project Plan including Risk, Quality, Migration, Resource, Change and Communication Management Plan.
- The name of the Project Manager who would be the single point of contact during the complete project implementation.
- A detailed implementation plan of the solution. Plan should include the full scope of the project as mentioned above. On acceptance of such plan by the Bank, the bidder is required to carry out the implementation and testing of the solution.

- The bidder should provide a detailed project plan in terms of activity and phase timelines indicating the number of days required for executing the project with the details of deliverables and milestones.
- The bidder shall be responsible for generation and submission of necessary documents required during various phases of the project. These would include planning, installation, commissioning, rollout, acceptance testing, project diagrams, technical drawings and configuration documentation. All such documents shall be accepted after the same is approved by the Bank.
- The successful bidder shall be responsible for Design, Supply, Installation, Configuration, Testing and Commissioning of the proposed NG-SIEM solution at the production and disaster recovery facility.
- Vendor shall install, configure, integrate and test all hardware and software components proposed in response to this RFP.
- Vendor shall provide operation, troubleshooting and technical manuals for the proposed solution.
- Vendor shall perform an initial setup drill test as a partial requirement of user acceptance testing.
- Vendor shall provide hands-on training for Bank Information Security staff in the management and operation of the solution and each of its components. Vendor must include an outline of the training plan provided. Training should cover topics related to technical as well as administrative aspects of the solution to enable the Bank to operate, modify and optimize the solution.
- The proposed solution must be supported for a period of five years (three years as warranty support, plus two years of maintenance, which would be at the same service level of warranty) as per RFP and the Bank's requirement.
- The bidder must analyze, review and gather performance metrics and ensure it performs optimally.
- The Bidder shall be responsible for installing, configuring all patches, updates and upgrades required for the offered solution, such that the system(s) is at the latest revisions at the time of hand-over to the Bank.
- Three years, 24/7 support for the proposed hardware and software.

4.3.2 Documentation

The successful bidder must provide:

- System and network architecture design documents
- A brief outline of the design and the factors that were considered in the design decision
- Detailed component design and configuration details; inclusive of IP addresses and port numbers and user account details.
- Security implementation for installed infrastructure components
- Operator manual for routine system maintenance

- Draft Acceptance test plan and procedure document
- Acceptance test reports, performance test reports of the components.
- A built system documentation

4.3.3 Acceptance Test Procedure

The User Acceptance Test procedures should:

- Demonstrate all aspects of the proposed solution work as per the custom log sources.
- Demonstrate the incident management life cycle.
- Demonstrate the high availability and recovery process.
- Demonstrate the threat hunting process.
- Demonstrate system performance, which is acceptable while performing multiple routine task including, log collection, report generation and incident management.
- Demonstrate the SOAR functionality.
- Demonstrate the integration and correlation of threat intelligence feeds.

5. Evaluation Criteria and Vendor Selection

5.1 Proposal Evaluation Weightings

Proposals will be evaluated based on the following weights (100%):

- Project Understanding and Proposed Solution – 25%
- Implementation Methodology and Approach – 20%
- Solution Cost (Implementation and Annual Recurring) – 20%
- Vendor Background, Experience & References – 15%
- Solution Support and Maintenance – 10%
- Quality, Clarity, and Responsiveness of Proposal – 5%
- Results of interviews and demonstrations – 5%

The bidder with the highest combined total points will be selected.

5.2 Rating and Scoring

Proposals will be evaluated and ranked according to the outline below. The evaluation will be based on a 0 to 10 scale. The score of each criterion will be determined by multiplying the criteria weight by the rating. The sum of all scores will be the total score.

Rating	Description
10	Exceeds expectations; Proposal clearly addresses and exceeds requirements, excellent probability of success.
8	Somewhat exceeds expectations; Proposal addresses all requirements, very good probability of success.
6	Meets expectations; Proposal addresses basic requirements, good Probability of success.
4	Somewhat meets expectations; minor weakness or deficiencies, Proposal partially addresses requirements, fair probability of success.
2	Does not meet expectations or demonstrate understanding of the requirements, low probability of success.
0	Lack of response or complete misunderstanding of the requirements, no probability of success.

5.3 Planned Evaluation Steps

The Bank plans to use the following multi-tiered process:

- Initial screening; see [Section 5.3.1](#).
- Preliminary evaluation of the written proposals and reference checks.
- Final evaluation of proposals.

5.3.1 Initial Screening

The Bank will conduct an initial screening step to verify bidder compliance with submission requirements. A proposal that fails to satisfy the minimum standards shall be considered nonresponsive and disqualified from the proposal evaluation process.

5.3.2 Evaluation of Written Proposals

The Bank will establish a Proposal Evaluation Committee composed of Bank employees and inclusive of subject matter experts to evaluate proposals received in response to this RFP.

5.3.3 Final Evaluation

The Bank will conduct final evaluations as a culmination of the entire process of reviewing bidder proposals and information gathering.

5.4 Proposal Evaluation

In evaluating the proposals submitted, the Bank will apply the "Best Value" standard based upon the criteria and standards contained in this RFP and from applying the weightings listed in [Section 5.1](#) above, as well as the considerations listed below. Purchase price is not the only criteria that will be used in the evaluation process. Any award resulting from this RFP will be made to that vendor whose offer conforms to the RFP and it is determined to be the most advantageous, of "best value" to the Bank, in the sole judgment of the Bank.

1. The quality and range of services the firm proposes to provide.
2. The extent to which the goods or services meet the Bank's needs.
3. The firm's overall experience, reputation, expertise, stability and financial responsibility.
4. The vendor's past relationship with the Bank, if any.
5. The experience and qualifications of the staff that will be assigned to implement the solution and service of the Bank's account. This should be accompanied with evidence of the relevant industry certifications.
6. The ability to provide service in an expedient and efficient manner.
7. Quality and range of management and performance reports.
8. Vendor's financial terms offered to the Bank.
9. The training options available and the supported delivery formats.
10. The total, long-term cost to the Bank to acquire the vendor's goods and services.
11. The ability to demonstrate how the solution will meet the requirements outlined.
12. Service Level Agreement (Triage and Response Times)
13. Any other relevant factor that the Bank would consider in selecting a supplier.

Reference checks will be used to refine and finalize preliminary scores.

5.4.1 Converting Costs to Points

The lowest cost proposal will receive the maximum number of points allocated to cost. The point allocations for cost on the other proposals will be determined through the methodology set out below. In the generic example below, cost is weighted as 25 percent (25%) of the overall total score.

Example - Formula Used to Convert Cost to Points

[STEP 1] - List all proposal prices

- Bidder #1 - \$140,000
- Bidder #2 - \$142,750
- Bidder #3 - \$147,500

[STEP 2] - Convert cost to points using this formula.

$$\frac{[(\text{Price of Lowest Bidder}) \times (\text{Maximum Points for Cost})]}{\text{(Cost of Each Bidder Proposal)}} = \text{POINTS}$$

The RFP allotted 25% (25 points) of the total of 100 points for evaluation.

Bidder #1 receives 25 points. The reason they receive that amount is because the lowest cost proposal, in this case \$140,000, receives the maximum number of points allocated to cost, 25 points.

Bidder #2 receives 24.52 points, i.e., $\$140,000 \times 25 = 2,800,000 \div \$142,750$

Bidder #3 receives 23.73 points, i.e., $\$140,000 \times 25 = 2,800,000 \div \$147,500$

6. Standard Proposal Information

6.1 Assignment

The contractor may not transfer or assign any portion of the contract without prior written approval from the Bank.

6.2 Disputes

Any dispute arising out of this agreement will be resolved under the laws of the Commonwealth of The Bahamas. Any appeal of an administrative order or any original action to enforce any provision of this agreement or to obtain relief from or remedy, in connection with this agreement, may be brought only in the Supreme Court for the Commonwealth of The Bahamas.

6.3 Severability

If any provision of the contract or agreement is declared by a court to be illegal or in conflict with any law, the validity of the remaining terms and provisions will not be affected; and the rights and obligations of the parties will be construed and enforced as if the contract did not contain the particular provision held to be invalid.

6.4 Supplemental Terms and Conditions

Proposals must comply with [Section 3.7: Right of Rejection](#). However, if the Bank fails to identify or detect supplemental terms or conditions that conflict with those contained in this RFP or that diminishes the Bank's rights under any contract resulting from the RFP, the term(s) or condition(s) will be considered null and void.

After award of contract:

- a. If conflict arises between a supplemental term or condition included in the proposal and a term or condition of the RFP, the term or condition of the RFP will prevail.
- b. If the Bank's rights would be diminished as a result of application of a supplemental term or condition included in the proposal, the supplemental term or condition will be considered null and void.

6.5 Clarification of Offers

To determine if a proposal is reasonably susceptible for award, communications to clarify uncertainties or eliminate confusion concerning the contents of a proposal are permitted between the Bank or the Proposal Evaluation Committee and a bidder. Clarifications may not result in a material or substantive change to the proposal. The evaluation by the Bank or the Proposal Evaluation Committee may be adjusted as a result of a clarification under this section.

6.6 Discussion with Bidders

The Bank may conduct discussions with bidders for the purpose of ensuring full understanding of the requirements of the RFP and proposal. Discussions will be limited to specific sections of the RFP or proposal identified by the Bank. Discussions will only be held with bidders who have submitted a proposal deemed reasonably susceptible forward by the Bank. Discussions, if held, will be after initial evaluation of proposals by the Proposal Evaluation Committee. If modifications are made as a result of these discussions, they will be put in writing. Following discussions, the Bank may set a time for best and final proposal submissions from those bidders with whom discussions were held. Proposals may be reevaluated after receipt of best and final proposal submissions.

If a bidder does not submit a best and final proposal or a notice of withdrawal, the bidder's immediate previous proposal is considered the bidder's best and final proposal.

Any oral modification of a proposal must be made in writing by the bidder.

Bidders with a disability needing accommodations should contact the Bank prior to the date set for discussions, so that reasonable accommodations can be made.

6.7 F.O.B. Point

All goods purchased through this contract will be F.O.B. final destination. Unless specifically stated otherwise, all prices offered **must** include the delivery costs, inclusive of all taxes, shipping and duties, to the Bank's main office in Nassau, The Bahamas. The Bank will **not** be responsible for storage fees prior to installation and commissioning of the solution.

6.8 Contract Negotiation

After final evaluation, the Bank may negotiate with the bidder of the highest-ranked proposal. Negotiations, if held, shall be within the scope of the request for proposal and limited to those items, which would not have an effect on the ranking of proposals. If the highest-ranked bidder fails to provide necessary information for negotiations in a timely manner, or fails to negotiate in good faith, the Bank may terminate negotiations and negotiate with the bidder of the next highest-ranked proposal. If contract negotiations are commenced, they may be held at the Bank's main office in Nassau, The Bahamas.

If the contract negotiations take place in Nassau, The Bahamas, the bidder will be responsible for their own travel and per diem expenses.

6.9 Failure to Negotiate

If the selected bidder:

- a. fails to provide information required to begin negotiations in a timely manner.
- b. fails to negotiate in good faith.
- c. indicates they cannot perform the contract within the budgeted funds available for the project.
- d. and the Bank, after a good faith effort, simply cannot come to terms, then the Bank may terminate negotiations with the bidder initially selected and commence negotiations with the next highest-ranked bidder.

6.10 Notice of Intent to Award

After the completion of contract negotiation, the Bank will issue a written Notice of Intent to Award (NIA) to the successful bidder and send copies to all bidders. The NIA will set out the names of all bidders and identify the proposal and supplier selected for award.

7. Standard Contract Information

7.1 Contract Approval

This RFP does not by itself obligate the Bank. The Bank's obligation will commence when the Governor of the Central Bank or the Governor's designee, in accordance with internal procedures, approves the contract. Upon written notice to the Contractor, the Bank may set a different starting date for the contract. The Bank will not be responsible for any work done by the contractor, even work done in good faith, if it occurs prior to the contract start date set by the Bank.

7.2 Proposals as Part of the Contract

The RFP and the successful proposal may be incorporated into the contract agreement.

7.3 Additional Terms and Conditions

The Bank reserves the right to add terms and conditions during contract negotiations. These terms and conditions will be within the scope of the RFP and will not affect the proposal evaluations.

7.4 Proposed Payment Procedures

The Bank will make payments based on a negotiated payment schedule. Each billing must consist of an invoice and progress report. Payment will only be made after the Bank's project manager approves the progress report and invoice. The Bank will not pay in full for hardware, software or services until received by the Bank.

7.5 Retainer

A withholding (retainer) of 15 percent (15%), will be taken off every invoice amount paid to the supplier under this contract. This accumulated balance will be paid at the end of the project, as defined in the final contract.

7.6 Contract Payment

No payment will be made until the contract is approved by the Governor of the Central Bank or the Governor's designee. Under no conditions will the Bank be liable for the payment of any interest charges associated with the cost of the contract.

The Bank is not responsible for and will not pay taxes. All costs associated with the contract must be stated in Bahamian currency.

7.7 Contract Personnel

Any change of the project team members named in the proposal must be approved by the Bank's project manager two weeks in advance and in writing. Personnel changes that are not approved by the Bank may be grounds for the Bank to terminate the contract.

7.8 Inspection and Modification

The contractor is responsible for the completion of all work set out in the contract. All work is subject to inspection, evaluation, and approval by the Bank's project manager. The Bank may employ all reasonable means to ensure that the work is progressing and being performed in compliance with the contract. Should the Bank's project manager determine that corrections or modifications are necessary in order to accomplish its intent, the Bank's project manager may direct the contractor to make such changes. The contractor will not unreasonably withhold such changes.

Substantial failure of the contractor to perform the contract may cause the Bank to terminate the contract. In this event, the Bank may require the contractor to reimburse monies paid by the Bank (based on the identified portion of unacceptable work received) and may seek associated damages.

7.9 Termination for Default

If the Bank's project manager determines that the contractor has refused to perform the work or has failed to perform the work with such diligence as to ensure its timely and accurate completion, the Bank may, by providing written notice to the contractor, terminate the contractor's right to proceed with part or all of the remaining work.

7.10 Schedule Delay Penalty

The Bank will include scheduled delay penalty in this contract to assure the timely completion of all major milestones. For the purposes of this contract, the Bank and bidder will agree to a set penalty rate. If the contractor fails to complete the milestone by the scheduled date identified in the approved project plan, the Bank retains the right to assess this daily penalty for each day that each milestone is late. In the event the delays are associated with the bank's resources, the contractor will not be penalized.

7.11 Contract Changes – Unanticipated Amendments

During the course of this contract, the contractor may be required to perform additional work that is not currently included in this RFP. That work will be within the general scope of the initial contract. When additional work is required, the Bank's project manager will provide the contractor a written description of the additional work and request the contractor to submit a firm time schedule for accomplishing the additional work and a firm price for the additional work. Cost and pricing data must be provided to justify the cost of such amendments.

The contractor will not commence additional work until the Bank's project manager has secured any required Bank approvals necessary for the amendment and issued a written contract amendment, approved by the Governor of the Central Bank or the Governor's designee.

7.12 Contract Invalidation

If any provision of this contract is found to be invalid, such invalidation will not be construed to invalidate the entire contract.

8. Appendix A: Supplemental Information

The Bank seeks to implement and migrate to a Next Generation SIEM platform. To enable the Bank to evaluate such factors, the items listed below are the required minimum qualifications for judging responsiveness of a proposal to this RFP. A proposal that fails to satisfy the minimum standards detailed in this section shall be rejected without further consideration.

1. **Proposal Response** - Bidders must provide a proposal using the format described in [Section 3.14: Proposal Format](#). Proposals that do not meet the required format will be rejected.
2. **Bidder Implementation Experience** - The prime bidder must have completed a similar solution implementation within the last five (5) years. The implemented solution must be described in the proposal, including descriptions of the hardware, software and services delivered.
3. **Transmittal Letter** - The response must include a Transmittal Letter as described in [Section 3.15.2: Transmittal Letter](#).
4. **Pricing Worksheet** - A 3-Year Total Cost of Ownership pricing worksheet ([Section 9](#)) must be completed.

9. Appendix B: Pricing Worksheet

For all available deployment models, bidders must provide an itemized listing of all hardware, software and services required to meet the specifications outlined in this request for proposal. Costs must include any and all taxes (e.g. Value Added Tax), shipping and duties. Additionally, bidders must provide a 3-year cost summary using the table displayed below.

Price Description	Non-Recurring (Base)	Recurring (Annual)	3-Yr Extended Cost
Product Costs			
Hardware Cost			
Software Licensing			
Other Licensing & Per Feature Cost			
Maintenance/Support			
Implementation Services			
Project Management			
Documentation & Training			
Additional Costs <i>(Attach description)</i>			
TOTAL			

Hardware: List, describe, and record the cost of each piece of hardware that is required.

Software: List, describe, and record the licensing, implementation, maintenance, support, and training fees associated with your proposed solution.

Documentation & Training: List, describe, and record the cost of developing/delivering the required technical, administrative and end-user documentation for the proposed solution. Please also include all training fees associated with your proposed solution.

Support/Maintenance: List, describe and record the ongoing costs associated with the maintenance, support and operation of your proposed solution.

Implementation: Describe any labor, equipment, supplies, or other costs associated with installing your proposed solution.

Project Management: If there are project management fees associated with your proposed solution, list and describe them here.

Miscellaneous: List and describe any other costs associated with your proposed solution.