Privileged Access Management (PAM) Solution

Request for Proposal

Version 2.0
November 26, 2024

TABLE OF CONTENTS

m,

1. Purpose and Background

1.1 Purpose

This Request for Proposal (RFP) is issued by the Central Bank of The Bahamas (hereinafter referred to as the Bank) to qualified bidders for the supply, delivery, installation, and commissioning of a Privileged Access Management (PAM) solution. This acquisition aims to secure and control access to critical systems, data, and resources by managing and securing privileged user accounts and actions.

The overall goal of this project is to:

- Mitigate security risks associated with unauthorised access to critical systems and data.
- Enforce least privilege principles and ensure privileged users have appropriate access rights.
- Monitor, audit, and track privileged user activities for compliance and non-repudiation.
- Enhance operational efficiency by streamlining privileged access workflows.

This RFP states the initiative's overall scope, desired project outcomes, minimum vendor qualifications, bid criteria, and evaluation process.

The Bank seeks a bidder with a proven track record of delivering the services and solutions outlined herein, a demonstrated awareness of the spectrum of solutions available in the market, and the capacity to manage timelines and deliverables. Other factors that shall contribute to the selection of a bidder include but are not limited to, price, service and support, solution ease of use, and integration with other applications.

1.2 Background

The Central Bank of The Bahamas, established in 1974, has as its mission “to foster an environment of monetary stability conducive to economic development and to ensure a stable and sound financial system.” The Bank recognises that to provide “stable and sound financial systems,” it is necessary to ensure that the information technology used to support the business is secure, reliable, and efficient.

The proposed Privileged Access Management solution will encompass the following key modules and functionalities:

- Privileged Access Control:
    - Automated provisioning and de-provisioning of privileged accounts.

- Password management and rotation for privileged users.
- Session recording and monitoring for privileged sessions.

- Access Request and Approval:
  - Workflow for requesting and approving temporary privileged access.
  - Just-in-time access provisioning for specific tasks.
- Audit and Compliance:
  - Audit trail of privileged user activities and access attempts.
  - Integration with existing security information and event management (SIEM) systems.

Overall, the selected PAM solution must provide the following:

- A complete commercial off-the-shelf solution that has been successfully implemented in the last 18 months for banking, regulatory, or public agencies of comparable size.
- Alignment with the functional requirements as defined in this RFP.
- A solution that requires no modification to base code but is configurable to meet the needs of the Bank now and into the future.
- An intuitive interface and an easy learning curve to facilitate rapid adoption and minimise the need for external ongoing training services.
- A system that is stable, secure and accessible and supports business processes, service delivery and transparency.
- Vendors must have an ongoing, sustainable product and corporate strategy to avoid obsolescence.
- Easy integration with other systems.

1.3 Types of Proposals

Bidders are limited to one proposal as the prime bidder. Bidders shall be allowed to collaborate with others who 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, submitting the proposal, and performing the entire contract. The Bank will consider the prime bidder the sole point of contact regarding all contractual matters, including payment of all charges resulting from any contracts.

1.4 Contract Terms

The terms of service requested are anticipated to commence within two to four weeks of the 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 and 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 represent 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, the rest of the schedule will be adjusted as needed.

EVENT	DATE	TIME
Request for Proposal Issue Date	November 26, 2024	
Deadline for Submitting Questions	December 5, 2024	4:00 pm (EDT)
Date for Question Responses	December 10, 2024	
Proposal Submission Deadline	December 17, 2024	4:00 pm (EDT)
Shortlisted Vendor Presentations	To Be Determined	
Notice of Intent to Award	On or about December 31, 2024	

2.2 Definition of Terms

This RFP uses the following terminology:

- "Automation" refers the technique of making an apparatus, a process, or a system operate automatically.
- "Bidder" refers to any recipient of this RFP who submits a Proposal. All references that would normally use the words Firm, Vendor, Offeror, or Bidder and Respondent, have been changed to Bidder for consistency.

- “The Central Bank” 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 vendors retained by the Bank for this Project.
- “Commercially available” means the material or goods must be available from a bidder 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.
- “EOL” refers to End of Life.
- “EOVS” refers to End of Vendor Support.
- "Just-in-Time (JIT) Privilege Access" refers to on-demand access control that provides short-term enhanced access solely for the time required to complete designated activities.
- “Orchestration” refers to the automation of linked workflows.
- “On-premises” refers to IT infrastructure hosted on an organisation's premises, allowing full control over server management, security, and maintenance of networking equipment and data storage.
- “PAM” refers to a Privileged Access Management Solution.
- “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.
- "Role-Based Access Control (RBAC)" refers to an access control method that assigns access rights based on user roles within the organisation.
- “Services” refer to labour, 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.

- "SIEM" refers to a Security Information and Event Management solution.
- "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 of this Request for Proposal who enters into a written contract with the Bank.
- "Supplier" refers to an individual, bidder, consultant, or group awarded an agreement under a Bank solicitation invitation.
- "TBD" refers to To Be Determined.

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: **IT202402 Privileged Access Management (PAM) Solution Request for Proposals**
Via E-Mail: **tenders@centralbankbahamas.com**

3.2 Delivery of Proposal

Electronic copies of the proposal must be received on December 17, 2024, at or before 4:00 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 (may be 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 an 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 the 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; and
- 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 perform 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 bidder or any individual 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 National Insurance Board (NIB) certificate, Value Added Tax (VAT) 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; and
d. the requirement that the offers will remain open and valid for at least ninety (90) 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, and 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 confidential, if the bidder requests, 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, New Providence, The Bahamas. All costs associated with a demonstration shall be borne entirely by the bidder.

3.14 Proposal Format

Vendors must organise their proposals in the following format:

1. Cover Page
2. Transmittal Letter
3. Table of Contents
4. Executive Summary (concise overview of solution proposed)
5. Introduction, Bidder's Background, Experience and References
6. General System Design, Functional Specifications, and Implementation Approach (including responses to the requirements outlined in Section 4: Scope of Work, including the specifications outlined in Appendix B, and Appendix C, (including responses using Appendix D)
7. Cost Proposal
8. Draft contract with the proposal based on information in the RFP
9. Copy of valid Tax Compliance Certificate
10. Copy of current Business License
11. 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 TECHNOLOGY DEPARTMENT

RESPONSE TO RFP No. 202402 Privileged Access Management Solution Request for Proposals

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

3.15.2Transmittal 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 individual who will sign the contract; name and title of the bidder contact person (if different); and for each key person: direct telephone number, fax number, and e-mail address;
b. A statement that the individual who signs the transmittal letter is authorised to commit the bidder;
c. A statement that the proposal is effective for a period of **ninety** (**90**) **days**;
d. 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;
e. Acknowledgement that the bidder has read this RFP and subsequent amendments;
f. A statement indicating whether or not the bidder or any individual working on the contract has a possible conflict of interest;
g. A statement identifying all subcontractor and joint venture partners.

3.15.3Table of Contents

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

3.15.4Executive 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, Bidder Background, Experience and References

The bidder must provide an introduction, the background of the bidder, and details of the organisation'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 organisation and the designation and identification of key staff;
b. Qualification of the candidate for project manager;
c. Qualifications of candidates for key bidder staff roles, i.e. solution design architects, solution engineers, etc.; and
d. References: last three implementations for this proposed solution.

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, the current release being proposed, and the number of operational installations for the proposed software solution;
b. Describe and illustrate the general system design of the proposed solution;
c. Provide a narrative on how the proposed solution addresses the requirements outlined in Section 4: Scope of Work, including the specifications outlined in Appendix B and Appendix C (including detailed explanations using Appendix D). Include all requested narrative responses.
d. 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;
e. Describe the security features of the proposed solution;
f. Describe alternative service delivery models (i.e. Software-as-a-Service, Application Service Provider, Hosted, etc.) available to the Bank and indicate how these might impact the proposed solution; and
g. Confirm ability to conform to the requirements in in Section 4: Scope of Work and the related Appendices or clearly articulate proposed alternatives.

3.15.7Implementation Approach and Work Plan

Bidders are required to describe and 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 organisation chart highlighting the key staff who will be assigned to the project. Provide names and resumes for the project manager and other key assigned resources;
c. Provide a detailed work plan that identifies major activities, tasks, deliverables, and resources. The work plan should assume that the project will kick-off within no more than three (3) weeks of 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) and 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 during the first five (5) years. 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 methodology and 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 training 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.

3.15.8Cost 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 and ongoing maintenance of the proposed solution. In this section, bidders must itemise 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 Appendix A: Pricing Worksheet.

3.15.9Contract Payment Details

This section should outline, among other things specific to your firm, the following terms and conditions (for further details, see Appendix A: Pricing Worksheet):

1. Total contract sum (inclusive of all taxes and charges)
2. Mobilisation deposit
3. Stage payments
4. Final payment
5. Retention terms

4. Scope of Work

4.1 Solution Scope

This section outlines the scope of work (SoW) for implementing and deploying a Privileged Access Management (PAM) solution for the Bank. The purpose of this document is to provide potential vendors with a clear understanding of the project's requirements and expectations.

4.2 Background:

CBOB operates within a dynamic and highly regulated financial sector, where the protection of sensitive information, data integrity, and operational continuity are paramount. In recent years, the escalating threat landscape, coupled with evolving compliance standards, has presented significant challenges to our IT infrastructure. Specifically, the following issues have highlighted the critical need for a robust PAM solution:

- Escalating Cybersecurity Threats: The financial services industry faces increasingly sophisticated cyber threats, including ransomware, phishing attacks, and insider threats. Malicious threats specifically target privileged accounts due to their elevated access levels, posing a significant risk to our systems and data integrity.
- Compliance Requirements: Stringent regulations necessitate strict controls and auditing mechanisms for privileged access. Compliance failures can lead to severe financial penalties and reputational damage.
- Inadequate Access Controls: Our current access management practices lack centralised control and monitoring capabilities for privileged accounts. This gap exposes vulnerabilities, hindering our ability to promptly detect and respond to unauthorised access.

- Operational Inefficiencies: Manual or decentralised management of privileged access leads to password management, access provisioning, and monitoring inefficiencies. This not only increases the risk of security breaches but also hampers operational agility.
- Audit and Reporting Challenges: Auditing privileged access activities is critical for compliance and risk management. The absence of robust logging, reporting, and real-time monitoring mechanisms makes it challenging to meet audit requirements effectively.

Given these challenges, implementing a comprehensive PAM solution is imperative to address security vulnerabilities, ensure compliance adherence, enhance operational efficiency, and fortify our overall cybersecurity posture. A successful PAM deployment will empower CBOB to proactively manage and monitor privileged access, mitigate risks, and safeguard our critical assets against evolving threats.

The Bank solicited proposals in early 2024 for a PAM solution and received bids from several vendors. However, following an extensive review of vendor bids, the Bank was compelled to review and revisit its requirements to ensure the selection of the best solution to achieve the overarching goal of implementing a robust, mature, secure, and comprehensive privileged management solution for the institution.

The revised solution requirements are detailed in Appendix B and Appendix C for the proposed Privileged Access Management Solution. The bidder must specify whether they comply with these specifications with necessary clarifications in the remark column. The scope will broadly include:

4.2.1 Supply of Hardware and Software

A. Hardware: The bidder will provide the required hardware, if applicable, along with the operating systems and database licenses. The Bank prefers hardened virtual and physical appliances if the solution requires hardware or services on-premise.

B. Software: The bidder will supply the required licenses per the specifications below.

Specifications	Quantity
Device Count (including servers (physical and virtual), operating systems, databases, switches, firewalls, routers, etc.)	Initially 3000 Devices
Administrator count	25

Recording retention	Three (3) months readily available, nine (9) months archival, and can be changed within the application by the Bank.

4.2.2 Implementation & Integration Services

The bidder will be responsible for the installation and commissioning of the entire solution. The installation and commissioning services will include the following but not limited to:

- Installing the Privileged Access Management solution at the Bank's primary and secondary datacenters.
- Configuring high availability for the solution.
- Operationalise and optimising the PAM solution.
- Configuration of all features included in this RFP.
- Project documentation.
- Project handover inclusive of user and administrator training.
- Completion of the project end-to-end.
- Stepwise documentation for all administrative activity.
- Post-implementation support for 60 days.

4.3 Solution Delivery

The Bank seeks to implement the proposal PAM solution in phases with an overall completion within eight (8) to ten (10) weeks from the firm order date. To accomplish this, the Bank envisages the following initial milestones that will be further developed and agreed with the selected vendor.

Number	Milestones	Week
1	Detailed Project Plan	1
2	Solution Requirements Specification and Detailed Design	2
3	Test Environment/Proof Of Concept Deployment	3
4	User Acceptance Testing, Security Review	4
5	Production Implementation	5-7
6	Training	8
7	Project completion sign-off	8

5. Evaluation Criteria and Vendor Selection

5.1 Proposal Evaluation Weightings

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

- Technical Proposal – 70%
- Financial Proposal – 25%
- Solution presentation and demonstration – 5%

The Technical Proposal will be evaluated based of the following attributes.

Attribute	Weight
Adherence to RFP submission requirements.	5
Solution design and compliance with the technical, functional and non-functional requirements of the delivered solution.	25
Relevant knowledge, experience and qualification of firm and team members including established record of success in similar projects.	20
Vendor and Solution References.	15
Implementation Methodology and Approach	15
Timeline for recommended solution to be implemented	5
Training, documentation, service, support, product warranty and maintenance	15

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.

Bidders must meet all the mandatory minimum requirements in this section by providing a written, affirmative response to each of the criteria stated below.

a. By submitting a response, the prime bidder accepts the terms of this request for proposal.
b. The proposed solution must currently be in production.
c. The prime bidder must be an authorised solution provider for the proposal solution.
d. The prime bidder must fully support the proposed solution throughout the life of the contract, including but not limited to: bug fixes, replacement parts, support, etc.
e. The bidder, and their subcontractors, must agree to protect the privacy and security of the Bank's data at all times and further agrees not to use or disclose such data other than to accomplish the objectives of the project.
f. The prime bidder has a minimum of three (3) years of experience providing PAM solutions in the banking, finance or regulatory sector for similarly scaled institutions.
g. The prime bidder will ensure that adequate and expert staffing is assigned for the duration of the project.

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 Bank.

1. The quality and range of services the bidder proposes to provide.
2. The extent to which the goods or services meet the Bank's needs.
3. The bidder's overall experience, reputation, expertise, stability and financial responsibility.
4. The bidder'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 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), if applicable.
13. Any other relevant factor that the Bank would consider in selecting a supplier.

Reference checks will be used to refine and finalise

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.

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

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 X 25 = 2,800,000 ÷ $142,750

Bidder #3 receives 23.73 points, i.e., $140,000 X 25 = 2,800,000 ÷ $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 for award 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 accommodation should contact the Bank prior to the date set for discussions so that reasonable accommodation 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 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. The agreed payment terms will be final and no amendments to the payment terms are permissible.

Each billing must consist of an invoice and progress report. The bidder must include all costs including travel and living expenses incurred during the project life cycle as a part of the Bill of Materials and the Bank will not bear any additional costs on these.

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

In the event of a delay in delivering the proposed solution beyond the agreed-upon timeline without justifiable cause, a penalty of one percent (1%) per week of delay or part thereof, subject to a maximum of five percent (5%) of the contract value shall be

deducted from the final contract payment after the successful installation and commissioning of the solution.

The vendor must promptly notify the Bank in writing of any foreseen delays, providing a detailed explanation and revised delivery schedule. Failure to notify in advance may impact penalty calculations.

Extensions to the delivery schedule may be considered under exceptional circumstances, such as force majeure events, provided that the vendor provides documented evidence supporting the delay.

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 time schedule for accomplishing the additional work and a 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: Pricing Worksheet

For all available deployment models, bidders must provide an itemised 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			
Another Licensing & Per Feature Cost			
Maintenance/Support			
Implementation Services			
Project Management			
Documentation & Training			
Additional Costs *(Attach description)*			
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.

9. Appendix B: Non-Functional Requirements

The proposed Privileged Access Management solution should meet or exceed the following non-functional requirements. Bidders must indicate in their proposal narrative how this is accomplished.

- Performance:
  - The solution should handle at least 20 concurrent privileged sessions with minimal latency.
- Scalability:
  - The solution should scale with the organisation's growth, supporting at least 3000 privileged accounts.
- Availability:
  - The solution should have a minimum uptime of 99.9% per annum.
- Security:
  - Compliance with industry-standard encryption protocols.
  - Strong access controls and encryption for sensitive data.
- Usability:
  - Intuitive user interface for administrators and end-users
  - Comprehensive documentation and training resources

10. Appendix C: Solution Functional and Technical Requirements and Specifications

10.1 Functional Requirements

The proposed Privileged Access Management solution should include, but not be limited to, the following functionalities:

- User Authentication and Authorisation:
  a. Centralised user authentication and authorisation mechanism.
  b. Role-based access control (RBAC) for defining user privileges.
  c. Privilege escalation and de-escalation mechanisms for access.
  d. User authentication against corporate directories (e.g., Active Directory) inclusive of multifactor authentication.
- Credential Management:
  a. Secure storage and management of privileged account credentials.
  b. Rotation and expiration of credentials.
  c. Integration with enterprise password management tools.
  d. Automatic password generation and retrieval
- Session Monitoring and Recording:
  a. Real-time monitoring of privileged sessions.
  b. Ability to record and audit privileged user activities.
  c. Alerts for suspicious or unauthorised access attempts
  d. Session recording and monitoring with real-time alerts for sensitive actions and high-risk commands.
  e. Ability to pause, lock, and terminate sessions in real-time for security purposes.
  f. Metadata tagging for easy retrieval of session recordings and logs for compliance audits.
  g. Secure access gateway for privileged sessions to prevent exposure of internal resources.
- Administration and Management:
  a. Centralised management console for configuration and administration
  b. User-friendly interface for policy management and access control
  c. Workflow for requesting and approving privileged access.
  d. Multi-level approval processes.

e. Support for regular security patches, updates, and version upgrades without major disruptions.
f. 24/7 technical support options for troubleshooting and urgent issue resolution.
g. Detailed Service Level Agreement (SLA) covering response times, issue escalation, and problem resolution.

- Audit and Reporting:
  a. Logging of privileged access activities
  b. Comprehensive reporting functionalities for compliance audits
  c. Customisable reports on access and usage patterns
- Policy Enforcement:
  a. Enforce policies for password complexity, session timeouts, etc.
  b. Ability to customise policies based on organisational requirements.
- Session Termination and Lockout:
  a. Automated session termination after defined idle time.
  b. Lockout mechanism for repeated unsuccessful login attempts.
- Integration Capabilities:
  a. Seamless integration with existing IAM systems, Active Directory, LDAP, etc.
  b. Seamless integration with various operating systems (Windows, Linux, etc.)
  c. Compatibility with cloud services and on-premises systems
  d. API support for custom integrations.
- Just-in-Time (JIT) Privilege Access
  a. Provisioning of temporary privileged access for specific tasks with defined start and end times.
  b. Support for one-time access for certain tasks without requiring ongoing privileged access.
  c. Ability to revoke access once the task is completed, with optional extension requests if needed.
- Automated Access Request Workflow
  a. Self-service portal for privileged access requests with customisable forms and fields.
  b. Automated workflow and notifications for requesting, approving, and revoking privileged access.
  c. Configurable multi-level approval workflows based on user roles, risk levels, or specific request criteria.

10.2 Detailed Technical Specifications

In addition to the minimum specifications listed above, the proposed solution must meet the following specific requirements. The following answer key should be used when responding to the specifications:

Y = Fully meets specification, "out-of-the box"
A = Available in the next version (include estimated date of release)
T = Specification is provided through third-party software
M = Modifications necessary to meet specification
W= Specification is not provided, but there is a reasonable work-around
C = Customisation/change of source code required to meet specification
N = Specification is not, and cannot, be provided

If any symbol other than "Y" or "A" is the response for a specification, the bidder must complete Appendix D: Bidder Comments to Technical Specifications Sheet. Any specification that is answered with a symbol other than what is listed above will be treated as a negative/non-response.

No.		Requirements	Response Code	Comments
System-wide Technical Specifications				
A	1	All modules utilise a graphical user interface, preferably via a standard browser. Please indicate the browsers supported by the proposed solution or exceptions.		
A	3	System allows a single user to be in multiple modules at the same time without running multiple sessions of the application.		
A	5	System uses drop-down menu lists or other look-up features, such as type ahead, to ensure the entry of data is consistent, and to provide validation during data entry.		

No.		Requirements	Response Code	Comments
A	7	All fields allow users to type information directly into the field. Look-up screens are optional.		
A	8	The solution is inherently (does not require a third- party interface) ODBC compliant providing the ability to access data without third-party products such as Microsoft Excel, Microsoft Access, etc.		
A	9	The solution is capable of running on Windows or Linux servers in a virtualised environment. Describe any other operating environment your proposed software will work with. In the event your software does not run on Microsoft or Linux products, explain what operating systems it does run on.		
A	10	The solution should have the capability to support high transaction volumes and simultaneous privileged sessions. Please indicate the supported simultaneous sessions for the solution proposed.		
Platform Support				
B	1	The solution must support multiple operating systems such as Windows Server 2019 and above, Linux, Unix, VMware ESX, and MacOS. Please specify and include whether support is offered via agent or agentless deployment.		
B	2	The solution must support databases such as Oracle, Microsoft SQL, IBM DB2, MySQL, etc. along with graphical interface for database installation, configuration and for db-client applications such as toad, sql developers, sql navigators, etc. Please specify.		

No.		Requirements	Response Code	Comments
B	3	The solution must support leading network, storage and security platforms such as Cisco, Palo Alto, Fortinet, DELL, IBM, Juniper, Symantec, Rapid7, DarkTrace, RSA, etc. Please specify.		
B	4	The solution should support core banking systems such as SWIFT. Vendors must provide a list of applications natively supported by the proposed solution in this table.		
Configuration				
C	1	The solution must include central access control configuration of groups/users for accessing the servers/databases through a single console.		
C	2	The solution must feature role-based access to privileged user accounts. Explain how role-based access is achieved.		
C	3	The solution must feature role-based access to devices. Explain how role-based access is achieved.		
C	4	The solution must feature secure access to users to all devices through a single console.		
C	5	The solution should support following authentication methods like identifier, LDAP, Active Directory, Radius, TACAS+, Kerberos, X509, OTP, Web SSO, SAML, etc. List all authentication methods available in the solution.		
C	6	The solution must support Unix or Windows operating systems, network devices, databases, mainframes, virtual infrastructures, or SU/SUDO injection.		

No.		Requirements	Response Code	Comments
C	7	The solution must have an open architecture to enable integration third-party vaults. Please list and explain the integration capabilities with third-party vaults.		
C	8	The solution must have bi-directional SIEM integration for advanced reporting and real-time processing of malicious behavior detection. List the supporting SIEM solutions that work well with the proposed solution.		
C	9	The solution must bulk onboarding feature for users, servers, domains, restrictions, groups etc. Explain how bulk onboarding can be achieved.		
C	10	The solution should not use any vendor provided thick client/agent application; it should work seamless with all major browser & native applications. Please indicate exceptions.		
C	11	The solution must support direct access to resources using native clients (PuTTY, WinSCP, MSTC, OpenSSH, etc.) with connection rules embedded directly into the PAM.		
C	12	The solution should have the capability to create connectors on the fly to meet needs to technology products at the client end.		
C	13	The solution should support delegation to third party systems for user authentication and identification (SAML2).		
C	14	The solution should must easy provisioning and synchronisation with central identity access management solutions within the REST API. Please specify.		

No.		Requirements	Response Code	Comments
C	15	The solution must support access to consoles, business web applications, and fat clients.		
C	16	The solution must support following protocols for integration like HTTP/HTTPS, RDP/TSE, SSH, Internet, SFTP, etc.		
C	17	On-premises, cloud-based, or hybrid deployment options should be available. Describe the various deployment models available for the proposed solution.		
C	18	The policy engine for setting and enforcing specific access restrictions should be based on user roles, device types, IP addresses, and time of access.		
C	19	The system should include customisable lockout policies to protect against brute-force attacks on privileged accounts.		
C	20	The solution should provide a secure sandbox environment for testing and validating automation scripts before deployment into production.		
Integration				
D	1	The solution must feature the ability to access the password safe via script/API to eliminate the need for hardcoded passwords in applications.		
D	2	The solution must allow integration with secure, responsive remote access tools (VNC, Remote Desktop, etc.) for control, support, monitoring, automation, or management.		
D	3	The solution should include threat analytics for PAM to detect breach attempts, user can be forced to re-authenticate and		

No.		Requirements	Response Code	Comments
		session recording can be automatically initiated or other configurable actions. Please specify.		
D	4	The solution should feature the ability to integrate with enterprise backup systems. Please detailed the backup and recovery options included in the proposed solution and list the natively supported backup and recovery solutions.		
D	5	The solution should have the capability to integrate or accessible by systems monitoring tools (e.g. SNMP, IP, agents, agentless, etc.) for monitoring system availability. Provide details in the solution narrative.		
D	6	The solution should be able to integrate with the ticketing tool for change and incident management for administrator notifications and access documentation. Provide options for this proposed integration, e.g. web hooks, APIs, etc.		
Single Sign-On (SSO) and Multifactor Authentication				
E	1	The solution must support multifactor authentication, SSO and achieve interoperability with different identity stores and solutions such as OKTA, DUO, etc. for users.		
E	2	The solution shall have support for multifactor authentication requirements during login, password retrieval, and sensitive command execution.		
E	3	The solution must allow single sign-on for servers, databases, routers, switches, firewalls, storage, thin clients, thick clients without any agent support for privileged/hidden accounts:		

No.		Requirements	Response Code	Comments
		• Windows Servers • ESXi Hosts • Linux/Unix/AIX servers • Databases accessed via command line • Databases accessed via tools like Toad, SQL Studio, etc. • Routers & Switches • Firewalls • Browser consoles • Thin and thick clients.		
Password Management				
F	1	Passwords stored in the password vault must be encrypted with a minimum of 256-bit AES encryption. Explain the various encryption standards and capabilities in the proposed solution.		
F	2	The solution must support credential management for privileged, shared, generic, application and service accounts. Explain how this is achieved.		
F	3	The solution must support password checkout with configurable timeouts and automatic password randomisation and reset after use.		
F	4	The solution must facilitate use of privilege account password by connecting directly through a requested resource without the user directly viewing or using the password.		

No.		Requirements	Response Code	Comments
F	5	The solution must support password obfuscation so that no user knows the password or a privilege, service, application, shared or generic account. Please detail how this is achieved.		
F	6	The solution must utilise policy-based credential management.		
F	7	The solution must include One-time password (OTP) functionality for temporary privileged access.		
F	8	The solution must utilise secure methods for password access, including time-based, approval-based, and just-in-time access.		
Security				
G	1	The system's security should allow read-only access to specific modules.		
G	2	The system's security should allow lock-out of specific menu items (no access).		
G	3	The solution must support configurable session and multifactor authentication time-out and logout inactivity.		
G	4	The solution must support time-restricted access to devices and privileged users. Access to a user or target device and/or group is limited to only a certain duration of time. Provide details.		
G	5	The solution must support maker checker approval and access rights configuration.		
G	6	The solution must be compatible with certificate and Kerberos-based authentication.		

No.		Requirements	Response Code	Comments
G	7	The solution must support fine-grained access control for sensitive account users predate password vaults. Provide a detailed response on how this is accomplished.		
G	8	The solution must support command restrictions and strong (MFA) authentication for highly sensitive commands. Provide a detailed response on how this is accomplished.		
G	9	The solution must allow for integration with Windows UAC and Linux/Unix SUDO for inline privilege escalation.		
G	10	The solution must manage privilege user control over files, folders, processes, registries, etc.		
G	11	The solution should support privilege account discovery and reporting for Active Directory and other directory sources. Provide a detailed response on how this is accomplished.		
G	12	The solution should support auto discovery of new assets and auto on boarding of assets and ID's. Provide a detailed response on how this is accomplished.		
G	13	User must be able to access only the domain/group which is assigned.		
G	14	The solution should prompt users to provide the reason for accessing a system, if configured.		
G	15	The solution must be hardened and privileged access should not be allowed. This should include the operating system, vault and database. Provide a detailed response on how this is accomplished.		

No.		Requirements	Response Code	Comments
G	16	The solution's database should be secure and encrypted. Provide a detailed response on how this is accomplished.		
G	17	The solution should comply with industry standards and regulations, where applicable. List the supported standards and regulations for the proposed solution.		
G	18	The solution should support end-to-end encryption for data at rest and in transit, with support for industry-standard protocols (e.g., AES-256).		
Auditing and alerting				
H	1	The solution must include detailed activity auditing for privileged accounts, including service and shared accounts.		
H	2	The solution should include the ability to log and provide an alert and audit of commands executed.		
H	3	The solution should include the ability to record clicks and keystrokes associated with a privileged account.		
H	4	The solution should include the ability to monitor and record live sessions in real time for privileged accounts.		
H	5	The solution should include the ability to capture network traffic associated with particular activities or commands.		
H	6	The solution should include the ability to perform sequential screen capture and full video recording.		
H	7	The solution should feature options to alert real-time of critical events.		
H	8	The solution must alert on access to sensitive devices.		

No.		Requirements	Response Code	Comments
H	9	The solution must alert on access to sensitive commands.		
H	10	The solution must alert on maker checker approvals.		
H	11	The solution must alert on change passwords.		
H	12	The solution must alert on open passwords.		
H	13	The solution must alert on critical settings change.		
H	14	The solution should alerts on multifactor authentication settings change.		
H	15	The solution must support pre-built compliance reports to meet regulatory requirements (e.g., GDPR, HIPAA, PCI-DSS, SOX). Please provide sample reports.		
H	16	The solution must support customisable reporting templates for internal audits and security assessments. Provide a detailed response on how this is accomplished.		
Scalability				
I	1	The solution must feature the ability to add more devices and users to be managed with 100% scalability to the existing requirement. Define in detail the scalability features of the solution.		
Redundancy and High-Availability				
J	1	The solution should have redundancy to failover in case the primary solution goes down. The solution should allow for clustering and failover mechanisms to ensure continuous availability (99.99%) of the PAM solution. Describe how the availability desired can be achieved.		

No.		Requirements	Response Code	Comments
J	2	The solution configurations must be recoverable in case of disaster. Provide a detailed explanation how this requirement will be achieved.		
J	3	The vendor shall provide data backup and recovery procedures for disaster preparedness.		
Reports				
K	1	The solution should provide standard reports out of the box. Please list and demonstrate the standard reports included in the solution.		
K	2	The solution must allow the Bank's administrators the ability to create custom reports. Define how custom reporting can be achieved within the proposed solution.		
K	3	The solution should allow reports to be distributed, via email, on a schedule.		
K	4	The solution should feature role-based reporting.		
K	5	The solution should be able to provide the report of passwords which are sealed and open and provide a risk dashboard.		
K	6	Reporting of the password not in sync should be available. Any retrieve of passwords from the vault should be alerted.		
K	7	The solution should support reporting of account login time, password history, and password policy compliance.		
User and Administrator Training				
L	1	In-person installation and administration training must be included in the solution delivery. The vendor must provide		

No.		Requirements	Response Code	Comments
		adequate and appropriate training to at least six to eight (6-8) Bank personnel using certified training material and delivered by a certified trainer for an efficient operation of the system. The trainer should have at least two years of experience and have delivered training on the specific domain on which training is being delivered.		
L	2	A detailed training plan with specifications for training courses, schedules, site and requirements must be defined and delivered.		
Deliverables				
M	1	A detailed design of architecture of the solution must be provided, inclusive of data and network flows.		
M	2	Detailed configurations of the implementation must be provided.		
M	3	Day to Day operation of maintenance manual must be provided.		
M	4	End-user manuals must be provided.		
M	5	Backup and recovery procedures to ensure recoverability in the event of data loss or corruption.		
Warranty				
N	1	Warranty and annual maintenance contracts should include repair or replacement of faulty parts. The quoted hardware, if applicable, should have enough CPU, memory and other resources from to run the proposed solution for at least three (3) years. The quoted hardware must include a warranty of three (3) years and AMC should be eligible for another two (2) years.		

10.3 Hardware and Networking Requirements

10.3.1 Architecture

Provide an introductory narrative of how the proposed system meets the overall objectives and functional requirements. It should cover the main features and benefits that distinguish your system. Your response should include a solution diagram, inclusive of network a data flows, which depicts the overall design as well as hardware specifications if proposing an on premise solution.

10.3.2 Operating System and Related Software

All proposals must provide the name and version number of the proposed operating system. In addition to the operating system, the following software packages, complete with any necessary licenses, must be specified with this proposal. The bidder must state the application that is being used for each of the following:

- Desktop and server application update solution.
- Industry Standard Relational Data Base Management System.
- System and application Backup and High Availability.

10.3.3 Backup and Failover Solution

Bidders must specify the type backup and solution redundancy that it can provide. If the Bank hosts the systems, the Bank will provide the backup solution as part of its standardised backup strategy. The bidder is to specify if it has a cloud-based backup solution.

10.3.4 Capacity

Bidders must specify optimal server and storage capacity for the proposed solution, if offering an on premise solution. Performance must be able to scale the meet the Bank's anticipated growth of 5% annually for at least 5 years. Identify exceptions.

10.3.5 Upgrades and Expansion

The proposed system must operate at no more than 35% of capacity (for CPU, memory, and I/O performance). It must have the capability to have a field upgrade to projected capacity without changing the initial CPU / disk equipment or other peripherals. The server hardware

must support five (5) years of transactions based upon five percent (5%) per year increase to present transaction volumes. Bidders must describe the expandability of their proposed solution in terms of processors, memory, I/O, disk drives, and peripheral devices for both the on premise and SaaS solution.

10.3.6 Server Functionality

The Bank will be responsible to provisioning all hardware based on the bidder's recommendation. Bidders must outline the required server sizing and specifications to support the application performance.

11. Appendix D: Bidder Comments To Technical Specifications

Item Number	Comment