PEOPLES OWN SAVINGS BANK OF ZIMBABWE (POSB)

BIDDING DOCUMENT FOR THE SUPPLY AND DELIVERY OF A CYBERSECURITY AWARENESS PLATFORM - PROCUREMENT REFERENCE: POSB2026/120

PEOPLE'S OWN SAVINGS BANK (POSB)

DATE OF ISSUE: 17 JULY 2026

CLOSING DATE: 14 AUGUST 2026

CLOSING TIME: 1100 HOURS (CAT)

PART 1: BIDDING PROCEDURES

BACKGROUND

The People's Own Savings Bank of Zimbabwe (POSB) intends to procure a Cybersecurity Training and Awareness Platform. Accordingly, the bank extends its invitation to reputable and relevant Suppliers to participate in this tendering process.

Procurement Reference – Competitive Tender Number: POSB2026/120

You are requested to bid for the supply and delivery of a Cybersecurity Training and Awareness Platform as specified in the Statement of Requirements provided in this document by completing and returning the following documents and information: -

Preparation of Technical Proposals: -

Bidders are advised to attach the following Mandatory documents:

a) Fully signed Bid Submission sheet in this Part.
b) NSSA Clearance Certificate for the current period for local bidders
c) A signed bid securing Declaration form hereunder
d) Copy of the Certificate of Incorporation
g) Copy of the CR6 formerly CR14 Form,
h) Copy of the VAT registration certificate,
i) Valid ITF 263 Tax Clearance Certificate
j) Three reference letters on company letterheads from different clients where a similar platform was supplied.
k) Manufacturer Authorization letter/Reseller/Dealership Certificate where the bidder is not the proprietary owner of the software/platform.
l) Company Profile
m) **Proposed Implementation Methodology, Workplan and Delivery Schedule**
(State the methodology and work plan you would propose to complete the required services, the associated resources and the schedule for commencement and completion).

You are advised to carefully read the complete Bidding Document before preparing your Bid. The standard forms in this document may be retyped for completion but the Bidder is responsible for their accurate reproduction. All pages of the Bid must be clearly marked with the Procurement Reference Number above.

Lots and Packages

This requirement is not divided into lots.

Number of bids allowed.

No Bidder may submit more than one Bid on the same lot, either individually or as a joint venture partner in another bid, except as a subcontractor. Where the requirements are divided into lots and packages, only one bid can be submitted for each lot. A conflict of interest will be deemed to arise if bids are received from more than one Bidder owned, directly or indirectly, by the same person.

Clarification

Clarification of the bidding document may be requested in writing by any Bidder up to 3 August 2026, 1100 hours Central African Time (CAT) and should be sent to procurement@posb.co.zw to the attention of Godfrey Marecha or Gibson Sibanda

Participation

Participation in this bidding procedure is open to **International and Domestic bidders.**

Validity of Bids

The minimum period that the Bidder's bid must remain valid is 90 days from the deadline for the submission of bids. **The bid validity must be clearly stated. Bids that do not clearly indicate the bid validity will be disqualified.**

Submission of Bids

The technical and financial proposals should be provided as one set of tender documents.

Bids must be submitted electronically through email address: tenders@posb.co.zw

Late bids will be rejected. POSB reserves the right to extend the bid submission deadline but will notify all potential bidders through email.

Date of deadline:	**14 August 2026**	**Deadline Time: 1100 Hrs (CAT)**
Means of submission:	**Electronically through email: tenders@posb.co.zw**	

The bidding submission documents should be scanned as a single document.

Bid opening.

No bidders or their representatives may witness the opening of bids, which will take place online immediately following the deadline.

Withdrawal, amendment, or modification of Bids

A bidder may withdraw, substitute, or modify its Bid after it has been submitted by sending a written notice, duly signed by an authorized representative. However, no Bid may be withdrawn, substituted, or modified in the interval between the deadline for submission of Bids and the expiration of the period of Bid validity specified by the Bidder or any extension of that period.

Bid Prices and Discounts

The prices and discounts quoted by the Bidder in the Bid Submission Form and in the Price Schedules must conform to the requirements specified below.

Prices must be quoted as specified in the Price Schedule included in the Statement of Requirements.

Bid Security

This tender does not require payment for bid security.

Bid Securing Declaration

Bidders are advised to complete and sign the bid securing declaration. Any bid not accompanied by a Bid Securing Declaration, will be rejected by the Procuring Entity as non-responsive.

The Bid- Securing Declaration of a Joint Venture (JV) must be in the name of the JV that submits the Bid. If the JV has not been legally constituted at the time of bidding, the Bid-Securing Declaration must be in the names of all intended partners

Evaluation of Bids

Bids will be evaluated using the following methodology:

1. Preliminary examination to confirm that all documents required have been provided, to confirm the eligibility of bidders in terms of this document and to confirm that the Bid is administratively compliant.
2. Technical evaluation to determine substantial responsiveness to the specifications in the Statement of Requirements. (A demonstration of the platform may be requested to ensure that all the requirements and specifications are adequately satisfied).
3. Financial evaluation and comparison to determine the evaluated price of bids and to determine the lowest evaluated compliant bid.

Evaluation criteria

Bids will be examined to confirm that all terms, conditions, and requirements of the bidding document have been complied with by the bidder. The assessment of responsiveness shall be determined in accordance with the criteria set out in the preparation of bids section of this tender document. The awarding of this tender shall use the least cost selection method among all compliant bidders.

Eligibility and Qualification Criteria

Bidders are required to meet the criteria set out in the Preparation of Bids section of this tender document to be able to participate and to be qualified for the proposed contract. Bidders must therefore provide any available documentation and certify their eligibility in the Bid Submission Sheet.

To be eligible, Bidders must: -

1. have the legal capacity to enter a contract.
2. not be insolvent, in receivership, bankrupt or being wound up, not have had business activities suspended and not be the subject of legal proceedings for any of these circumstances.
3. have fulfilled their obligations to pay taxes and social security contributions in Zimbabwe.
4. not have a conflict of interest in relation to this procurement requirement.

Bid Currency:

Bids should be priced in United States Dollars (US$)

Payment Currency:

Payment will be processed in USD Nostro.

Award of Contract

The lowest evaluated bid, which is substantially responsive to the requirements of this bidding document will be recommended for award of contract. The proposed award of contract will be by issue of a Notification of Contract Award which will be effective until signature of the contract documents. Unsuccessful bidders will be advised of the successful bidder/s and details of the proposed prices by the successful bidder/s.

Right to Reject

POSB reserves the right to accept or reject any bid or to cancel the procurement process and reject all bids at any time prior to contract award.

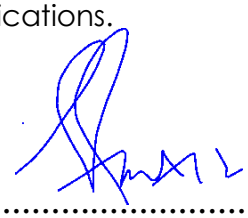
Corrupt Practices

The People's Own Savings Bank requires that bidders and contractors, observe the highest standard of ethics during the procurement and execution of contracts. In pursuit of this policy: -

1. POSB will reject a recommendation for award if it determines that the bidder recommended for award has, directly or through an agent, engaged in corrupt, fraudulent, collusive, or coercive practices in competing for the contract or been declared ineligible to be awarded a procurement contract.
2. POSB may impose sanctions on fraudulent or collusive bidders in terms of its procurement policy.
3. Any conflict of interest on the part of the bidder must be declared.

Declaration by the Accounting Officer

I declare that the procurement is based on neutral and fair technical requirements and bidder qualifications.



Signed …… Date……

G. Changunda

CHIEF EXECUTIVE OFFICER Signed on 21 Jul 2026, 12:42 PM CAT

Bid Submission Sheet

{Note to Bidders: Complete this form with all the requested details and submit it as the first page of your Bid. Attach the completed Statement of Requirements and any other documents requested in Part 1. Ensure that your Bid is authorised in the signature block below. A signature and authorisation on this form will confirm that the terms and conditions of this Bid prevail over any attachments. If your Bid is not authorised, it ***will be rejected****. If the Bidder is a Joint Venture (JV), the Bid must be signed by an authorized representative of the JV on behalf of the JV, and to be legally binding on all the members as evidenced by a power of attorney signed by their legally authorized representatives.*

Bidders must mark as "CONFIDENTIAL" information in their Bids which is confidential to their business. This may include proprietary information, trade secrets or commercial or financially sensitive information}.

Procurement Reference Number:

Subject of Procurement:

Name of Bidder:

Bidder's Reference Number:

Date of Bid:

We offer to provide the services listed in the attached Statement of Requirements, at the prices indicated on the attached Price Schedule and in accordance with the terms and conditions stated in your Bidding Document referenced above.

We confirm that we meet the eligibility criteria specified in Part 1: Procedures of Bidding.

We declare that we are not debarred from bidding and that the documents we submit are true and correct.

The validity period of our bid is: …….. *{days}* from the date of submission.

We confirm that the prices quoted in the attached Price Schedule are fixed and firm for the duration of the validity period and will not be subject to revision, variation, or adjustment within the bid validity period.

Bid Authorised by:

Signature	……	**Name**	……
Position:	……	**Date:**	……*(DD/MM/YY)*
Authorised for and on behalf of:			
Company	……		
Address:	……		
	……		

Bid-Securing Declaration

{The Bidder must fill in this Form in accordance with the instructions indicated, where it has been stated in the Bidding Procedures that a Bid-Securing Declaration is a requirement of bidding}.

Procurement Reference number:

Date: ……..……*[date (in day, month and year format)]*

To: *{full name of Procuring Entity}*

We, the undersigned, declare that:

We understand that, according to the terms and conditions of your bidding documents, bids must be supported by a Bid-Securing Declaration.

We accept that we may be debarred from bidding for any contract with a Procuring Entity in Zimbabwe for a period to be determined by the Authority, if we are in breach of our obligation(s) under the bidding conditions, because:

(a) we have withdrawn our Bid during the period of Bid validity; or

(b) having been notified of the acceptance of our Bid by the Procuring Entity during the period of bid validity, we fail or refuse to execute the Contract.

We understand this Bid Securing Declaration will expire if we are not the successful Bidder, either when we receive your notification to us of the name of the successful Bidder, or twenty-eight days after the expiration of our Bid, whichever is the earlier.

Signed ……. **Name:** ……

In capacity of: ……. **Date:** ……*(DD/MM/YY)* **Duly authorised for and on behalf of:**

Company ……

Address: ……

……

Corporate Seal (where appropriate)

{Note: In case of a Joint Venture, the Bid Securing Declaration must be in the name of all the partners to the Joint Venture that submits the Bid.}

PART 2 STATEMENT OF REQUIREMENTS

Below are the Technical Requirements against which technical evaluation will be based for the provision of a cyber security training and awareness platform.

Bidders are advised to provide a quotation for the entire specified platform below (ranging from section 1.1 to 1.9).

1. TRAINING/AWARENESS

1.1. Training Content Library

i. **Security Content Library Scope**: The platform must provide a comprehensive and regularly updated security awareness training library covering diverse topics including phishing, social engineering, password security, AI, PCI-DSS, compliance frameworks, and other relevant cybersecurity subjects.

ii. **Content Customization Capabilities**: The platform must offer customization options for training materials to align with organizational branding, specific security policies, and unique security requirements.

iii. **Compliance-Specific Modules**: The Platform must include specialized training modules addressing key regulatory frameworks including GDPR, Anti-Money Laundering (AML), and Anti-Bribery and Corruption requirements.

iv. **Adaptive Learning Technology**: The platform must employ artificial intelligence to recommend personalized training paths based on users' roles, previous performance, identified knowledge gaps, and security risk profiles.

v. **Multi-Format Content Delivery**: The Platform must provide diverse learning formats including videos, audiocasts, interactive modules, quizzes, and gamified learning experiences to optimize user engagement and knowledge retention.

vi. **Administrative Tracking and Reporting**: The platform must offer robust administrative capabilities for tracking employee progress, completion rates, knowledge assessments, and compliance status with detailed reporting options.

vii. **Accessibility Compliance**: The Platform must adhere to Web Content Accessibility Guidelines (WCAG) version 2 or higher to accommodate all users including those with special needs.

viii. **Mobile and Cross-Platform Functionality**: The platform must support training content access across various devices including desktops, tablets, and mobile phones with responsive design. The platform shall also allow content to be downloaded on the mobile app.

ix. **SCORM Compatibility**: The Platform must provide training content in SCORM (Sharable Content Object Reference Model) format to ensure compatibility with existing Learning Management Systems.

x. **Implementation Support Services**: The Platform must provide comprehensive technical support for platform implementation, content integration with existing training programs, and ongoing assistance for optimal utilization.

1.2 Compliance Training Requirement

i. **Comprehensive Compliance Training Library**: The Platform must provide an extensive library of compliance training modules addressing key regulatory frameworks, industry standards, and relevant governance requirements of the Bank.

ii. **Regulatory Coverage Scope**: The platform must include specific training modules covering critical regulations including but not limited to GDPR, PCI DSS, Data Privacy and Protection and other applicable compliance standards, with demonstrable capabilities to meet regulatory requirements.

iii. **Content Currency and Updates**: The Platform must maintain a rigorous update schedule for all compliance training materials, ensuring content reflects the latest regulatory changes, legal interpretations, and compliance best practices.

iv. **Multi-Format Compliance Learning**: The platform must deliver compliance training through diverse learning formats including videos, interactive modules, scenario-based learning, and assessment quizzes to accommodate different learning preferences and maximize engagement.

v. **Compliance Tracking and Reporting**: The Platform must provide robust audit-ready reporting features that document training completion, knowledge verification, and compliance status to demonstrate due diligence to regulators and auditors.

vi. **Industry-Specific Compliance Solutions**: The Platform must provide tailored compliance training addressing sector-specific regulations and requirements relevant to the Bank's industry vertical and business activities.

vii. **Risk Reduction Methodology**: The platform must employ instructional design approaches specifically engineered to reduce compliance incidents and breaches through behavior modification, risk awareness, and practical application of compliance principles.

viii. **SCORM Content Compatibility**: All compliance training content including videos, interactive modules, and assessment quizzes must be available in SCORM format to ensure seamless integration with existing learning management infrastructure.

ix. **Compliance Program Integration**: The Platform must provide implementation guidance and support for integrating compliance training into the Bank's broader governance, risk management, and compliance (GRC) framework to establish a holistic compliance culture.

1.3 Assessments and Training Completion

i. **Comprehensive Assessment Framework**: The platform shall provide multiple assessment methodologies including baseline security awareness measurements, phishing simulation benchmarks, knowledge verification quizzes, and behavioral analysis tools with department-specific assessment capabilities and industry benchmarking comparisons.

ii. **Adaptive Learning Pathways**: The platform must support conditional training assignments based on assessment performance, user role, department classification, risk level, and behavior patterns, automatically enrolling users in appropriate remedial or advanced content without manual intervention.

iii. **Enterprise Campaign Automation**: The platform must deliver robust campaign management capabilities including recurring schedules, role-based training paths, automated enrollment for new employees, configurable reminder systems, and progress tracking with minimal administrative overhead.

iv. **Learning Management Integration**: The platform must support bidirectional integration with existing Learning Management Systems through standard protocols (SCORM, AICC, xAPI) while also providing comprehensive native LMS functionality including course assignment, completion tracking, and certification management.

v. **Customizable Notification System**: The Platform must enable fully customizable email communications including enrollment notices, training reminders, escalation alerts to managers, completion acknowledgments, and policy notifications with custom branding and configurable message content.

vi. **Policy Management Suite**: The platform must include tools for creating, distributing, tracking, and attesting to Bank policies with signature capture, version control, compliance reporting, and the ability to incorporate policy acknowledgment into training curricula.

vii. **Branded Learning Experience**: The platform must support extensive customization of the training environment including organizational logos, custom certificates, branded interfaces, personalized welcome/completion messages, and visual alignment with internal systems.

viii. **Content Customization Capabilities**: The platform must enable the Bank to modify existing training content, upload proprietary materials, create custom courses, and blend internal policies with the Platform's security awareness library to create a cohesive learning experience.

ix. **Learner-Centric Interface**: The platform must provide an intuitive, accessible user experience with personalized dashboards showing assigned courses, completion deadlines, learning progress, achievement history, and available optional training with multilingual support and responsive design.

x. **Multi-Device Learning Environment**: The platform must deliver seamless training access across desktop and mobile devices with synchronized progress tracking, offline learning capabilities, native mobile applications for major platforms (iOS/Android), and optimized content delivery for various screen formats and network conditions.

1.4 Phishing

i. **Customizable Phishing Templates:** The platform must provide an extensive library of phishing templates that can be fully customized to match organizational branding, communication styles, and departmental variations, including the ability to incorporate custom logos, email signatures, and authentic formatting.

ii. **Advanced Phishing Simulation Types:** The platform must support diverse phishing attack simulations including but not limited to email-based phishing, spear phishing, USB/physical phishing, phone phishing, attachment-based phishing, and reply-to phishing.

i. **Campaign Targeting and Scheduling:** The Platform must enable precise targeting of phishing campaigns to specific departments, roles, or risk groups with flexible scheduling options including immediate deployment, scheduled dates/times, and automated recurring campaigns.

iii. **Difficulty Progression Framework:** The platform must offer graduated difficulty levels for phishing simulations that can adapt based on user performance, allowing organizations to progressively challenge employees as their security awareness improves.

iv. **Real-Time Analytics Dashboard:** The platform must provide comprehensive real-time reporting capabilities that track click rates, response actions, improvement trends, and high-risk user identification with exportable data for compliance documentation.

v. **Phish Alert Button (PAB) Implementation:** The platform must include a cross-platform compatible reporting tool (Phish Alert Button) for major email clients that enables users to report suspected phishing emails with customizable appearance and feedback messaging.

vi. **Automated Email Security Response:** The platform must provide functionality to automatically remove, or quarantine identified phishing emails after user reporting, including handling of forwards/replies and selective attachment removal.

vii. **Threat Intelligence Integration:** The platform must continuously analyze current threat landscapes to regularly update phishing templates reflecting emerging threats, with particular attention to industry-specific attack methodologies relevant to the Bank.

viii. **Educational Landing Pages:** The platform must provide customizable landing pages with educational content that appear when users interact with phishing simulations, including options for interactive elements, videos, and tailored messaging aligned with custom training objectives.

ix. **Reported Email Analysis System:** The platform must include AI-powered analysis capabilities for user-reported emails that can distinguish between simulated and actual threats, prioritize genuine security incidents, and provide actionable intelligence to security teams while offering immediate feedback to reporting users.

1.5 Reporting

i. **Comprehensive Metrics Dashboard**: The platform must provide an intuitive, centralized dashboard displaying key security awareness performance indicators including training completion rates, phishing simulation results, compliance status, and risk score trends with customizable viewing options.

ii. **Multi-level Reporting Hierarchy**: The platform must support role-based reporting access with tailored dashboards for different stakeholder groups including executive summaries for senior leadership, departmental analytics for managers, and detailed operational reports for security administrators.

iii. **Granular Data Analysis Capabilities**: The platform must enable deep-dive analytics with drill-down functionality from overviews to departmental comparisons to individual user performance metrics, supporting comprehensive root cause analysis of security awareness issues.

iv. **Custom Report Builder**: The platform must include a flexible report creation tool allowing administrators to design custom reports based on specific organizational criteria, metrics combinations, and business requirements with savable templates for recurring use.

v. **Comparative Analytics Framework**: The platform must provide robust comparative reporting capabilities allowing benchmarking of performance across business units, job functions, and time periods to identify security awareness gaps and improvement opportunities.

vi. **Automated Report Distribution**: The platform must support scheduled report generation and automated distribution to designated recipients at configurable intervals (daily, weekly, monthly, quarterly) in preferred formats to streamline security awareness program management.

vii. **Data Visualization Suite**: The platform must deliver a comprehensive set of data visualization options including trend graphs, heat maps, comparative charts, and performance matrices to effectively communicate complex security awareness metrics to diverse audiences.

viii. **Export Functionality**: The platform must support multiple data export formats including PDF, Excel, CSV, and API access to facilitate integration with other business intelligence tools and enterprise reporting platforms.

ix. **ROI and Business Impact Metrics**: The platform must provide analytical tools to correlate security awareness activities with business outcomes including risk reduction measurements, incident prevention calculations, and compliance readiness assessments.

x. **Custom Field Implementation**: The platform must allow for the creation and integration of organization-specific custom fields and metadata into the reporting system to accommodate unique business contexts, specialized tracking requirements, and industry-specific compliance needs.

1.6 User Management

i. **Directory Integration Framework**: The Platform shall provide comprehensive integration with existing directory services including Active Directory, Azure AD, and LDAP, supporting bidirectional synchronization of user accounts, attributes, and organizational structures.

ii. **Enterprise Authentication Standards**: The platform must implement industry-standard authentication protocols including SAML 2.0 for Single Sign-On (SSO) and support multi-factor authentication (MFA) that integrates with existing organizational authentication infrastructure.

iii. **SCIM Provisioning Support**: The Platform shall support the System for Cross-domain Identity Management (SCIM) standard for automated user provisioning, deprovisioning, and attribute synchronization between enterprise identity systems and the security awareness platform.

iv. **Configurable Synchronization Schedule**: The platform must provide flexible configuration options for synchronization frequency between The Platform and enterprise identity systems, including real-time, scheduled, and manual synchronization capabilities to accommodate varying operational requirements.

v. **Role-Based Access Control**: The Platform must implement granular permission sets that can be mapped to organizational roles, enabling precise control over platform features, data access, and administrative capabilities based on user responsibilities within the security program.

vi. **Dynamic User Grouping**: The platform must support rule-based user segmentation with dynamic group membership that automatically updates based on changing user attributes, organizational structures, and security requirements without manual intervention.

vii. **Attribute-Based Assignment Automation**: The Platform must enable automated assignment of training, phishing simulations, and security initiatives based on user attributes, group memberships, risk profiles, and organizational roles to ensure targeted security awareness activities.

viii. **User Lifecycle Management**: The platform must provide comprehensive user lifecycle capabilities including automated onboarding, role transitions, status changes, archiving, and account termination synchronized with enterprise identity systems.

ix. **Custom Attribute Support**: The Platform shall allow for the creation, mapping, and utilization of organization-specific attributes within the user management system to accommodate unique structures, business requirements, and security program needs.

x. **Administrative Hierarchy Configuration**: The platform must support the establishment of multi-tiered administrative structures with customizable access scopes, allowing decentralized management of specific user populations while maintaining centralized program governance and oversight.

1.7 Implementation & Service

i. **Structured Implementation Methodology:** The Platform shall provide a comprehensive, phased deployment framework including discovery, planning, configuration, integration, testing, and launch stages with clearly defined milestones, deliverables, and timelines.

ii. **Dedicated Implementation Team:** The vendor must assign a dedicated implementation manager and technical specialists who will serve as primary points of contact throughout the deployment process, providing expertise, guidance, and continuity from contract execution through production launch.

iii. **System Integration Services:** The Platform shall deliver technical integration services for connecting the security awareness platform with existing enterprise systems including identity management, email infrastructure, learning management systems, and security tools with documented APIs and integration methods.

iv. **Administrator Enablement Program:** The platform provider must deliver comprehensive administrator training covering platform configuration, user management, content administration, campaign execution, reporting capabilities, and program optimization through both live instruction and self-paced learning resources.

v. **Multi-tier Support Structure:** The Platform shall maintain a multi-level technical support system with clearly defined severity classifications, response time commitments, escalation procedures, and resolution timeframes accessible through multiple channels including phone, email, chat, and online ticket submission.

vi. **Enterprise-grade Infrastructure:** The platform must be delivered as a secure, scalable SaaS solution hosted on tier-1 cloud infrastructure with guaranteed 99.9% minimum uptime, comprehensive disaster recovery capabilities, regular security assessments, and transparent status monitoring.

vii. **Continuous Knowledge Resources:** The Platform shall provide ongoing access to cybersecurity expertise through regularly updated knowledge bases, best practice guides, implementation playbooks, user forums, webinars, and industry trend analysis to maximize platform effectiveness.

viii. **Customer Success Program:** The vendor must implement a proactive customer success framework including regular account reviews, health checks, optimization recommendations, benchmarking, and roadmap consultations to ensure continued alignment with security objectives.

ix. **Community Engagement Platform:** The Platform shall facilitate a user community enabling peer networking, best practice sharing, implementation insights, and collaborative problem-solving among security awareness professionals utilizing the platform.

x. Service Level Guarantees: The platform provider must establish clear service level agreements covering system availability, performance metrics, support responsiveness, implementation timelines, and quality standards with defined remediation processes for any service shortfalls.

1.8 Platform Minimum Requirements

i. **Cloud-Based SaaS Architecture**: The Platform shall provide its security awareness platform as a fully managed Software as a Service (SaaS) solution utilizing enterprise-grade cloud infrastructure from industry-leading providers (AWS, Azure, or Google Cloud) with no on-premises hardware or software installation requirements.

ii. **Multi-Tenant Environment**: The platform must employ a secure multi-tenant architecture that logically separates organizational data while enabling efficient resource utilization, streamlined updates, and consistent performance.

iii. **High Availability Infrastructure**: The Platform shall maintain redundant, geographically distributed data centers with automated failover mechanisms, ensuring a minimum of 99.9% platform uptime guaranteed through formal Service Level Agreements with defined remediation procedures.

iv. **Scalable Resource Allocation**: The platform must dynamically scale to accommodate varying workloads, growing user populations, and peak demand periods without performance degradation.

v. **Comprehensive Disaster Recovery**: The Platform shall implement robust disaster recovery protocols including regular data backups, geographically dispersed redundancy, documented recovery procedures, and annual disaster recovery testing with published Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).

vi. **Enterprise Access Management**: The platform must support industry-standard authentication protocols including SAML 2.0, OpenID Connect, and SCIM, enabling secure integration with enterprise identity providers, single sign-on implementations, and multi-factor authentication systems.

vii. **Secure Data Processing**: The Platform shall employ comprehensive data security measures including encryption for data in transit (TLS 1.2+) and at rest (AES-256), secure API implementations, regular security assessments, and strict access controls.

viii. **Performance Monitoring**: The platform must include real-time performance monitoring, automated alerting systems, and transparent status reporting.

ix. **Compliance Certifications**: The Platform shall maintain relevant security and privacy certifications including SOC 2 Type II, ISO 27001, and GDPR compliance, with documentation available to the Bank for compliance verification requirements.

x. **Future-Proof Technology Stack**: The platform must utilize modern, supported technologies with a clear obsolescence management plan, regular version updates, and a documented product roadmap ensuring continued functionality, security, and compatibility with the evolving environment of the Bank.

1.9 Data Security and Privacy:

i. **Data Residency Framework**: The Platform shall maintain transparent documentation of all data storage locations, processing facilities, and data flows, with options for regional data residency to support compliance with local data sovereignty requirements and organizational governance policies.

ii. **Comprehensive Encryption Protocol**: The platform must implement industry-leading encryption standards including TLS 1.2+ with perfect forward secrecy for all data in transit and AES-256-bit encryption for all data at rest, with robust key management practices and regular cryptographic assessment.

iii. **Defense-in-Depth Security Architecture**: The Platform must employ multiple security layers including network segmentation, web application firewalls,

intrusion detection/prevention systems, endpoint security, and regular penetration testing to protect the Bank's data from unauthorized access.

iv. **Identity and Access Management Controls**: The platform must enforce strict access controls based on the least privilege principles, with multi-factor authentication, role-based permissions, contextual access policies, comprehensive audit logging, and automated anomaly detection for all system access.

v. **Privacy by Design Implementation**: The platform must adhere to privacy by design principles throughout the data lifecycle, including data minimization, purpose limitation, automated retention policies, and anonymization/pseudonymization capabilities where necessary.

vi. **Security Compliance Certifications**: The platform provider must maintain current industry security certifications including SOC 2 Type II, ISO 27001, and applicable standards (e.g., GDPR, CDPA) with regular independent attestation and documentation available.

vii. **Incident Response Protocol**: The platform must establish comprehensive security incident management procedures including 24/7 monitoring, defined response teams, notification processes, forensic capabilities, and documented recovery procedures tested through regular simulations.

viii. **Vendor Security Management**: The platform provider must implement rigorous third-party risk management for all sub processors with documented security requirements, regular assessments, contractual safeguards, and transparency regarding all entities that may process customer data.

ix. **Data Processing Documentation**: The platform must maintain detailed records of processing activities, data flows, retention periods, and lawful processing bases.

x. **Security Development Lifecycle**: The platform must be developed under a formal security development methodology including secure coding practices, automated security testing, vulnerability management, and regular code reviews to prevent security vulnerabilities throughout the application lifecycle.

2. DEMONSTATION & PRESENTATION

A demonstration of the platform may be requested to ensure that all the requirements and specifications are adequately satisfied.

3. PRICE SCHEDULE

Currency of Quotation/Contract: ____**USD**__

Bidders are required to complete the Price schedule below and provide all costs that make up the total price for the Supply and Delivery of a Cybersecurity Training and Awareness Platform (as specified on the Statement of Requirement in Part 2 Section 1.1 to 1.9) for **550 users.**

Item No[1]	Description of Services	Licensing Model	Input Quantity	Unit Rate Price	Total Price[2]
1	**Once-off Software License Fees**		550		
2	**Annual Software License Fees**		550		
3	**Annual Support Fees**		550		
4	**Implementation Fees**		550		
			Other additional costs		
			VAT 15.5%		
			Total		

Quote to be based on 550 users and also provide any additional costs that may not be indicated on the above schedule

Technical Specification and Compliance Sheet

Name of Bidder:

Bidder's Reference Number:

The Goods and Related Services must comply with following Technical Specifications and Standards:

[Columns a and b are completed by the Procuring Entity. Column c must be completed by the Bidder to indicate the full specification of the items offered and their compliance with the specification required (in Column b)]

a	b	c
	Item description and full technical Specification required (including applicable standards)	***{Confirm full specification of items offered by Bidder <u>and</u> compliance of items to detail in column b}***
1	Supply and Delivery of a Cybersecurity Training and Awareness Platform (as specified on the Statement of Requirement in Part 2 Section 1.1 to 1.9)	

Delivery Schedule

Name of Bidder: Bidder's Reference Number:

{Note to Bidders: If the delivery period offered, or any other details, differs from the requirements below, this should be stated in your tender}.

Description of Goods	**Quantity**	**Delivery Date Required by Procuring Entity and applicable INCOTERM**	**Bidder's offered Delivery period**
Supply and Delivery of a Cybersecurity Training and Awareness Platform (as specified on the Statement of Requirement in Part 2 Section 1.1 to 1.9)	1	Delivery Duty paid (DDP) Within one calendar month	{*to be provided by the Bidder*}

The delivery period required is measured from the date of the signing of the Contract between the Procuring Entity and the Bidder.

The Site for delivery of the goods is the final destination which is:

POSB HEAD OFFICE CAUSEWAY BUILDING CNR 3RD AND CENTRAL AVENUE, HARARE