

CYBER SECURITY AWARENESS & TRAINING SOLUTION FOR A PERIOD OF THREE (3) YEARS BID

ANNEXURE A – RESPONSE TEMPLATE FOR FUNCTIONAL REQUIREMENTS

Please provide a detailed explanation of your company's capability to comply with and meet the requirements outlined in the following elements related to the paragraphs of the Terms of Reference.

NB: Bidders who score less than 70 of the 100 points of the functionality points will be disqualified and thus will not be evaluated further. (7.2. Stage One: Phase Two – Evaluation on Functionality Criteria)

1. TRAINING, AWARENESS AND SIMULATION
4.1.1. Visual and Computer-Based Training: How does your solution deliver visual and computer-based training materials tailored to SASSA users, including assessments and simulations?
4.1.2. Gamified and Engaging Training: What gamified training features are included to enhance user engagement and retention?
4.1.3. Continuously Updated Content Library: How is the solution's content library maintained and updated, and what role does AI play in ensuring relevance and responsiveness to emerging threats?

4.1.4. Integration of SASSA Policies: How does your solution incorporate SASSA's internal policies and regulatory requirements (e.g., POPIA, GDPR) into training content?

4.1.5. Engaging Compliance Training: What mechanisms are used to deliver engaging compliance training that effectively modifies user behaviour and reduces risk?

4.1.6. Customized Phishing Awareness Training: How does your solution personalize phishing awareness training using AI, and what capabilities exist for simulating phishing attacks tailored to SASSA's threat landscape?

4.1.7. Baseline Phish-Prone Percentage: How is the baseline phish-prone percentage established, and what methods are used for continuous testing and risk assessment?

4.1.8. User Categorization and Classification: How does your solution support user categorization and classification to enable targeted training and reporting?

4.1.9. Active Feedback Loops: What analytics and feedback mechanisms are included to monitor user awareness and improve resilience against social engineering threats?

2. REPORTING, CONTENT MANAGEMENT AND CUSTOMISATION

4.2.1. Progress Reports and Recommendations: How does your solution generate progress reports and provide actionable, data-driven recommendations?

4.2.2. Data-Driven Dashboard: What dashboard features are available to summarize phishing assessments, detection rules, training compliance, and security events?

4.2.3. Training Compliance Monitoring: How does your solution monitor training completion and escalate non-compliance to supervisors?

4.2.4. Risk Monitoring Customisation: How does your solution enable SASSA to define and customise the monitoring of specific risky user behaviours?

4.2.5. Training Effectiveness Metrics: What metrics are used to assess training effectiveness and user understanding?

4.2.6. Compliance Overview Visualization: How does your solution visualize SASSA's overall compliance status and track improvement measures?

4.2.7. Customisable Templates and Landing Pages: What customisation options are available for phishing templates, landing pages, passing scores, and branding to align with SASSA's regulatory and organizational requirements?

--

3. ADVANCED EMAIL THREAT PROTECTION

4.3.1. Automatic Blocking of Email Threats: How does your solution automatically detect and block email threats that bypass existing security measures?

--

4.3.2. Crowdsourced and AI-Driven Threat Intelligence: What role does crowdsourced intelligence and AI play in enhancing threat detection and blocklisting?

--

4.3.3. Automated Quarantine and Safe Simulations: How does your solution quarantine malicious emails and convert reported phishing attempts into safe simulations for training purposes?

--

4. CLOUD-BASED ARCHITECTURE AND DATA HANDLING

4.4.1. Architecture and Management: How is your solution architected for cloud-based deployment and ease of management?

--

4.4.2. Data Inventory: Can you provide a detailed inventory of the types of data processed by your cloud system (e.g., IP address, device name, user ID), and how is transparency ensured?

4.4.3. Data Transparency and Compliance: How does your solution ensure compliance with POPIA and GDPR when handling cross-border data transfers and processing?