

## TECHNICAL EVALUATION CRITERIA – CYBERSECURITY AWARENESS SOLUTION

<b><u>GATE KEEPER CRITERIA – 100%</u></b>					
<b>The tenderer will be disqualified and not further evaluated for the paper-based technical evaluation if they provide only one letter or none at all.</b>					
	#	Question	Components	Response (Y/N)	Substantiate/ Indicate in RFP Response
<b>Gate-keepers (Mandatory requirements)</b>	1	The tenderer must provide evidence that they successfully supported at least two customers with cyber security awareness.	Provide two signed reference letters from each customer that indicates the awareness scope of the service offered.		Provide two signed reference letters from each customer that indicate the awareness scope of the service offered.

<b><u>PAPER-BASED TECHNICAL EVALUATION CRITERIA – 45%</u></b>					
<b>The minimum required threshold for the Paper-based Technical Evaluation is 80% of 45% (Minimum score of 36). The tenderer that does meet the required minimum threshold of 80% will be disqualified and not further evaluated.</b>					
Category	#	Requirement	Weight	Response Y/N	Substantiate/ Indicate in RFP Response
<b>Paper-based Technical Evaluation Criteria - 45%</b>	1	The tenderer must provide the complete scope of work as stated in the tender documents and can demonstrate the proposed solution.	<b>7%</b>  Letter provided and can fully meet the solution = 7%  Letter provided and can partially meet the requirement = 3.5%  Does not meet the requirements or no letter provided= 0%		Provide a signed letter that confirms that the tenderer will provide Eskom with the full scope.
	2	The tenderer can deliver cybersecurity awareness and training campaigns targeted at IT and OT environments respectively and can demonstrate the proposed solution.	<b>7%</b>  Letter provided and can fully demonstrate the solution = 7%  Letter provided and cannot fully demonstrate the solution = 3%  No letter provided = 0%		Provide a signed letter that confirms that the tenderer will deliver on the requirement for both IT and OT environments.
	3	The proposed solution must be in the latest Gartner Magic Quadrant for Computer-Based Training or the Forrester Wave of Security Awareness and Training Solutions.	<b>6%</b>  Leaders =6%  Challenger/Strong performer = 3%  Niche/Contenders = 2%  Visionary/Risky bets = 1%  Not in any quadrant / nonresponsive = 0%		Provide proof of where the Solution was rated in past 3 years, i.e., Gartner Magic Quadrant or Forrester Wave

	<b>4</b>	The tenderer is a certified product specialist or service delivery partner of the proposed solution.	<b>7%</b>  Letter provided = 7%  No letter = 0%		Provide a letter from the OEM that confirms the relationship.
	<b>5</b>	The professional resources (1 change manager, 4 support personnel, 1 security governance specialist) must have relevant certification to support awareness and training activities on the proposed solution, provide change management and security governance to ultimately create a proactive cybersecurity culture.	<b>8%</b>  4x support staff, 1 change manager and 1 security governance specialist = 8%  3x support staff, 1 change manager and 1 security governance specialist = 6%  2x support staff, 1 change manager and 1 security governance specialist = 4%  4x support staff, 0 change manager and 0 security governance specialist = 2%  Non-responsive = 0%		Please provide detailed CV's (including applicable certification related to the proposed solution and/or area of expertise) clearly indicating number of years related to awareness and training services.
	<b>6</b>	The tenderer should be located in the Republic of South Africa.	<b>2%</b>  Document submitted = 2%  No document submitted = 0%		CIPC registration document
	<b>7</b>	The tenderer or/bidding company must be ISO27001 certified.	<b>4%</b>  Certified = 4%  Not certified/non-responsive = 0%		Provide ISO27001 certificate
	<b>8</b>	Does the tenderer have a Privacy Policy with regards to its employees, partners, and subcontractors?	<b>4%</b>  Fully Compliant - respondent has a policy covering Eskom legal requirements = 4%  The respondent does have a policy but does not sufficiently cover all Eskom legal requirements = 2%  Totally deficient or Non-responsive or Respondent did not provide own privacy policy = 0%		Provide evidence of the Policy.

### **FUNCTIONAL DEMONSTRATION – 55%**

The minimum required threshold for the Functional Demonstration is 80% of 55% (Minimum score of 44). The tenderer that does not meet the required minimum threshold of 80% will be disqualified and not further evaluated.

The tenderer must demonstrate that their solution meets the functional requirements listed below. Throughout the functional demonstration, Eskom will ask questions. The demonstration will be performed online via MS Teams.

Category	#	Requirement	Weight	Achieved Y/N	Comments
<b>DEMO Criteria – 55%</b>	<b>1</b>	<b>Awareness Campaigns for IT/OT</b>	<b>10%</b>		
		<ul style="list-style-type: none"> <li>The tenderer must demonstrate cybersecurity awareness and training campaigns targeted at IT and OT environments respectively.</li> </ul>	Requirement met = 10% Requirement partially met = 5% Requirement not met = 0%		
	<b>2</b>	<b>Templates</b>	<b>10%</b>		
		<ul style="list-style-type: none"> <li>The proposed solution must provide customizable templates for different business environments i.e., Information Technology, Operational Technology, Legal and other targeted business environments.</li> <li>The solution must provide customizable templates for different user levels (e.g., general employees, Senior Management, Executives).</li> </ul>	Requirement met = 5% Requirement partially met = 2.5% Requirement not met = 0%  Requirement met = 5% Requirement partially met = 2.5% Requirement not met = 0%		
	<b>3</b>	<b>Solution Capabilities</b>	<b>11%</b>		
		<ul style="list-style-type: none"> <li>The solution must provide phishing simulations that can test a variety of variables such as opening file attachments, clicking embedded links and also track performance of the users on the previous phishing simulations, identify risky users or repeat offenders.</li> <li>The solution must provide a comprehensive and customisable content, which receives regular updates on cyber threat landscape and Information Technology regulatory compliance requirements.</li> </ul>	Requirement met = 2% Requirement not met = 0%  Requirement met = 2% Requirement not met = 0%		

		<ul style="list-style-type: none"> <li>The solution must support well known and secure web browsers such as Microsoft Edge and Mozilla Fire Fox.</li> </ul>	Requirement met = 1% Requirement not met = 0%		
		<ul style="list-style-type: none"> <li>The solution must provide a reporting dashboard with analytics capabilities.</li> </ul>	Requirement met = 2% Requirement not met = 0%		
		<ul style="list-style-type: none"> <li>The solution must be able to send automated reminders about any upcoming or outstanding awareness campaigns and training.</li> </ul>	Requirement met = 2% Requirement not met = 0%		
		<ul style="list-style-type: none"> <li>Access to the solution must be secure, user-friendly, and not require VPN access as a pre-requisite.</li> </ul>	Requirement met = 2% Requirement not met = 0%		
	<b>4</b>	<b>Campaigns &amp; Training</b>	<b>11%</b>		
		<ul style="list-style-type: none"> <li>The solution should be able to create a “target list” campaign to address users who failed the phishing test.</li> </ul>	Requirement met = 2,75% Requirement not met = 0%		
		<ul style="list-style-type: none"> <li>The solution must be able to send targeted campaigns to selected users from different Divisions and Departments.</li> </ul>	Requirement met = 2,75% Requirement not met = 0%		
		<ul style="list-style-type: none"> <li>Campaigns and training templates should be customizable</li> </ul>	Requirement met = 2,75% Requirement not met = 0%		
		<ul style="list-style-type: none"> <li>The solution should allow the scheduling of awareness campaigns and send them to the target list at specific times.</li> </ul>	Requirement met = 2,75% Requirement not met = 0%		
	<b>5</b>	<b>Reporting</b>	<b>11%</b>		
		<ul style="list-style-type: none"> <li>Provide campaign and training reports that can be filtered according to user levels or groupings.</li> </ul>	Requirement met = 2% Requirement not met = 0%		
		<ul style="list-style-type: none"> <li>Reports on emails sent for each campaign</li> </ul>	Requirement met = 2% Requirement not met = 0%		
		<ul style="list-style-type: none"> <li>Reports on emails received and opened for each campaign</li> </ul>	Requirement met = 1% Requirement not met = 0%		

		<ul style="list-style-type: none"> <li>• Reports on users who adhere to email instructions, access the Awareness and Training solution to start and finish their training.</li> </ul>	Requirement met = 2% Requirement not met = 0%		
		<ul style="list-style-type: none"> <li>• Report on built in threat intelligence to identify risky behaviour based on emerging threats and vulnerabilities</li> </ul>	Requirement met = 2% Requirement not met = 0%		
		<ul style="list-style-type: none"> <li>• Trend reports indicating awareness and training performance and examines the changes of employee behaviour as a result of campaigns.</li> </ul>	Requirement met =2% Requirement not met = 0%		
	<b>6</b>	<b>Other Capabilities</b>	<b>2%</b>		
		<ul style="list-style-type: none"> <li>• Elaborate on other capabilities provided by the solution.</li> </ul>	Requirement met =2% Requirement not met = 0%		

**To pass the Cybersecurity Awareness Solution Technical Evaluation, the tenderer must receive a total of 80% from the combined scores of the Paper-based Technical Evaluation and Functional Demonstration.**

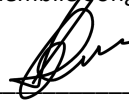
## DOCUMENT ACKNOWLEDGEMENT

*By signing this document, the people listed record their agreement on the contents of this document.*

Senior Manager – IT Security  
Services (Approver)

**Name:** Sithembile Songo

**Signature:**



**Date:** 06-12-2022

Middle Manager – Information  
Security (Supporter)

**Name:** Mmabatho Singo

**Signature:**



**Date:** 06/12/2022

Senior Advisor – Information Security  
(Compiler)

**Name:** Mabongi Ngidi

**Signature:**



**Date:** 06/12/2022