

1. Background Information

Security awareness and training is one of the crucial controls in the management of cyber security attacks in organisations and Eskom. End-users are known as the weakest link when it comes to cyber security attacks as attackers target them through spam emails, ransom ware, computer viruses, malware, advanced techniques and other forms of social engineering and use their naïveté to provide information or inadvertently take an action that opens up the organisation to attack(s).

Cyber security awareness and training provides indisputable defence for Eskom as a national key point to protect its valuable information resources. Although investments in cyber security software or hardware and cyber security insurance are an important, it may all be in vain if cyber awareness and training is not emphasised to end users. Improving cyber awareness will have a major impact on employees to be able to identify and respond appropriately to various cyber security attacks.

Eskom information resources users are stewards of Eskom's critical information resources and with suitable awareness and training mechanisms and services that are recognised by international IT research institutions such as Gartner and Forester, Eskom can benefit from users who are equipped to manage the persistent cyber security related risks.

Currently, Eskom conducts most of security awareness campaigns through email and random presentation at various staff meetings. However, these approaches are not sufficient, and Group IT has observed that some Eskom users still fall victim to unsolicited phishing, spam email and other forms of cyber security attacks.

As a result, Group IT requires an agnostic Awareness and Training solution to be implemented Eskom-wide i.e., Divisions and Subsidiaries to improve the awareness level of Eskom employees by conducting modernised awareness and training campaigns that are effective and measurable.

The purpose of this document is to request approval to issue an open tender to the market to acquire software licences, solution configuration, maintenance and support, premium support and professional services for awareness and training solution. This solution needs to cater for both Information Technology and Operations Technology user base which is 50 000 users. The contract is required over a period of five (5) years.

2. System Lifecycle Consideration

Eskom System Lifecycle Classification					Eskom	
End User Technology & Tools	Enterprise Applications	Digital & Analytics	Line of Business Applications	Real Technology & Infrastructure	Life of Fleet Applications	
Business productivity tools <ul style="list-style-type: none"> Desktop Products Tablets Mobile Conferencing Desktop OS Exchange email Cloud storage Mobile devices Mobile applications Mobile security Mobile management Mobile training 	Shared internal applications <ul style="list-style-type: none"> Customer Relationship Management (CRM) Enterprise Resource Planning (ERP) Human Capital Management (HCM) Supply Chain Management (SCM) 	Reporting and development tools <ul style="list-style-type: none"> Analytics Center of Excellence provides the necessary platform Cloud Business Analytics DevOps Platform 	Energy, Utility & Customer Services <ul style="list-style-type: none"> Generation (Primary Energy, Gas, Coal, Nuclear, Wind, Hydro, etc.) Transmission Regulation, Grid, and Planning and Distribution (Customer Services) 	System software (Hardware & Technology tools) <ul style="list-style-type: none"> Database Security Networks Monitoring Tools Development Tools Operating Systems Integration Platform 	System software (Hardware & Technology tools) <ul style="list-style-type: none"> Database Security Networks Monitoring Tools Development Tools Operating Systems Integration Platform 	
i.e. systems of information and innovation	i.e. systems of record, information and innovation	i.e. systems of information and innovation	i.e. systems of record	Many tied to Systems of record	Tied to life of plant	
Life Cycle						
5 - 7 Years	10 - 15 Years	5 - 7 Years	10 - 15 Years	5 - 10 Years	Tied to life of plant	
Implementation Period						
1.5 - 3 Years (to complete an idea)	Min 2.5 - 4 Years	Min 1.5 - 2 Years	2 - 3 Years	4 Years	Tied to life of plant	
		Low Impact	Medium Impact			

3. Motivation

a. Business motivation:

Eskom's Information Security is inundated with cyber-attacks and sometimes crafted to be targeted to infiltrate on the Eskom environment. The cyber-attacks are launched in various ways, including spam emails (e.g. spoofing of specific email addresses), email attachments with malware, hacking attacks, downloaded malicious files from internet websites etc.

The common denominator in successful cyber-attacks is user action (e.g. clicking on a link, visiting a malicious website, entering Eskom credentials in spoofed websites etc.) in triggering the attack. Research has shown that 90% of the biggest cyber threats to any organization is that organization's own employees and 10% is through tools/technology. This means that a lot more effort is required in directing people's behaviour to become more cyber security conscious and encourage adherence to the Information Security Policy, Procedures and Standards. It has to come to a point where information security becomes part of their day to day responsibilities as Eskom guardians.

In addition to the above, a comprehensive Information Security Awareness solution must be implemented at all levels in the organisation i.e. management and lower levels; and should cater for departmental /roles unique needs. For example, Database administrators require different levels of Information Security Awareness as compared to Programmers. These unique needs must be catered for in a comprehensive and cohesive manner to ensure sustainability and continuity.

Ultimately, it would be in Eskom's best interest to have an end user base who has knowledge of cyber security and understands their responsibilities as users. This is only possible if the training and awareness solution is implemented and utilised to educate Eskom users of cyber-security risks and how they can assist Eskom in reducing the risk.

b. Benefits to Eskom

The acquisition of the Hybrid Cyber Security Awareness service is expected to benefit Eskom in many ways, including the following:

1. Improve end user awareness regarding cyber security attacks and secure Eskom information resources.
2. Alignment with best practice in the deployment of Information Security Awareness campaigns and training interventions
3. Central repository for Information Security Awareness information and training. The envisaged tool will serve as a 'one-stop' platform to access information and training
4. Offering the users a new and engaging way to interact with Information Security, thereby encouraging them to engage with the material presented
5. Increased participation, leading to greater understanding of end user responsibility when accessing and using Eskom information resources
6. Conducting end user activity tracking, and reports will be shared with Eskom's leadership to hold management and employees accountable where participation is lacking
7. Automated reporting will assist Eskom in better understanding the impact of the training and where to improve as well as ensuring compliance with governance and audit requirements

4. Scope of work/Business requirements

The solution and related services must possess the following capabilities but not limited to:

A. Solution

1. The Service Provider will be required to implement, manage, and provide Awareness and Training to Eskom resources
2. Service Provider to develop and implement a process to enable the delivery of the solution's functionalities / capabilities
3. Every process, information and documentation developed during this contract phase will remain Eskom's IP
4. The service provider to propose a delivery model on how to implement the solution in the Eskom environment
5. The vendor will develop a Change Management and rollout plan of the solution.
6. The vendor will be required to provide formal training to Eskom IT Security resources for the proposed solution.
7. The awareness and training services should cater for both IT and OT environment
8. The Supplier has a confidentiality policy with regards to its employees, partners and subcontractors

B. Tool Capabilities

1. The solution must be a cloud solution that provides assessment, training, and reporting capabilities.
2. The solution must assure data confidentiality and data sovereignty (data storage must be subject to RSA laws)
3. Provide a secure end user authentication platform.
4. Offer interfaces to integrate reporting with internal Eskom's Learning Management System and business intelligence tools.
5. Provide content through mobile devices and computers.
6. Provide security awareness training solutions that covers a broad threat intelligence.
7. Provide content that is customizable for increased internal relevance.
8. Administrative interface should be able to synchronise with Microsoft Active Directory and other LDAP related directories.
9. Support random scheduling of the phishing campaign as well as random distribution of campaign templates to different users.
10. Provide the ability to enrol users if they miss a predetermined number of questions.
11. Automatic enrolment of training should also be available for users who fail a phishing simulation or tests.
12. Support compliance for learners with visual disabilities.
13. Customisable reporting which Include the following:
 - Benchmarking against other cyber security awareness-training customers and customers of specific verticals.
 - Support reporting for individuals as well as for defined groups of users.
 - Training reports should provide in-depth results beyond simple completion tracking and should provide metrics such as category/subject performance that drives and focuses training program.

- Offer options to easily export and schedule reports to be sent in a secure manner to designated administrators and/or stakeholders
14. The solution must have capacity to support 50 000 or more user base.
 15. The solution must have a capability to create awareness for both IT and OT environment

C. Professional Services

1. Developing a cyber-security awareness-training and communication plan
2. Design and provide campaign material that will be used across ESKOM which includes:
 - Prepopulated and customized assessments that map to best security practices.
 - Unlimited use for the license term.
3. Develop and configure ESKOM specific training and reassessment campaigns to address high-priority risks (e.g. repeat offenders).
4. Provide training across the user base including cybersecurity best practices and regulatory compliance requirements.
5. Provide detailed reports and recommendations based on awareness campaigns.
6. Provide change management activities related to cyber security awareness
7. Provide security governance activities related to cyber security policies, standards, procedures & guidelines
8. Provide cyber security awareness & training support activities related to the solution
9. Provide project management services

D. Premium Support


1. 24x7 Technical Support
2. Telephonic and on-site (when needed)
3. Provide 2nd line and 3rd line support for the duration of the contract
4. Quick response time to incidents or service requests logged

E. Training

1. Provide onsite, classroom-based and web-based training for IT Security personnel as and when required
2. Train the trainer
3. Solution backend training and administration

5. Service Level Agreement requirements

Service Level	Description	Escalation to SP	Escalations to OEM
Critical	Business has stopped	Response within 1 (one) hour – Level 1 Response within 3 (three) hours – Level 2	Response within 4 (four) hours – Level 3
Major	Business severely impacted	Response within 1 (one) hour – Level 1 Response within 3 (three) hours – Level 2	Response within 4 (four) hours – Level 3
Normal	Minor business impact/ product failure	Response within 1 (one) business day – Level 1 Response within 2 (two) business days – Level 2	Response within 1 (one) business day – Level 3

	<p style="text-align: center;">Group IT Scope of Work</p> <p style="text-align: center;">Awareness and Training Solution</p>
---	--

Low	No business impact but requires one or more updates	Response within 2 (two) business days – Level 1 Response within 2 (two) business days – Level 2	Response within 2 (two) business days – Level 3
Informational	Request for information	Response within 3 (three) business days – Level 1 Response within 3 (three) business days – Level 2	Response within 3 (three) business days – Level 3

6. Technical Evaluation Criteria


See attached

DOCUMENT ACKNOWLEDGEMENT

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

Senior Manager – IT Security
Services (Approver)

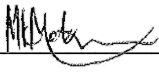
Name: Sithembile Songo

Signature: 

Date: 08-08-2022

Middle Manager – Information
Security (Supporter)


Name: Mmabatho Singo

Signature: 

Date: 08/08/2022

Senior Advisor – Information
Security (Compiler)

Name: Mabongi Ngidi

Signature: 

Date: 08/08/2022