ANNEXURE A – SCOPE OF WORK

Cybersecurity Awareness Platform

Scope of Work

Glossary and Abbreviations

Item	Description
ACSA	Airports Company South Africa
IS	Information Security
ISM	Information Security Management
IP	Internet Protocol
SIEM	Security Information and Event Management
SVM	Security Vulnerability Management
SoW	Scope of Work

Table 1 Glossary and Abbreviations

TABLE OF CONTENTS

1 INTRODUCTION

1.1 PURPOSE

Airports Company South Africa SOC Ltd hereby invites proposals for the provisioning of a managed cyber awareness training platform consisting of an AI-powered tool and trainers for conducting a comprehensive approach to training of all ACSA system users, both internal and external, about cybersecurity threats and best practices that helps protect ACSA to reduce the risk of data breaches and other cyber incidents for the period of 5 years (60 months). The provisioning of a managed cyber awareness platform will include maintenance and support during the same period.

1.2 OBJECTIVE

The objective of this procurement is to source a structured cyber awareness training platform to enhance the cybersecurity posture of the organization through training ACSA system users, both internal and external, on cyber threats, safe practices, and compliance requirements.

1.3 BACKGROUND

One of the critical and high rated risks in technology is Cyber and Information Security (including Protection and Privacy). The increase in cyber security threats, regulatory security safeguard requirements, and low cyber readiness, may lead to loss of data, denial of services, financial loss/fines and unavailability of system or services. The behaviour of employees and contractors with access to data affects information systems and assets. Furthermore, the human factor (what users do or do not do) is the biggest threat to information systems and assets.

The implementation of a managed cyber awareness training platform directly supports ACSA's strategic objectives of strengthening cybersecurity posture, mitigate the cybersecurity risks, safeguarding critical infrastructure, and enhancing operational resilience. This is to ensure that all users are adequately trained and aware of the common tricks and traps used by cybercriminals to exploit vulnerabilities.

The key focus areas for awareness includes knowledge on phishing attacks, weak passwords, unpatched software, unsecured networks, and social engineering tactics, but not limited to these. By recognizing these threats and adopting safe online practices, all ACSA users can significantly reduce their risk of falling victim to cybercrime. A well-managed cybersecurity awareness training program is a crucial investment for ACSA to protect itself from the ever-increasing threat of cyberattacks. By training all users and fostering a strong security culture, ACSA can significantly reduce the risk of data breaches and other security incidents.

2 SCOPE

2.1 IN SCOPE

The following outlines the items that are in scope of the project but not limited to the list, section 3 details the scoped requirements:

- Implementation of an online cybersecurity training platform to educate employees on cyber threats and best practices.
- Development of tailored training modules aligned with ACSA's security policies and risk profile.
- Interactive learning features such as videos, quizzes, and phishing simulations.
- User tracking and reporting tools to monitor participation, progress, and completion rates.
- Regular content updates to reflect evolving cyber threats and compliance requirements.
- Integration with internal systems (e.g., LMS) for user management and reporting.
- Launch of internal awareness campaign to promote engagement and participation.

2.2 OUT OF SCOPE

The following outlines the items that are not in the scope of this project:

- Requirements that are not explicitly defined in this scope of work.
- Cyber awareness training programme design
- Non-ACSA users including boardrooms and service accounts
- Non-ACSA sites

3 FUNCTIONAL REQUIREMENT

ID	FUNCTIONAL REQUIREMENTS
BR 3.1.	**Training Delivery** o Focuses on distributing engaging, relevant, and role-specific cybersecurity education across ACSA. o It ensures that users receive timely and accessible learning materials through secure and scalable channels. Key elements include:
BR 3.1.1	**Secure, cloud-based training platform.** o Training platform that leverages cloud infrastructure to ensure high availability, data protection, and seamless access across devices. Key features include:

	(a) End-to-End Encryption for data in transit and at rest (b) Role-Based Access Control (RBAC) to manage user permissions (c) Multi-Factor Authentication (MFA) for secure login
BR 3.1.2	**Delivery formats:** (a) E-learning modules (b) Simulated phishing campaigns (c) Interactive videos and gamified learning (d) Monthly newsletters and security tips (e) Live webinars and workshops (f) Gamified quizzes and challenges (g) Ability to learn the user's behaviour (h) Comprehensive training library of at least 1000 training content
BR 3.1.3	**AI-Driven Features and Functionalities** o The training platform must include or support the following AI capabilities: (a) Personalization I. Adaptive learning paths based on user behaviour, role, and risk profile. II. AI-generated content recommendations tailored to individual learning needs. (b) Phishing Simulation Intelligence I. AI-generated phishing emails that mimic real-world threats. II. Dynamic difficulty adjustment based on user performance. III. Real-time feedback and coaching after simulation interactions. (c) Behavioural Analytics I. AI-based analysis of user engagement and learning patterns. II. Identification of high-risk individuals or departments. III. Predictive modelling to forecast potential insider threats.
BR 3.2	**Reporting & Analytics**
BR 3.2.1	Dashboards for training progress and phishing simulation results.
BR 3.2.2	Monthly and quarterly executive reports.
BR 3.2.3	Monthly detailed training reports per department
BR 3.2.4	Risk scoring based on user behaviour.

BR 3.2.5	Integration with Active Directory (AD) to allow sign into the platform and enable the deactivation of non-compliant users.
BR 3.3	**Compliance & Certification** o The training awareness platform shall comply, and generate the below:
BR 3.3.1	Regulatory-compliant training modules with POPIA, GDPR, NIST, ISO27001
BR 3.3.2	Certificates of completion to a user on completion of training.
BR 3.4	**Target Audience**
BR 3.4.1	All employees, contractors, and service providers
BR 3.4.2	High-risk departments (e.g., Finance, HR, IT)
BR 3.4.3	Executives and senior leadership
BR 3.5	**Training Modules** o The training library must include the following topics as a minimum:
BR 3.5.1	(a) Cybersecurity Fundamentals (b) Phishing and Social Engineering (c) Password Hygiene and Multi-Factor Authentication (MFA) (d) Data Protection and Privacy (e) Secure Use of Devices and Networks (f) Incident Reporting Procedures (g) Compliance and Regulatory Awareness (e.g., POPIA, GDPR, ISO 27001)
BR 3.5	Each published training content must have an expiry date. The system must be able to track it and generate reminders targeted to a user.
BR 3.5.1	The system must integrate with Outlook to send notifications to users when there is an assigned training(s)
BR 3.5.2	**Cyber Awareness Mascot** o Create a digital and physical cybersecurity awareness mascot that can resonate with ACSA employees and contractors o Ensure that the mascot is embedded on all cyber awareness content

BR 3.6	**Physical training** o The trainer must have the follow requirements.
BR 3.6.1	**Qualifications** o IT qualification with one cyber security certificate such as CompTIA Security, ITIL etc.
BR 3.6.2	**Knowledge & Expertise** o Cybersecurity Fundamentals – trainer must understand core concepts such as phishing, malware, social engineering, password hygiene, and data protection regulations
BR 3.6.3	**Experience & Communication Skills** o Two years' experience in facilitating cyber awareness training as well as being capable of developing or adapting training materials to suit different learning styles and roles. o Effective communication skills.
BR 3.6.4	o One trainer per site, with mascot during the quarterly trainings that must be conducted in all 10 ACSA sites countrywide.

Table 2: Functional Requirements

4 Non-functional Requirements

4.1. Hosting

4.1.1. The solution must be cloud based and hosted in a Tier level 3 or more data centre.

4.1.2. Regulatory and compliance certificates must be provided, e.g. ISO27001.

4.2. Platform performance (Speed & Latency)

4.2.1. The solution must respond quickly when users are working on it, i.e. not click a section and wait for more than 5 seconds.

4.2.2. The solution must cater for bandwidth constraints and geographically dispersed locations.

4.2.3. Users at different sites must have similar experiences when using a tool.

4.3. Scalability

4.3.1. The solution must cater for future growth, e.g. additional employees, functions, and/or users.

4.4. Usability

4.4.1. The solution must be easy to use with minimal user training.

4.5. Reliability & Availability

4.5.1. The solution must be available 24/7 with a minimum availability of 99.8%.

4.5.2. The solution must cater for high availability.

4.5.3. The solution must be backed up such that the training records and data be retained for the entire duration of the service.

4.6. Security

4.6.1. The Service Provider must provide ACSA with their security best practices or controls detailing how they secure their solution.

4.6.2. Assurance - the solution must maintain data integrity and quality. The solution must be a single source of truth in terms of data.

4.6.3. Availability - the solution must be secured to prevent denial of service to ACSA users.

4.6.4. Asset Protection - the solution must protect ACSA data from being viewed by unauthorized personnel.

4.7. Privacy and data ownership

4.7.1. The solution must comply with ACSA's Information Security policies and standards (to be provided to the Service Provider once contract agreement is awarded).

4.7.2. The solution must comply with POPI Act and other related laws or regulations.

4.7.3. All training reports to remain the property of ACSA.

4.7.4. The service provider must provide a certificate of compliance detailing how they comply with data management and/or cybersecurity industry best practice standards, such as ISO 27001, SOC, NIST, etc.

4.8. Solution Accessibility

4.8.1. The solution must be accessible via laptops, desktops, and mobile devices.

4.9. Support & Maintenance

4.9.1. First line support for technical and user issues.

4.9.2. Content support to update course content.

4.10. Look and Feel

4.10.1. The solution appearance and style to align with ACSA Corporate identity and branding.

4.11. Environments (Development, Quality Assurance and Production)

4.11.1. The solution must have the capability to migrate customizations created in a development environment to a quality environment then production environment.

4.12. Integration

4.12.1. The solution must integrate with Outlook and Active Directory to pull user accounts.

5 Roles and Responsibilities

This section describes the roles and responsibility of all relevant stakeholders.

5.1 Service Provider

5.1.1 Deliver and manage the training platform.

5.1.2 Provide technical support and content updates

5.1.3 Conduct phishing simulations and analyse results.

5.1.4 Conduct physical and virtual classroom-based trainings

5.2 Cybersecurity Team

5.2.1 Define training objectives and review content.

5.2.2 Monitor vendor performance and compliance.

5.2.3 Use analytics to inform security strategy.

5.3 HR / Learning and Development

5.3.1 Coordinate onboarding and compliance tracking.

5.3.2 Communicate training requirements to employees.

5.4 ACSA Users

5.4.1 Complete assigned training modules.

5.5 BREACH AND PENALTIES

This section describes the consequences and remediation steps in the event of a breach of contract, non-compliance, or failure to meet agreed-upon cybersecurity awareness training standards.

5.5.1 Breach Scenarios

The following will be considered breaches of the scope of work:

- **Failure to Deliver Training:** Not delivering training modules within the agreed timeline.
- **Incomplete Coverage:** Not training all in-scope employees or failing to meet minimum participation thresholds.
- **Data Breach:** Any unauthorized access, disclosure, or loss of employee data used during training.
- **Inaccurate Reporting:** Providing false or misleading training completion or assessment data.
- **Non-Compliance:** Failure to align with regulatory or internal policy requirements (e.g., POPIA, ISO 27001, NIST).
- **Negligence in Phishing Simulations**: Poorly executed simulations that cause operational disruption or reputational harm. Penalties and remedies

Breach Type	Penalty	Remediation Timeline
Missed Training Deadlines	5–10% service credit deduction per week delayed	7 days
Incomplete User Coverage	20% per untrained user or 10% of contract value	14 days
Data Breach	Full liability for damages + regulatory reporting	Immediate
Inaccurate Reports	Formal warning; repeated offense leads to contract review	5 days
Non-Compliance	Escalation to legal/compliance; potential termination	30 days
Simulation Negligence	Written warning and mandatory review of simulation design	7 days

Table 3: penalties and remedies penalty

5.5.2 Escalation Process

- Level 1: Internal review with vendor or training provider.
- Level 2: Escalation to Cybersecurity Manager and Legal/Compliance.
- Level 3: Contractual penalties enforced, or termination initiated. Documentation & Audit
  - All breaches and penalties must be documented.
  - Reports must be available for internal and external audits.
  - Corrective actions must be tracked and verified.

6 REPORTING

(a) As part of ongoing performance management, ACSA requires that the Service Provider provides the following reports as contained in the table below. These reports will be presented to ACSA on demand and during implementation and ongoing support of the services.

(b) ACSA reserves a right to change a list of reports as requested and will review these on a regular basis, and such changes should not attract additional costs.

(c) The project meetings will be held weekly, and/or on demand for the duration of the contract and arranged by the ACSA Information Security team to discuss the following, but not limited to

6.1 WEEKLY AND MONTHLY REPORTS

#	Report Name	Frequency	Submitted to
1	Participation Metrics	Monthly: Summary dashboards and key metrics. Quarterly: Detailed analysis and trends. Annually: Strategic review and recommendations.	Security Team
2	Assessment Results	Monthly: Summary dashboards and key metrics. Quarterly: Detailed analysis and trends.	Security Team

		Annually: Strategic review and recommendations.	
3	Behavioural Indicators	Monthly: Summary dashboards and key metrics. Quarterly: Detailed analysis and trends. Annually: Strategic review and recommendations.	Security Team
4	Feedback and Engagement	Monthly: Summary dashboards and key metrics. Quarterly: Detailed analysis and trends. Annually: Strategic review and recommendations.	Security Team
5	Compliance and Audit Readiness	Monthly: Summary dashboards and key metrics. Quarterly: Detailed analysis and trends. Annually: Strategic review and recommendations.	Security Team
6	Issues for ACSA's attention.	Monthly: Summary dashboards and key metrics.	Security Team
7	Ad-hoc	Monthly: Summary dashboards and key metrics.	Security Team

Table 4: Reporting Matrix