

Penetration Testing and On Demand Security Assurance Services

Annexure A – Scope of Work

Glossary and Abbreviations

Item	Description
ACSA	Airports Company South Africa
IS	Information Security
ISM	Information Security Management
IP	Internet Protocol
TLS	Transport Layer Security
DLP	Data Leakage Protection
DMARC	Domain-based Message Authentication, Reporting & Conformance
SPF	Sender Policy Framework
DKIM	Domain Keys Identified Mail
SoW	Scope of Work
IOC	Indicator of Compromise
URL	Uniform Resource Locator

Table 1 Glossary and Abbreviations

TABLE OF CONTENTS

1	INTRODUCTION.....	5
1.1	PURPOSE	5
1.2	OBJECTIVE	5
1.3	BACKGROUND	5
2	SCOPE	6
2.1	IN SCOPE	6
2.2	OUT OF SCOPE.....	8
3	EVALUATION CRITERIA.....	8
4	SUPPORT AND MAINTENANCE.....	10
4.2	DEFINITION OF INCIDENTS, PRIORITIES AND SLA'S.....	10
4.3	INCIDENT MANAGEMENT RESPONSE AND RESOLUTION TIMES	11
4.4	INCIDENT LOGGING PROCEDURE.....	11
4.5	BREACH AND PENALTIES	11
5	REPORTING	13
5.1	WEEKLY AND MONTHLY REPORTS	13
5.2	MEETINGS	14
6	APPROVAL	17

TABLES

Table 1 Glossary and Abbreviations	2
Table 2: Functional Requirements	8
Table 5: Incident Response and Remediation Time	11
Table 6: SLA breaches and penalty for incidents	12
Table 7: SLA breaches and penalty for unresolved incidents	12
Table 8: Failure to provide maintenance	12
Table 10: Reporting Matrix	14
Table 11: Meetings Matrix	16

1 INTRODUCTION

1.1 PURPOSE

Airports Company South Africa SOC Ltd hereby invites proposals for the provision of Penetration Testing and On Demand Security Assurance services for the period of 2 years (24 months).

1.2 OBJECTIVE

The aim is to obtain a proposal from a Bidders, in respect of the relevant scope of services, and to evaluate these in order to appoint a Service Provider for the provision of Penetration Testing and On Demand Security Assurance services for the period of 2 years (24 months).at ACSA.

The service provider will be required to fulfil the requirements set out in this RFP. The duration of this contract is anticipated to be for a period of twenty-four (24) months. Upon appointment of the Service Provider, a professional services contract shall be concluded with the Service Provider. ACSA may at any time, terminate the contract or postpone or delay all or any part of the contract upon written notice to the selected Bidder in line with the prescribed process.

1.3 BACKGROUND

ACSA is a critical organ of state, one that interconnects the country with the international economy, operating in an industry that has major appetite for the use of technology not only for profitability but also for providing safety to all stakeholders. In order to pursue its mandate, ACSA has been leveraging technology, digitizing its business operations and bolstering its technology security as our threat landscape and its complexity increases.

ACSA has adopted a hybrid cloud and on-premise hosted architecture that comes with multiple risk considerations and thus requires a security assurance capability for applications, network and holistic infrastructure scrutiny. With the success of modern day advanced persistent attacks, the robustness of and consistent delivery of security controls for perimeter network, core applications and the fundamental Identity and Access Management Infrastructure as part of delivery an Identity Governance and Administration strategy is key. Over and above this, a structured approach to quarterly or bi-annual reviews of focused areas of the ACSA Information Technology, IOT landscape, applications and network security reviews are vital.

This done as part of its overall defence in depth strategy to ensure that multiple controls are applied to secure ACSA as a whole. As the digital dexterity of most company employees has increased along with the adoption of cloud services, the cyber landscape has necessitated the need for ACSA to continuously improve its tactical and strategic approach to cloud and on-premises security. In order to achieve this, there needs to be a more holistic series of on demand security assurance and penetration tests carried out depending on overall applications, networks and infrastructure.

Private & Confidential

The ACSA future looking cyber and information security strategy looks to explore a continued cloud and on-premise aware security architecture with capabilities that leverage the current ACSA investment in M365 security features as well as enables the internally hosted applications and systems. ACSA's cyber and information security journey to date has been focused on multiple approaches to cyber and information security with fragmented solutions that aren't effectively integrated and functioning seamlessly together. To this end, security activities have been focused on deployment of technologies, without a structured effort and approach to a more integrated security strategy. This presents ACSA with an opportunity to see what the market has to offer and how they can support ACSA with On Demand assurance capabilities that adapt to ACSA's ever changing cyber security landscape.

ACSA requires a service provider with a penetration testing team built around a consistent delivery of quality, service, and results, that can be an extension of the ACSA internal team (CISO office, CTO office and the rest of business) and will bring ACSA the foundational support we need to drive our vulnerability and patch management program and thus enable a key component of overall cyber resilience for the organisation.

2 SCOPE

The following sections consist of requirements that are in scope for provisioning of Penetration Testing and On Demand Security Assurance services for the period of 2 years (24 months).

2.1 IN SCOPE

The following are considered an integral part of the business requirements.

ID	REQUIREMENT
BR1	Advanced Manual and Automated Testing Provide ACSA with a detailed testing methodology that is clearly articulated and can demonstrate how vulnerability, threat and patch management along with cyber resilience will be enabled. These may or may not align with security frameworks like OWASP, OSSTMM, PTES, WASC and NIST. Their processes for delivering the penetration and security assurance activities must indicate multiple features for manual and automated penetration testing. Possibility articulated through an estimated ratio of automated testing to manual testing. As an example, the Red Team estimates each security assurance project phase may average about 30% automated and about 70% manual and advanced pen-testing (70 – 30 rule).
BR2	Stakeholder Engagement with constant communication Provide ACSA with scheduled Teams or conference calls, meeting in person along with some sort of structured and secure project management approach to enable the right amount of communication. The project management communications should illustrate the phases of the penetration test, which phase your project sits in, percentage completed, and allow you to easily

	(electronically) communicate with the consultants and project manager(s). One of the most prominent of its capabilities must be informing you/your team when a new finding has been discovered (app, system, estimated impact, estimated criticality, minor finding info), preferably in near real-time. This communicated to the ACSA Cyber SOC team.
BR3	Remediation Assistance & Re-testing <p>Provide ACSA with assurance that you will walk the 24-month journey with them, while ensuring that as each Phase is delivered, there is an outlined methodology that follows a Plan-Do-Check-Act (PDCA) approach to security assurance. Each of the 4 phases will be completed in no more than 6 months to ensure sufficient PDCA enablement is allocated to each of the 4 phases across the total 24-month period. This allowing for a proper methodology to be followed as well as ensuring that there is support from the service provider to ACSA in terms of ensuring remediation and re-testing to ensure successful and ongoing remediation. This work can take weeks or months depending upon the number and complexity of findings. ACSA want to be sure that the successful penetration test service provider will be there to help its technology and cyber security teams during remediation cycles and ensure the team fully comprehends the findings (impact, likelihood, criticality) and is on the right track toward remediation.</p>
BR4	Output For Governance, Risk and Compliance <p>Provide ACSA with assurance that you will walk the 24-month journey with them, while ensuring as each Phase is delivered, at least 6 months are allocated to each of the 4 phases across the 24-month period. ACSA expects the service provider to deliver penetration testing results in a format that's manageable for us as an organisation, such as XML or CSV, for ingestion into our GRC solutions or be viewed from the service providers customer reporting portal. Expectations to at least provide results in Excel format enabling an optimized way to manage ACSA findings and ensure consistent findings can be effectively managed</p>
BR5	Management, Data Analysis, Operations and Reporting <p>Ensure that the ACSA is provided the best skills locally to examine, analyze and report on the data collected during the penetration testing and security assurance activities along with identifying remediation steps. This followed by summarizing of the results of the tests, including what vulnerabilities were detected and exploited and how to fix them, in a report for company management to consume and make decisions on. Any online or cloud solutions utilized for purposes of reporting ACSA specific information, and progress management should be accessed through Role-based administration, Role-based graphical user interface (GUI) and Multi-Factor Authentication login.</p>
BR6	Deployment and Integration <p>Ensure that ACSA is enabled with all required integration to make the Penetration testing and security assurance activities a success. This could include but is not limited to considerations</p>

Private & Confidential

	for threat intelligence sharing, API integration, SIEM integration, Identity provider integration, Cloud access security broker (CASB) integration and other integration and deployment and support.
BR7	Governance Alignment Ensure adherence to ACSA Enterprise, Cyber and Information Security governance, policies, standards, and guidelines
BR8	Continuous Improvement Advise and recommend improvements to the overall Cyber and Information Security efforts within ACSA, whether related to strategy, framework, policy or any other improvement considerations.

Table 2: Functional Requirements**2.2 OUT OF SCOPE**

The requirements that are not explicitly defined in in this scope of work.

3 EVALUATION CRITERIA

1. Evaluation Criteria			
4.1 Administrative/ Mandatory Evaluation Criteria		Yes	No
4.1.1	Bidders must provide relevant Accreditation and/or Certification for the proposed Penetration Testing and On Demand Assurance Service.		
4.1.2	Bidders must provide relevant Methodology for the proposed Penetration Testing and On Demand Assurance Service.		
4.1.3	The Bidder must provide the certification for any cloud environments that will be utilized ensuring that they are certified in the following (SOC-2 or ISO 27001)		
4.1.4	Minimum of three (3) contactable reference(s) letters where a Penetration Testing and On Demand Assurance Service was successfully implemented. (The service provider should have provided such a service for a minimum of 3 years)		

Private & Confidential

No.	Functional / Technical Criteria	Max	Min
4.2	Implementation Plan	30	20
4.2.1	<p>The Bidder shall provide a Service Implementation Plan. The Service Implementation Plan will be evaluated by scrutinizing the implementation methodology provided by the bidder. The implementation methodology should provide the following artefacts:</p> <ol style="list-style-type: none"> Executive Overview Major Tasks or Milestones Implementation Schedule (Across 4 Phases in Scope of Work) Planning and Penetration Testing Approach Remediation and Re-Testing Approach The Implementation Plan must bear evidence of a complete Project Management Life Cycle Reporting areas and mechanism/s and the frequency thereof during project implementation. <ul style="list-style-type: none"> If all the criteria (1 to 7) set out above are evident in the Bidder's submission and solution is set up in less than 2 months. [30] If all the criteria (1 to 7) set out above are evident in the Bidder's submission and solution is set up within 2 to 3 months. [20] Incomplete submission by the Bidder; OR if the Bidder solution will be set up in above 3 months (1 to 7). [0] 	30	20
	Experience in delivering Penetration Testing and On Demand Assurance Services	40	30
4.3	Experience in meeting ACSA's requirements		
4.3.1	<p>The Bidder needs to provide the High-Level Solution Architecture detailing the Penetration Testing and On Demand Assurance Service Components and how they will interface with ACSA internal and public facing assets. The following principles being at the forefront:</p> <ol style="list-style-type: none"> Penetration testing Should be Agile, Yet Consistent Over Time The Penetration testing Process Should be customized to ACSA yet based on a standard approach providing best practice guidance A focus on automation from penetration testing team to assist with administrative tasks while providing insights to ACSA for decision making A focus on ACSA skills development as part of the process, enabling penetration testing talent, improved and streamlined processes, better understanding of technology, and improved culture to ensure most value out partnership. <ul style="list-style-type: none"> If 100% (4 out of 4) of the criteria set out above are evident in the Bidder's submission, including principle alignment for all SOW business requirements. This must include a proposed high level solution architecture. [40] 	40	30

Private & Confidential

	<ul style="list-style-type: none"> If 50% (2 out of 4) of the criteria set out above are evident in the Bidder's submission, including principle alignment for all SOW business requirements. This must include a proposed high level solution architecture. [30] Below 50% (Below 2 out of 4) of the criteria set out above are evident in the Bidder's submission, including principle alignment for all SOW business requirements. This must include a proposed high level solution architecture. [0] 		
4.4	Maintenance Plan for delivery of the service	30	20
4.4.1	<p>The Bidder must submit a maintenance plan and/or a draft Service Level Agreement that supports its capability in supporting and maintaining the delivery of the Penetration Testing and On Demand Assurance Service</p> <ul style="list-style-type: none"> The Bidder has provided a maintenance plan and draft SLAs.[30] The Bidder has provided a maintenance plan or draft SLAs. [20] The Bidder has not provided a maintenance plan or draft SLAs. [0] 	30	20
Total		100	70

4 SUPPORT AND MAINTENANCE

This section describes what Support and Maintenance entail in general and further describes what maintenance entails for ACSA.

ACSA requires a Penetration Testing and On Demand Security Assurance service from a Service Provider as described below:

- 4.1.1 Day to day support activities to ensure that any issues with the software, operations, governance activities or any other factor related to its Security Assurance operational efficiency to achieve required business requirements
- 4.1.2 The Service Provider will be required to respond to and remediate all issues related to the Penetration Testing and On Demand Security Assurance service and its functioning.
- 4.1.3 The response and remediation times depicted below must be adhered to. This will form part of the SLA's that will be agreed to between the Service Provider and ACSA.

4.2 DEFINITION OF INCIDENTS, PRIORITIES AND SLA's

Priority 1: Total system failure

Priority 2: Partial system failure with minimum monitoring functionality

Private & Confidential

Priority 3: Non-critical fault/failure logged at night or over the weekend. It has no impact on the operations of the airport

Priority 4: Minor incidents or move/change or installation of new item

4.3 INCIDENT MANAGEMENT RESPONSE AND RESOLUTION TIMES

Incident management response and remediation times for (Office Hours, After Hours, Weekends and Public Holidays)			
	Response	Restoration	Update Feedback
P1	15min	2hrs	30min
P2	30min	4hrs	1hr
P3	2hrs	8hrs	2hrs
P4	4hours	24hrs	8hrs

Table 3: Incident Response and Remediation Time

4.4 INCIDENT LOGGING PROCEDURE

ACSA requires the Service Provider to adhere to the following incident logging procedure:

- 4.4.1 All security incidents must be logged with ACSA service desk via email, telephone or on the self-service web portal. The incident status must be updated regularly depending on the priority of the incidents until resolution is met;
- 4.4.2 All security incidents must be updated with a detailed resolution before closure. The Service Provider must notify the service desk immediately on resolution of the incident.

4.5 BREACH AND PENALTIES

The following penalties as detailed out in the next sections shall apply in an event of breach of service levels as agreed.

Service Level Agreement (SLA) breach	Penalty
P1 Incidents are resolved within one hour after SLA time lapsed for two consecutive times in one month across any of the sites in scope	20 % of the monthly fee will be deducted per invoice up to 60% in one contractual year thereafter termination procedures will be implemented.

Private & Confidential

Incidents are resolved within two hours and beyond after SLA time lapsed for three consecutive times in one month across any of the sites in scope	30 % of the monthly fee will be deducted up to 60% in one contractual year thereafter termination procedures will be implemented.
If a Bidder misses Incident Management SLA's in any 3 consecutive months across any sites in scope	50 % of the monthly fee will be deducted.
If a Bidder misses Incident Management SLA's consecutive in any 4 months across all site's ins cope – will be deemed as a material breach, and the contract will be referred for performance management and termination procedures	50 % of the monthly fee will be deducted.
Five or more missed SLA's across all sites in scope on or across Acquisition Management, IMACDs; Asset Management; Configuration Management; Maintenance and Repair in a measuring period	20% of the monthly fee will be deducted per invoice

Table 4: SLA breaches and penalty for incidents

The following **SLA penalties** shall apply when the Service Provider does not comply with the agreed SLA.

SLA Breach	Penalty
Failure to comply to agreed SLA	10% of contract capital value withheld

Table 5: SLA breaches and penalty for unresolved incidents

Failure to perform Maintenance and/or services in accordance with the scheduled dates or Priority list and SLA agreements shall result in the following penalties:

Maintenance	Penalty
Maintenance not done or proof of carrying maintenance out not submitted.	No payment of invoice.

Table 6: Failure to provide maintenance

5 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:

5.1 WEEKLY AND MONTHLY REPORTS

#	Report Name	Frequency	Content and Format	Submitted to
1	Service Request Status (not incidents)	Every day of the week and a consolidated version for all 4 weeks on the last day of the month end	Status of new enhancements, fixes, requests	Security Team
2	Weekly Service Review Reports for open, closed incidents, status of each incident in terms of SLA.	Every day of the week and a consolidated version for all 4 weeks on the last day of the month end.	Open and closed incidents. Status of each incident in terms of SLA. Reason of SLA breaches if any and measures that will be put in place to avoid breach.	Security Team
3	Maintenance reports: report against the maintenance schedule. This will include issues	Every day of the week and a consolidated version for all 4 weeks on the last day of the month end	Modules worked on. Issues discovered per module and how they were resolved.	Security Team

Private & Confidential

#	Report Name	Frequency	Content and Format	Submitted to
	picked up during their maintenance.		Details on any general maintenance work carried out.	
4	Monthly Systems Availability Report against the ACSA required target of 99.9 % uptime.	Last day of the month	System availability System downtime	Security Team
5	Preventative work done.	Monthly (i.e., 4 th of the following month).	Report on various preventative work as per section 4.2 above.	Security Team
6	Issues for ACSA's attention.	Last day of the month	Any relevant issues that needs to be brought to ACSA's attention by the Service Provider.	Security Team
7	Ad-hoc	As and when required	Ad-hoc, depending on the request at hand.	Security Team

Table 7: Reporting Matrix**5.2 MEETINGS**

As part of ongoing performance management and project delivery, ACSA requires that the Service Provider attend monthly and weekly meetings.

Private & Confidential

Frequency	Meeting Name	Standing Agenda	Participants and Role	Prior documents to be submitted by the Service Provider	Documents to be produced after meeting
Monthly	Project Board Meeting	<p>Discuss all aspects of Monthly reports as stated in.</p> <p>Discuss Project Costs, Timeline, Risks, Issues, Resources, etc.</p> <p>Discuss all deliverables produced to trace successful delivery on Business Requirements.</p>	IT PMO, Service Provider's Service Delivery Manager, ACSA contract owner, ACSA Technical Lead, Project Sponsor, Other Stakeholders per Invitation	<p>Project Board Pack including Planned Presentation.</p> <p>Previous Minutes.</p> <p>Monthly Reports.</p>	<p>Attendance Register</p> <p>Minutes of meeting including updated Action items, Decisions Made, Risk & Issue Log</p> <p>Acceptance of deliverables</p>
Weekly	Progress Meeting	<p>Progress Reporting, Performance Management, Security Posture, Security Incidents/Threats Reporting, Exception Reports, Risk Register, Areas of Focus, discuss high level service deliverables / milestones, Timelines and delivery, Environment Risks / Issues / Assumptions,</p>	Service Provider's Service Delivery Manager, Technical Resources and ACSA Security team	<p>Minutes of Previous Meeting.</p> <p>Updated Risk and Issue Log.</p>	<p>Attendance Register.</p> <p>Minutes of Meeting.</p> <p>Acceptance of deliverables.</p>

Private & Confidential

Frequency	Meeting Name	Standing Agenda	Participants and Role	Prior documents to be submitted by the Service Provider	Documents to be produced after meeting
		Contractual/Financial and Governance, General and all other requirements related to the services. Internal and External Audits of the Services in Scope.			
Ad-hoc	Ad-hoc	Ad-hoc	Stakeholders as and when required	Ad-hoc	As agreed by all parties
Monthly	Operational Meetings	Review system operations, vendor performance	Service provider & IT Operations Department	Operational reports	Minutes, attendance register.

Table 8: Meetings Matrix

Private & Confidential

6 APPROVAL

THE MATTER IS SUBMITTED FOR CONSIDERATION BY:

COMPILED BY:

Name: Nonhlanhla Manana
Designation: Cyber Security Administrator
Date: _____

Signature

SUPPORTED BY:

Name: Thipe Khaole
Designation: Group Manager: Information Security
Date: _____

Signature

APPROVED BY:

Name: Mthokozisi Mncwabe
Designation: Chief Information Officer
Date: _____

Signature