AIRPORTS COMPANY
SOUTH AFRICA

ANNEXURE A

Compliance Management Solution

Scope of Work

Document Review and Distribution

This document will be managed and controlled in terms of the ACSA IT Project Management Office document management procedure.

Glossary

Acronym	Description
ACSA	Airport Company South Africa
AVSEC	Aviation Security
ES & C	Enterprise Security & Compliance
IT	Information Technology
RFI	Request For Information
SACAA	South African Civil Aviation Authority
SOW	Scope of Work

Table Of Contents

AIRPORTS COMPANY
SOUTH AFRICA

1. Introduction:

Airports Company South Africa SOC Ltd (ACSA) hereby invites suitably qualified and experienced service providers to submit bid proposals for the implementation. The bid proposals must clearly indicate how the solution will be implemented, and also how it will be supported and maintained once rolled out in Operation.

1.1 Objective

The objective of the project is to implement a cloud-based Compliance Management Solution Compliance that primarily will enforce compliance and reduce the risk of breaching laws, regulations, and standards applicable to the business.

1.2 Background

Enterprise Security & Compliance is committed to building and maintaining compliance in its processes. Currently, there is no automated solution that is used to manage risks and compliance across the enterprise. The solution should support the enterprise compliance framework which is a structured set of guidelines that details an organization's processes for maintaining accordance with established regulations, specifications or legislation. The unavailability of the solution makes it difficult for the department to conform to the organization's commitment to ensure compliance and risk mitigation across all business areas.

2. Scope

The following activities will be in scope for the project:

a) Procurement of the Compliance Management Solution
b) Installation, configuration, commissioning and integration of the solution.
c) User acceptance testing.
d) User training.
e) Handover the solution to operations.

3. Business Requirements:

Listed below are business requirements that have delivered and met by the solution.

3.1 Functional Requirements:

The new solution must be able to deliver the following functional requirements.

	Compliance Requirements	
REQ #	**High Level Requirement**	**Detailed Requirement**
BR1	**Reporting**	1.1. The system must allow the user to be able to filter, customise and draw the reports and be able to export report to the acceptable Microsoft programme e.g. – pdf, spreadsheet. Examples of reports: 1.1.1 HEAT maps report 1.1.2 Compliance risk per treatment plans status 1.1.3 Compliance risk movement report 1.1.4 Non-compliance status 1.1.5 Legislative updates 1.1.6 CRMP for specific Act 1.1.7 Compliance requirements per Act
		1.2. The system must provide library of all past reports.
BR2	**Compliance Universe and Compliance Risk Management Plan (CRMP)**	2.1. The system must be able to house the list of regulatory/compliance universe of the company. It should allow a user to develop Compliance Risk Management Plans (CRMP) for every legislation in the universe. 2.1.1 Be able to store and access the actual copies of acts, regulations, standards, and best practices from the system. 2.1.2 Categorize the legislatives into core, secondary and topical. 2.1.3 Categorize the legislatives into core, secondary and topical. 2.1.4 Allow user to assign regulatory risk to risk owners and assign task/corrective actions. 2.1.5 The system must be able to provide the user with a summary of compliance information for a full act or multiple acts assigned to them (act owners)

		2.2. The system must be able to provide an overview page of an act or multiple acts an 'act owner' is responsible for. The overview page must show the following fields: 2.2.1 Act or Legislative name 2.2.2 Act Owner 2.2.3 Reason for applicability 2.2.4 Overall Strategic Objective of a Legislation/s 2.2.5 Responsible department 2.2.6 Legislation type: National, Provincial or By-law 2.2.7 Number of conditions 2.2.8 Percentage (%) Complied: (0% - 100%) 2.2.9 Category: Core, Secondary, Tropical 2.2.10 Progress Update 2.2.11 Legislative Change (s)
BR3	**Legislative Updates**	3.1. Provide a real time monitoring and update notification of all regulatory developments derived from the regulatory sources in all areas of South African law applicable to the company requiring further scrutiny and/or action. 3.1.1 The notification should comprise of summary of the regulatory development and attached copy of the government gazette of a hyperlink to the site. 3.1.2 User should be able to assign tasks to certain users to participate in comment submission to the government or review internal policies and processes to ensure compliance with new regulatory requirements. 3.1.3 The task can be given an order of priority and a due date. Once assigned, the task assignee can update the assigner of progress via the system.
BR4	**Compliance Monitoring**	4.1. The system must allow the compliance Administrator to create and monitor a yearly audit plan. The system should allow the user to do the following: 4.1.1 Create a monitoring schedule example; audit schedule inspections relating to the requirements of legislations, relevant regulations, and organizational procedures or policies. 4.1.2 The audit monitoring schedule shall include topics such as name: link, legislative conditions, area of review, scope, review criteria, auditee, level of assurance, frequency, start and end date,

		responsible person and status of review example; not due, in progress, complete, overdue, deferred, cancelled or on hold. 4.1.3 Populate reasons for deferred, cancelled, on hold and overdue audits on a text free tab 4.1.4 Compile monitoring scope and information request list 4.1.5 Compile an information request list, containing; items to be audited on, information requested, response status (yes, no or not applicable), auditee feedback and compliance remarks. 4.1.6 Complete and forward compliance audit draft report for reviewal and provision of corrective action plan from the relevant department/site. 4.1.7 The system should allow the user to rate the audit findings according to the company's risk matrix. 4.1.8 Receive corrective action, consolidate the final report, and send to the auditee, which constitutes the official report of the audit. 4.1.9 Document corrective actions and the system should allow the user to track action plans and update were required
BR5	**Incident, Accident, non-compliance & non-conformance occurrences**	5.1. The system should have the capability to allow record incidents Incident, Accident, non-compliance, and non-conformance occurrences. 5.1.1 All incidents must be link to a non-compliance or legislation that is housed in a regulatory universe or company's policy or procedure. 5.1.2 All occurrences should have a unique system generated reference number. 5.1.3 The investigation page must have the below: 5.1.4 Incident logged date 5.1.5 Logger details 5.1.6 Verifier details 5.1.7 Root cause 5.1.8 Recommendation 5.1.9 Corrective action applied. 5.1.10 Save/complete button. 5.1.11 Assign closure. 5.1.12 Risk 5.1.13 Location grid (location where incident took place)

<table>
<tr><td></td><td></td><td>5.2. The system must allow user to log the occurrence based on the relevant category of involved items (e.g., property, facility, equipment, vehicle, emergency phase, wildlife etc.)</td></tr>
<tr><td></td><td></td><td>5.3. The system must allow user to assign, action, review and report on occurrences on an end-to-end process with the below type of users:
5.3.1 Compliance administrator- user must be able to load, review and update compliance universe and CRMP.
5.3.2 Act Owner- user must be able to rate the impact and likelihood of non-compliance to relevant legislation. Be able to load compliance controls to legislation.
5.3.3 Logger/investigator- user must be able to log occurrences, upload comprehensive investigation reports and upload supporting files.
5.3.4 Verifier- user should be able to review all occurrences logged within a particular department.
5.3.5 Closer- user to ensure that the report provided by the logger/ investigator has sufficient information to close the occurrence.</td></tr>
<tr><td></td><td></td><td>5.4. The system should also allow users to categorize the incident as per the following:
<table>
<tr><td>Level of Non-conformance</td><td>Priority</td><td>Action</td></tr>
<tr><td>Catastrophic</td><td>High</td><td>Immediately</td></tr>
<tr><td>Critical</td><td>Medium to High</td><td>24hours</td></tr>
<tr><td>Significant</td><td>to Low</td><td>3 days</td></tr>
<tr><td>Moderate</td><td>Low</td><td>7 days</td></tr>
<tr><td>Minor</td><td>Low</td><td>Discretionary</td></tr>
</table></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>BR6</td><td>Security quality control processes automation</td><td>6.1. The system must be able to automate the security quality control. processes across the following security control categories:
6.1.1. People, processes, and systems
6.1.2. Equipment
6.1.3. Infrastructure
6.1.4. ‘Vehicle
6.1.5. Perimeter/ Barriers
6.1.6. Access Gates
6.1.7. Vehicle Security Checkpoints</td></tr>
</table>

		6.1.8. Passenger Security Checkpoints 6.1.9. Staff and Crew Security Checkpoints 6.1.10. General Aviation Gates 6.1.11. Valuable Cargo Access gates 6.1.12. Aircraft Catering 6.1.13. Training 6.1.14. Incident Reporting (Major and minor incidents) 6.1.15. Security Breaches
BR7	**System functionality**	7.1. The system must have the following functionality at a minimum: 7.1.1. User Management-Manage the registration of users on the system according to pre-defined user access rights. 7.1.2. Capturer- the person who completes the audits. 7.1.3. Scheduler – the person who captures the assessment on the system. 7.1.4. Report viewer – the person who has report access to the system. 7.1.5. System Owner – the person responsible for the overall procurement, development, integration, modification, operation, maintenance, and retirement of the system 7.1.6. Site Administrator – the system who administers the system. 7.1.7. Reporting – manages the reports generated by the system. 7.1.8. Assessment reports 7.1.9. Dashboard reports per type of security control category per airport, per incident, per date 7.1.10. Non-compliance / non-conformance reports 7.1.11. Inspections completed per auditor per month. 7.1.12. Findings per location 7.1.13. Action reports 7.1.14. Raw data 7.1.15. Miscellaneous reports. 7.1.16. Schedule Management – manage the completion of the quality assessment by the users. 7.1.17. Audit Management – manage the completion of the quality assessment by the users. 7.1.18. Questionnaire Administration management – manage the assessment questions centrally across all airports for standardization.

BR8	**Audit assessment Management**	8.1 The system must validate if an assessment is incomplete when a user tries to submit. 8.2 The system must allow the user to complete outstanding actions assigned to an assessment or audit. 8.3 The system must enable workflow approval for the review of assessment or audits prior to reporting. 8.4 The system must allow the Scheduler to schedule assessments to users at each airport. 8.5 The system must allow the Questionnaire administrator to manage the Security assessment questions online. 8.6 The system must display audits that are scheduled to required users via workflow. 8.7 The system must generate notifications when an assessment is overdue.
BR9	**Image Management**	9.1 The system must allow the user to capture images. 9.2 . The system must enable the user to select options from embedded images. 9.3 The system must update the camera upload functionality with embedded paintbrush functionality to allow users to edit pictures before saving.
BR10	**System access management**	The system must allow access to authorized users only.
BR11	**User profile management**	The system must manage user registrations and user profiles
BR12	**Server synchronization**	11.1. The system must allow the user to work offline and enable the user to synchronize to the server. 11.2. For dead Wi-Fi zones, the system should allow the ability to save an inspection and synchronize when in live Wi-Fi zone.
BR13	**Mobile platform portability**	The system should be available in a range of mobile device platforms.
BR14	**Camera upload functionality**	The system must update the camera upload functionality with embedded paintbrush functionality to allow users to edit pictures before saving.
BR15	**System integration**	The system must be designed in such a way that it can be integrated to other ACSA Systems

5.4 Non-Functional Requirements

The system must adhere to the following non-functional requirements:

5.4.1 Hosting

5.4.1.1 The solution must be hosted on Cloud.

5.4.2 Platform performance (Speed & Latency)

5.4.2.1 The solution must respond in less than 5 seconds. The Service Provider to provide the estimated bandwidth requirement.

5.4.3 Scalability

5.4.3.1 The solution must cater for 10% growth per year in terms of additional leases, functions and/or users.

5.4.4 Usability

5.4.4.1 The solution must be web based.

5.4.5 Reliability & Availability

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

5.4.5.2 The solution must cater for high availability.

5.4.5.3 The solution must be able to backup daily and should also have offsite storage for backups.

5.4.5.4 The solution must be able to recover deleted data from backups. The recovery point objective (RPO) must be at most one (1) day.

5.4.6 Security

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

5.4.6.2 The solution must ensure that data is transmitted in a non-readable format (encrypted) and has strong key management. The solution must provide encryption capabilities for stored data to ensure that data at rest is protected. For example, Transport Layer Security (TLS) must be version 1.2 or up.

5.4.6.3 The solution must also detect anomalies in functionality, user accessibility, traffic flows, and tampering.

5.4.6.4 Authentication – the solution must uniquely identify users and authenticate them. Administrator accounts must be segregated from normal user accounts.

5.4.6.5 Authorization – the solution must enable users and/or role-based permissions to be configured in order to control what solution features and data users can access.

5.4.6.6 Audit – the solution must keep an audit trail of all activities performed in the solution (includes but not limited to the following: who created, updated, and deleted (must be authorized by super users) the record, with time and date stamp.

5.4.6.7 Assurance – the solution must maintain data integrity and quality. The solution must be a single source of truth in terms of data and calculations.

5.4.6.8 Availability – the solution must be secured to prevent denial of service to ACSA users. It must also provide threat protection.

5.4.6.9 Asset Protection – the solution must protect ACSA data from being viewed by unauthorized personnel.

5.4.6.10 The solution must limit access to suspicious visitors and monitor for traffic spikes to prevent overloads like DDoS attacks.

5.4.7 Privacy and data ownership

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

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

5.4.7.3 All data to remain the property of ACSA.

5.4.7.4 The Service Provider must issue ACSA with a certificate of compliance or external audit reports detailing how they comply to data management and/or Information Security Management, e.g., ISO 27001 or SOC.

5.4.8 Solution Accessibility

5.4.8.1 The solution must be accessible in one central platform.

5.4.8.2 The solution must be accessible via laptops and desktops.

5.4.9 Disaster Recovery

5.4.9.1 The solution must have an alternative way to ensure business continuity in cases where there is an unfortunate event of downtime.

5.4.9.2 The solution disaster recovery must be tested at least once annually and also be audited by an external audit company.

5.4.10 Local Support

5.4.10.1 First line and second line support for the solution must be based in South Africa (international support can form part 3rd line support).

5.4.11 Look and Feel

5.4.11.1 The solution must be white labelled to align with ACSA Corporate identity and branding.

5.4.12 Environments (Development, Quality Assurance and Production)

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

5.4.13 Infrastructure and data storage

5.4.13.1 Ensure enough space that will be able to store all the uploaded documents of all sizes and provide the different space options.

5.4.13.2 The Service Provider must provide the infrastructure specifications for their system to function optimally. The following must be provided:

5.4.13.2.1 Servers (must include for all servers)

5.4.13.2.2 Storage

5.4.13.2.3 Network (e.g., ports to be opened, bandwidth required).

5.5 Service Management, Preventative and Corrective Maintenance (annexure B).

For a detailed scope of work, please see **Annexure A**.

Annexure B

Refer to annexure B for Service Management, Preventative and Corrective Maintenance (to accompany the SOW).