AIRPORTS COMPANY SOUTH AFRICA

Audit Management System

Scope of Work

Glossary

Acronym	Description
ACSA	Airports Company South Africa
AMS	Audit Management System
BR	Business Requirement
CTIA	Cape Town International Airport
CM	Change Management Requirement
IIA	Institute of Internal Standards
KSIA	King Shaka International Airport
NFR	Non-Functional Requirement
ORTIA	OR Tambo International Airport
PMR	Project Management Requirement
SG	Solution Guidelines
TR	Training Requirement

Table 1: Glossary

AIRPORTS COMPANY SOUTH AFRICA

TABLE OF CONTENTS

AIRPORTS COMPANY SOUTH AFRICA

1. Introduction

1.1. Purpose:

Airports Company South Africa (ACSA) is inviting bidders to submit proposals for the implementation, support & maintenance of an Audit Management solution that will support the Internal Audit functions. This system will aid in audit planning, audit scheduling, documenting findings, and initiating investigations. It will also help manage compliance, facilitate walkthroughs, and perform data analysis, allowing ACSA to identify weaknesses, inefficiencies, and non-compliance issues and take corrective actions as needed. The system must comply with the latest global IIA standards.

1.2. Project Objectives

The objective of the project is to deliver a solution that will do, among other things, the following:

a. Audit Planning
b. Scheduling
c. Execute Audits
d. Track audit progress
e. Initiate Investigations
f. Document findings
g. Enforce compliance

1.3. Scope

The following milestones are in scope for the project:

a. Software license procurement, installation of the new solution, hardware & software
b. Configuration, and customization of the new solution to suit ACSA environment
c. Data migration.
d. Integration
e. Solution Testing
f. User Training
g. Deploying solution to production environment
h. System's post go-live support
i. Handing over the solution to Operations

2. Functional Requirements

The following are functional requirements that need to be delivered by the system. The Audit Management System (AMS) is expected to help streamline the audit process, improve efficiency, and ensure better compliance and reporting. Below are the internal audit requirements that shall be delivered by the system.

BR #	Requirement Description	Available	Not available, but can be developed	Priority P1/P2/P3
BR 2.1	**Risk Identification, Assessment & Prioritization**			
BR 2.1.1	Risk Identification & Assessment			
BR 2.1.1.1	The system shall enable the user or auditor to define risk categories, criteria, and thresholds.			**P1**
BR 2.1.1.2	The system shall be capable of collecting historical, current, and external data relevant to a risk.			**P1**
BR 2.1.1.3	The system shall include templates, checklists, and collaboration features to assist in identifying potential risks.			**P1**
BR 2.1.1.4	The system shall enable the user to assign likelihood, impact, and exposure scores to each risk and calculate a total risk score.			**P1**
BR 2.1.1.5	The system shall be able to utilize risk matrices or heat maps to prioritize high-risk areas for attention.			**P1**
BR 2.1.1.6	The system shall enable the user to assign mitigation actions, responsible parties, and timelines.			**P1**
BR 2.1.1.7	The system shall enable the user to continuously track and reassess risks, adjusting mitigation strategies as needed.			**P1**
BR 2.1.1.8	The system shall maintain a risk register and generate risk reports for stakeholders.			**P1**

BR 2.1.2	Risk Prioritization			
BR 2.1.2.1	The system shall enable the user to define risk assessment criteria for likelihood, impact, and risk appetite.			**P1**
BR 2.1.2.2	The system shall enable the user to identify and list all risks in a centralized Risk Register.			**P1**
BR 2.1.2.3	The system shall enable the user to evaluate each risk's likelihood and impact using predefined scoring systems.			**P1**
BR 2.1.2.4	The system shall generate a risk heat map or risk matrix to visually prioritize risks based on their likelihood and impact.			**P1**
BR 2.1.2.5	The system shall enable the user to rank risks by risk exposure to identify high, medium, and low-priority risks.			**P1**
BR 2.1.2.6	The system shall incorporate organizational risk appetite to flag risks that exceed acceptable thresholds			**P1**
BR 2.1.2.7	The system shall enable the user to assign owners and mitigate actions for high-priority risks, ensuring accountability.			**P1**
BR 2.1.2.8	The system shall enable the user to regularly review and adjust priorities as the risk landscape evolves.			**P1**
BR 2.2	**Audit Planning**			
BR 2.2.1	Defining audit objectives			
BR 2.2.1.1	The system shall enable the user to set objectives, goals, outcomes and boundaries for the audit.			**P1**
BR 2.2.1.2	The system shall enable the user to track the objectives and scope throughout the audit lifecycle.			**P1**
BR 2.2.1.3	The system shall enable the user to link the objectives to specific audit tasks.			**P1**
BR 2.2.1.4	The system shall enable the user to specify departments, processes, or systems to be audited.			**P1**

BR 2.2.1.5	The system shall enable the user to define what is not part of the audit scope.			**P1**
BR 2.2.2	Audit Checklist:			
	The system shall enable the user to create checklists based on audit standards or guidelines. These will serve as the audit framework.			**P1**
BR 2.2.3	Assigning Auditors			
	The system shall enable the user to assign roles and responsibilities to auditors to track team members, timelines, and milestones.			**P1**
BR 2.2.4	Scheduling an Audit:			
BR 2.2.4.1	The system shall enable the user to schedule audit tasks			**P1**
BR 2.2.4.2	The system shall be able to send reminders or notifications to auditors about upcoming deadlines.			**P1**
BR 2.2.5	Audit Preparation (Pre-Audit Activities)			
BR 2.2.5.1	The system shall enable the user to create an audit checklist that specifies the steps, procedures, and tests that need to be followed during the audit.			**P1**
BR 2.2.5.2	The system shall enable the user to upload and organize all relevant documentation (e.g., financial statements, compliance reports, policies, procedures, prior audit reports) for auditors to review.			**P1**
BR 2.2.5.3	The system shall enable the user to access documents remotely and securely.			**P1**
BR 2.2.5.4	The system shall enable the user to notify stakeholders (such as department heads or relevant teams) about the audit, including preparation requirements.			**P2**

BR 2.3	Audit Execution			
BR 2.3.1	The system shall enable the user to log their observations, findings, and evidence in real-time, ensuring all information is captured electronically.			**P1**
BR 2.3.2	The system shall support mobile access, allowing auditors to update findings on the go.			**P1**
BR 2.3.3	The system shall enable the user to communicate with management, department heads, and other stakeholders			**P1**
BR 2.3.4	The system shall enable the user to track and manage queries or follow-up requests			**P1**
BR 2.3.5	The system shall provide audit trails, allowing for easy tracking and retrieval of supporting documents, comments, and observations			**P1**
BR 2.3.6	The system shall enable the user to log non-compliance, discrepancies, or risks identified for further investigation or resolution.			**P1**
BR 2.3.7	The system shall enable the user to track the status of the findings and ensure corrective actions are planned and implemented.			**P1**
BR 2.3.8	The system shall enable auditors to categorize and rank findings based on their severity.			**P1**
BR 2.3.9	The system shall enable the user to track meeting notes, actions, and outcomes.			**P2**
BR 2.3.10	The system shall enable collaboration between auditors, management, and other relevant stakeholders. Documents, findings, and comments can be shared, discussed, and reviewed in real time.			**P1**

BR 2.4	Reporting and Finalization			
BR 2.4.1	The system shall enable the user to generate comprehensive audit reports that detail the findings, issues, recommendations, and overall audit conclusions.			**P1**
BR 2.4.2	The system shall provide templates for generating consistent and professional audit reports			**P1**
BR 2.4.3	The system shall track the approval process and allow for comments or edits to be made before finalizing the audit report.			**P1**
BR 2.4.4	The system shall enable the user to share audit reports with stakeholders, management, and other relevant parties			**P2**
BR 2.4.5	The system shall enable the user to track corrective actions			**P2**
BR 2.4.6	The system shall track the progress of corrective actions, ensuring that issues identified in the audit are addressed.			**P1**
BR 2.4.7	The system shall send alerts to managers and auditors about the status of the actions			**P1**
BR 2.4.8	The system shall enable the user to schedule follow-up audits or reviews to verify whether corrective actions have been effectively implemented and whether the issues have been resolved.			**P2**
BR 2.4.9	The system shall enable the user to formally close the audit once all findings have been reviewed, corrective actions implemented, and any follow-up audits completed			**P1**
BR 2.4.10	The system shall ensure that all documentation, reports, and audit records are archived for future reference and compliance requirements			**P1**
BR 2.4.11	The system shall ensure that the records are securely stored and easily retrievable when needed.			**P1**

3. Non-Functional Requirements

The system needs to adhere to the following non-functional requirements.

NFR #	Requirement Description
NFR 3.1	Hosting
	The best environment to host the solution will be determined by the appointed Service Provider
NFR 3.2	Single sign-on capability
	The system shall use the ACSA Ad system for authentication. (either on-prem or cloud)
NFR 3.3	Scalability
	The system shall be capable of scaling up to accommodate future increases per year in terms of additional functions and/or users.
NFR 3.4	Availability
	The Audit Management System shall be operational 24/7/365, with a target availability rate of 99.9%
NFR 3.5	Fault Tolerance
	The system shall be able to operate under partial system failures (e.g., one or more failed components) without losing overall functionality.
NFR 3.6	Recoverability
	The system shall feature robust disaster recovery capabilities to quickly restore operations after a system failure, with clearly defined recovery time objectives (RTO): 24 hours and recovery point objectives (RPO): 4 hours.
NFR 3.7	Usability
	The system's User Interface (UI) shall be intuitive, user-friendly, and be able to accommodate users with varying levels of technical skills.
NFR 3.8	Maintainability
	Modularity: The system shall be designed in a modular fashion, allowing for easy updates, maintenance, and replacement of individual components without affecting the overall system.
NFR 3.8.2	Documentation: Comprehensive, clear, and up-to-date documentation shall be provided to support system maintenance and upgrades.
	Supportability: the vendor support shall include 24/7 technical support with specified maximum response times for different types of issues.
NFR 3.9.	Compliance
	Standards Compliance: the system shall adhere to relevant industry standards, such as ISO/IEC 27001 for information security management
NFR 3.10	Environmental
NFR 3.10.1	**Sustainability**: Design and operation shall minimize environmental impact, promote energy efficiency and using environmentally friendly materials wherever possible.
NFR 3.10.2	**Durability:** The system components shall be robust enough to withstand the physical conditions of the airport environment, including variations in temperature, humidity, and handling.

NFR 3.11	Encryption
NFR 3.11.1	The system shall encrypt all sensitive data at rest and in transit.

4. Project Management Requirements:

The following are project management requirements that must be met by the bidder:

PR #	Requirement Description
PMR 4.1	Project Management Approach
PMR 4.1.1	Utilize project management methodologies, knowledge, skills, tools, and techniques consistent with leading internationally recognized and accepted project management practices such as those contained in the Guide to the Project Management Body of Knowledge (PMBOK) or Prince 2
PMR 4.1.2	Perform project management review and oversight, attend scheduled project meetings, ensure key milestones are achieved by Service provider, ensure all ACSA project governance processes are in place and are being achieved throughout the project
PM 4.2	Define Project Team
	The project manager must be able to define a group of people responsible for executing the tasks and producing deliverables outlined in the project plan and schedule
PMR 4.3	Resource Planning
	The project manager must be able to determine what resources are required to deliver projects and then allocating and scheduling the work based on team capacity
PMR 4.4	Define Project Plan
PMR 4.4.1	Provide project definition and plan, identify major critical milestones, ensure delivery within budget and project deliverables aligned and approved by the ACSA Project Manager.
PMR 4.4.2	Provide, maintain, and update detailed integrated project planning, identify critical path dependencies.
PMR 4.4.3	Approve project plan, critical milestones, budget forecast, and project deliverables
PMR 4.4.4	Schedule and facilitate weekly project meetings to review detailed project plan and critical path dependencies.
PMR 4.4.5	Manage an integrated baselined project schedule, which will include all ACSA and third-party tasks, and all known dependencies.
PMR 4.4.6	Project schedule to include all project milestones, including billing milestones
PMR 4.4.7	Project schedule to be baselined within the first four weeks of project kick off. Any changes to the baseline to be presented to project board for review and approval
PMR 4.5	Manage project progress and execution
PMR 4.5.1	The project manager must be able to track project activities and tasks in MSP to ensure that the project does not go off course or hit any delays or setbacks along the way.
PMR 4.5.2	The project manager must ensure project management activities are carried out and ensure updated communication to project stakeholders is done.
PMR 4.5.3	The project manager must report on project progress, budget, risk, issues

PMR 4.5.4	The project manager reviews and escalate any issues risk etc. for action to higher governance authorities as required
PMR 4.6	Budget Management
	The project manager must be able to manage total projected costs needed to complete a project over a defined period of time
PMR 4.7	Asset Management
	The project manager must ensure all assets are asset tagged and documented prior to installation.
PMR 4.8	Stakeholder Management
	The project manager must be able to do stakeholder identification, analysis, and management to ensure alignment, secures support, identifies risks, enhances decision-making, fosters communication, facilitates adaptation, and contributes to the organization's reputation.
PMR 4.9	Project Governance
PMR 4.9.1	The project manager must be able to enforce project governance to ensure adherence to the procedures and policies that determine how projects are managed and overseen.
PMR 4.9.2	Draft project charter with input from ACSA for sign off by all stakeholders
PMR 4.9.3	Complete all required project artifacts, and ensure approved through required forums and stakeholders – which may include, but is not limited to solution design, test plans, integration plans, migration plans, change controls, communication plans, decommission plan, asset management forms
PMR 4.9.4	All project documentation to be saved in ACSA central document repository
PMR 4.9.5	Minute all meetings within 48 hours of the meeting, list all actions from the minutes in the RAID log
PMR 4.9.6	Include end to end asset management requirements aligned to ACSA policy and procedure in scope of deliverables – this includes asset tagging of ALL assets, completing asset capitalization form and submitting such forms with invoices to enable payment
PMR 4.10	Project reporting
	The project manager must provide weekly project reports, and monthly Steerco reports to the project board in ACSA format.
PMR 4.11	Project Close Out
	The project manager must ensure that all activities required to close out the project are carried out to ensure that the project is properly closed out and seamlessly handed over to operation without incomplete activities.

5. Training:

The Service Provider is required to provide comprehensive training to ensure smooth adoption and effective use of the system. This structured training plan ensures that the Service Provider covers all necessary aspects of training and equips ACSA staff with the skills required for successful system implementation and ongoing operations. Let me know if you need further adjustments. The training should cover the following areas:

TR #	Requirement Description
TR 5.1	**Training Objectives**
TR 5.1.1	The Service Provider shall ensure that all relevant stakeholders (internal staff, end-users, and administrators) are proficient in using the system.
TR 5.1.2	Equip users with the skills to utilize the system's full functionality
TR 5.1.3	Empower users to perform tasks efficiently and minimize the risk of errors or security breaches.
TR 5.1.4	Enable administrators to manage the system's configurations, user access, and ongoing maintenance.
TR 5.2	**Types of Training:**
TR 5.2.1	End-User Training:
	Training for those who will be using the system regularly, including procurement, risk management, and compliance teams. • **Key areas**: Basic system navigation, task execution (e.g., data entry, report generation), and troubleshooting common issues.
TR 5.2.2	System Administrator Training:
	In-depth training for the IT staff or system administrators who will be responsible for managing, configuring, and maintaining the system. • **Key areas**: System setup, user management, data integrations, backup and recovery procedures, and advanced troubleshooting.
TR 5.2.3	Super User Training:
	Training for individuals who will act as in-house experts and support end-users in their day-to-day operations. • **Key areas:** Advanced features, customization options, and troubleshooting support.
TR 5.3	**Training Deliverables:**
TR 5.3.1	Training Materials:
	Provide comprehensive training documentation, guides, and user manuals, tailored to the roles of the different user groups. • Include step-by-step instructions, screenshots, and best practices for using the system.
TR 5.3.2	Online and In-person Training Sessions:
	Depending on the preference of the organization, training should be provided through a combination of virtual (e.g., webinars, video tutorials) and in-person sessions.
TR 5.3.3	Knowledge Transfer:
	The Service Provider must ensure effective knowledge transfer to internal teams, ensuring sustainability and the ability to address future queries or issues independently.
TR 5.3.4	Hands-on Sessions
	: Ensure interactive sessions where users can practice using the system with guidance from trainers.

TR 5.3.5	Post-Training Support:
	Offer support through Q&A sessions, refresher courses, or a dedicated helpdesk during the initial post-implementation phase.
TR 5.4	**Training Schedule:**
TR 5.4.1	The training should be scheduled in phases, starting with system administrators and super users, followed by end-users.
TR 5.4.2	Training sessions should be planned to minimize disruption to daily operations, with flexible timing options available.
TR 5.4.3	A detailed training plan should be provided ahead of time, specifying training dates, topics covered, and expectations.
TR 5.5	**Assessment and Feedback:**
TR 5.5.1	Post-training assessments should be conducted to evaluate the effectiveness of the training and ensure that users have acquired the necessary skills to operate the system efficiently.
TR 5.5.2	Gather feedback from trainees to identify any areas where additional training or clarification may be needed.
TR 5.5.3	Provide certificates of completion to participants, ensuring they are formally recognized for completing the training.
TR 5.6	**Ongoing Support and Training Updates:**
TR 5.6.1	Refresher training sessions should be provided periodically to ensure users remain up to date with any system upgrades or new features.
TR 5.6.2	Ensure that users are supported through helpdesk services or training resources in case of difficulties encountered during regular system use.

6. Change Management:

The Audit Management System's people change management will be implemented using the following structured approach:

CM	Requirement Description
CM 6.1	**Stakeholder Identification and Analysis**
CM 6.1.1	Identify Key Stakeholders:
	Understand who will be impacted by the changes. This includes auditors, compliance officers, IT support teams, managers, and end users.
CM 6.1.2	Conduct Stakeholder Analysis:
	Determine each group's role, concerns, and needs to tailor the change management approach effectively

CM 6.2	**Communication and Engagement Plan**
CM 6.2.1	Clear Messaging:
	Develop clear communication that explains the reasons for the change, the benefits of the new system, and how it will impact users.
CM 6.2.2	Communication Channels:
	Use a mix of communication channels (emails, meetings, intranet, newsletters) to keep stakeholders informed.
CM 6.2.3	Engagement Strategy:
	Involve key stakeholders early in the process (e.g., by gathering feedback, forming focus groups, or involving them in pilot testing) to ensure buy-in.
CM 6.3	**Impact Assessment and Risk Management**
CM 6.3.1	Assess the Impact on People:
	Evaluate how the new system will change user roles, workflows, and responsibilities. Identify areas where users will need additional support.
CM 6.3.2	Identify Potential Resistance:
	Address concerns and resistance to change proactively by understanding the reasons behind them (e.g., fear of the unknown, disruption of routine).
CM 6.3.3	Risk Mitigation:
	Develop strategies to manage risks associated with people's resistance to change, such as offering incentives for adoption or creating champions within teams.
CM 6.4	**Training and Support Programs**
CM 6.4.1	Tailored Training:
	Provide role-specific training sessions for different user groups (e.g., auditors, managers, IT staff) on the new system's features and functionality.
CM 6.4.2	Training Materials:
	Develop user manuals, quick reference guides, video tutorials, and FAQs to support learning.
CM 6.4.3	Ongoing Support:
	Offer a helpdesk, user forums, and peer-to-peer support to assist users as they adapt to the new system.
CM 6.5	**User Involvement and Feedback**
CM 6.5.1	User-Centered Design:
	Involve end-users in testing and providing feedback during the design and implementation phases. This ensures the system meets their needs and reduces resistance.
CM 6.5.2	User Acceptance Testing (UAT)
	Conduct UAT sessions where real users test the system and provide feedback, ensuring it aligns with their workflows.
CM 6.5.3	Feedback Channels:
	Set up mechanisms (e.g., surveys, suggestion boxes, focus groups) to capture feedback post-implementation.

CM 6.6	**Deployment and Adoption Strategy**
CM 6.6.1	Phased Rollout:
	Implement the system in phases (e.g., start with a pilot department) to allow for adjustments and ensure a smooth transition.
CM 6.6.2	Super-Users and Champions:
CM 6.6.2.1	Appoint super-users or change champions to assist with the transition and act as go-to resources for other users.
CM 6.6.3	Monitor Adoption Rates:
	Track system usage metrics (e.g., login frequency, feature adoption) to assess how well users are adapting.
CM 6.7	**Resistance Management**
CM 6.7.1	Address Concerns Early:
	Actively listen to concerns and provide solutions or reassurance. This can include offering additional training, clarification of benefits, or demonstrating the system's value.
CM 6.7.2	Incentivize Adoption:
	Consider incentives or recognition for users who successfully adopt the new system and integrate it into their workflows.
CM 6.7.3	Offer Personal Support:
	Provide one-on-one coaching or mentoring for users who are struggling with the transition.
CM 6.8	**Post-Implementation Review and Continuous Improvement**
CM 6.8.1	Evaluating Change Impact:
	After the system is fully rolled out, assess the effectiveness of the change management efforts. Review user feedback, adoption rates, and performance to gauge success.
CM 6.8.2	Lessons Learned:
CM 6.8.2.1	Document lessons learned from the change management process to improve future change initiatives.
CM 6.8.3	Continuous Feedback Loop:
CM 6.8.3.1	Maintain a system for ongoing feedback and make continuous improvements to the AMS based on user input and evolving needs.
CM 6.9	**Sustaining Change**
CM 6.9.1	Reinforce Adoption:
	Continuously encourage users to adopt the new system by emphasizing its benefits, sharing success stories, and highlighting the efficiencies it provides.
CM 6.9.2	Refresher Training:
	Provide periodic refresher courses or updates when new features or processes are introduced to ensure continued competency and engagement.
CM 6.9.3	Celebrate Success:
1	Recognize individuals or teams who have successfully embraced the new system, reinforcing a positive culture of change.

7. Solution Guidelines:

SG #	Solution Guideline Description
SG 7.1	The solution shall provide the functions and services required to support the business capability.
SG 7.2	There shall be a single application to support a given business capability, i.e., the solution must not re-implement a capability already available in the portfolio, unless it is replacing the current one.
SG 7.3	The solution shall be as secure as business requirements dictate.
SG 7.4	The solution shall meet legal and conformance requirements, including those for privacy.
SG 7.5	The solution shall provide adequate performance and responsiveness.
SG 7.6	The solution shall be able to scale, without redevelopment, for anticipated increase in volumes for the next 5 years.
SG 7.7	The solution shall be reliable and easily recoverable.
SG 7.8	The solution shall validate input data and maintain integrity of any data added, updated or exported.
SG 7.9	The solution shall provide APIs which allow services to be accessed via an interface conforming to industry standards adopted by ACSA, e.g., Web Service (REST, SOAP).
SG 7.10	The solution shall avoid “hard coding” of value, i.e., any variables which are likely to change must be externalized to the database or parameter/rule files.
SG 7.11	The solution shall trap errors and report them in a meaningful and persistent way.
SG 7.12	The solution end user interfaces must. be intuitive, and standards based to facilitate ease of adoption and reliable usage as well as reduced training requirements.

AIRPORTS COMPANY SOUTH AFRICA

8. IT Standards

ACSA has a prescribed **IT Standards** to which all IT infrastructure-based solutions must adhere. For detailed standards, please refer to **Annexure A**: **IT Standards,** which will accompany this document

9. Service Level Agreement Standards

ACSA has prescribed service levels to which a successful Service Provider needs to adhere. For detailed service levels, please refer to **Annexure B: Service Management, Preventative and Corrective Maintenance** which will accompany this document.

10. Information Security Standards

ACSA IT Information Security has prescribed **Web Application Security Standards** to which ACSA web-based applications need to adhere. For detailed standards, please refer to: **Information Security: Web application Security Standards**, which will accompany this document.