Glossary

Acronym/Term	Description
3G and 4G	Three and Four Generation Cellular Technologies.
ACSA	Airports Company South Africa.
CCTV	Closed Circuit Television.
CPU	Central Processing Unit.
ENATIS	Electronic National Administration Traffic Information System.
GPRS	General Packet Radio Service.
GSM	Global System for Mobile Communications.
HDD	Hard Disk Drive.
IPsec	Internet Protocol Security.
ID	Identity Document.
IT	Information Technology.
IVS	Identity Verification System.
LPR	License Plate Recognition.
OHS	Occupational Health and Safety Act.
ORTIA	Oliver Reginal Tambo Airport.
OS	Operating System.
PC	Personal Computer.
POPI	Protection of Personal Information Act.
PSU	Power Supply Unit.
RFID	Radio Frequency Identification.
SABS	South African Bureau of Standards.
SAPS	South African Police Service.
SIM	Subscriber Identity Module.
SLA	Service Level Agreement.
SMS	Short Message System.
SOW	Scope of Work.
SSL	Secure Sockets Layer.

TCP/IP	Transmission Control Protocol/Internet Protocol.
UPS	Uninterruptible Power Supply.
VPN	Virtual Private Network.
WIFI	Wireless Fidelity.

Table 1 : Glossary

AIRPORTS COMPANY SOUTH AFRICA

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

EXECUTIVE SUMMARY

This document is an extensive specification of the Automated Access Control Solution to be procured, installed commissioned, maintained and supported at Cargo main gate by the incumbent Service Provider. The need to install an automatic access control solution was dictated by rising crime levels and the proliferation of other undesirable security incidents and threats within the precinct. This is because the manual access control dispensation is laborious, error prone, vulnerable to collusion, grossly inadequate, inefficient and ineffective in proactively and reactively dealing with security challenges or incidents. This scope of work commences with a succinct expression and contextualization of the business challenge or need, background and objectives to be achieved, it then proceeds to unpack the scope or delimitations of the Project. The current AS IS or baseline situation is captured and documented. Next is a deployment of the overarching requirements encompassing business, server, generic, non-functional and reporting. The preceding is trailed by a disintegration and postulation of the support and maintenance requirements, service level agreements and Service Provider performance requirements. The document culminates with transformation requirements and solicits for approval to proceed.

1. INTRODUCTION

1.1. Background and problem statement

Currently, access to Cargo precinct at OR Tambo International Airport (ORTIA) is semi-automated. This dispensation is clearly error prone, laborious, vulnerable to collision and poses a serious security threat and vulnerability. This security situation is glaringly not ideal given that ORTIA is a National Key Point (NKP). At Cargo main gate, there is an incomplete small scale access control system that captures pedestrian, vehicle, driver and passenger details. The system is made up of scanners, access to a remote database and a web based user interface. This partial installation is still inadequate and has not completely met the security and access control needs required at the Cargo precinct as per ACSA's security standards.

Two identification documents are used by ACSA and Cargo stakeholders to gain entry to the area as follows; the first is an ACSA permit card issued by ACSA's permit office. The second is an Identity Verification System (IVS) card used by majority of cargo stakeholders. IVS is an industry system that is used by majority of the cargo community in South Africa for access control purposes.

All other non ACSA and non-Cargo staff use their ID documents, driver's license and passports (foreign nationals) to gain access to the area.

Further to the above, traffic congestion challenges are rife especially during peak hours owing to the structural configuration of the gate.

1.2 Recommendation

Cognisance of the preceding background just articulated, the recommendation is to replace the current semi-automated access control system with a complete electronic or automated access control solution. Implementing the full scale automated system will lead to the following benefits and objectives;

1.2.1. Improve safety and security;
1.2.2. Curb car theft;
1.2.3. Mitigate or eradicate armed robbery, cash in transit heist and other petty crimes;
1.2.4. Eliminate or minimize the potential of collusion;
1.2.5. Alleviate traffic congestion to some extent;
1.2.6. Comply with Act 53 of 1985 (control of access to public premises and vehicles); and
1.2.7. Improve operational efficiencies and effectiveness at Cargo precinct.

The solution will be complemented and reinforced with License Plate Recognition (LPR) which is a system that makes it impossible for a motorist to drive out of the parking precinct if transaction credentials upon exit do not match the entry ones.

1.3 Purpose of this document

The purpose of this Scope of Work (SOW) document is to express and concisely specify the work activities, material or equipment specifications, deliverables, milestones, quality requirements, support and maintenance requirements as well as performance management and evaluation criteria applicable to a comprehensive replacement of the current manual system with an automated access control solution.

2. SCOPE

2.1. **In Scope**

The following are considered in scope for the initiative:

2.1.1. Supply, commission, maintain and support the solution;
2.1.2. All electronic hardware and software to manage and control access. All software for the purpose of access management and vetting entry. Capture of all data, storage of all data for an acceptable time frame permissible by the protection of personal information (POPI) act;
2.1.3. Provision of alerts of activities concerning entry and exit;
2.1.4. Have the ability to provide detailed reports on entry, purpose of entry (Delivery or Collection), destination, duration of stay (not more than 3 hours) and other related reports that may be deemed necessary and to assist with operations and security;
2.1.5. Scanning identification credentials (ID, driver's licenses, license disc, passports and all bar-coded access cards, any other relevant cards deemed necessary by ACSA etc.) of all drivers and passengers (if applicable) prior to granting access;
2.1.6. Identification of people unknown to ACSA;

2.1.7. Online integration to the following but not limited to the third-party databases for checks;

2.1.7.1. SAPS;

2.1.7.2. ENATIS (Minimum valid car license disk and drivers license); and

2.1.7.3. Any other relevant database deemed necessary by security stakeholders.

Furthermore, the prospective Service Provider is expected to have a memorandum of understanding (MOU) for integrating to the above-mentioned third-party databases. MOU is an agreement between the Service Providers (SP(s) and Third party database providers. The SP(s) to facilitate acquisition of the MOU. ACSA will not be involved in soliciting these MOU's. It is a requirement for the bidders to have these MOU's.

Furthermore, the solution must be able to perform the following:

2.1.8. Real-time notifications via SMS and email;

2.1.9. Ability to automatically identify returning visitors;

2.1.10. Must capture facial images of drivers and visiting the precinct;

2.1.11. Customized electronic reporting;

2.1.12. Turnstile controlled by the solution

2.1.13. Must have License plate recognition;

2.1.14. Ability for the scanner software to scan and interpret information from 1D, 2D and 3D bar codes;

2.1.15. Compatibility and seamless integration of solution to existing ACSA systems and applicable Infrastructure where necessary and applicable;

2.1.16. All applicable infrastructure like Servers, Workstations, Routers, uninterruptible power Supplies (UPS) and Switches will be provided by ACSA's IT infrastructure team, however the specifications will be furnished by the Service Provider;

2.1.17. Bidders must provide training and skills transfer plan;

2.1.18. Structural reconfiguration of the main gate might be required. This will assist with the elevation of traffic congestion caused by the high volume of visitors, logistics deliveries and pickup vehicles;

2.1.19. The duration of support and maintenance is **3 (three)** years;

2.1.20. All equipment supplied must have a minimum warranty of **5 (five)** years;

2.2. **Out of scope**

The following are considered out of scope:

2.2.1. Installation of additional Surveillance cameras or Closed-circuit television (CCTV);

2.2.2. The provision of GSM SIM cards for the handheld scanners. This will be provided by ACSA.

2.2.3. Access control via turnstiles or pedestrian access; and

2.2.4. Anything not explicitly mentioned herein is out of scope.

2.2.5. Although the following are out of scope, Bidders must propose equipment that supports PoE (Power over Ethernet Equipment). Each device proposed must not draw over 30 watts of power per network point.

2.2.6.Maintenance and Support of the PIDS's command and control;

2.2.7.Space in Wire centre;

2.2.8.Installation of power;

2.2.9.Cooling in the wire centre;

2.2.10. Uninterruptable power supply; and

2.2.11. Network and Cabling;

2.2.12. Network switches; and

2.2.13. Servers, storage, and backup

3. HIGH LEVEL CURENT AS IS CONFIGURATION

3.1. **Semi-automated access control solution**

The current system is semi-automated in the sense that there are still manual interventions involved e.g. opening and closing of booms. The solution is made up of the following integral components:

3.1.1. 6 x handheld scanners;

3.1.2. Integration to remote databases for real time online checks; and

3.1.3. A web based use interface.

The data collected by the scanner is sent to remote databases for verification via a secure VPN connection. The user accesses the application via a standard web browser. The forgone articulation is schematically represented in figure 1. The solution functionality includes a number of options, including (a) Driver's License scanning and verification (b) Vehicle License disc scanning and verification (c) Recording the number of passengers (d) Taking of photos and (e) Recording the motorist destination.

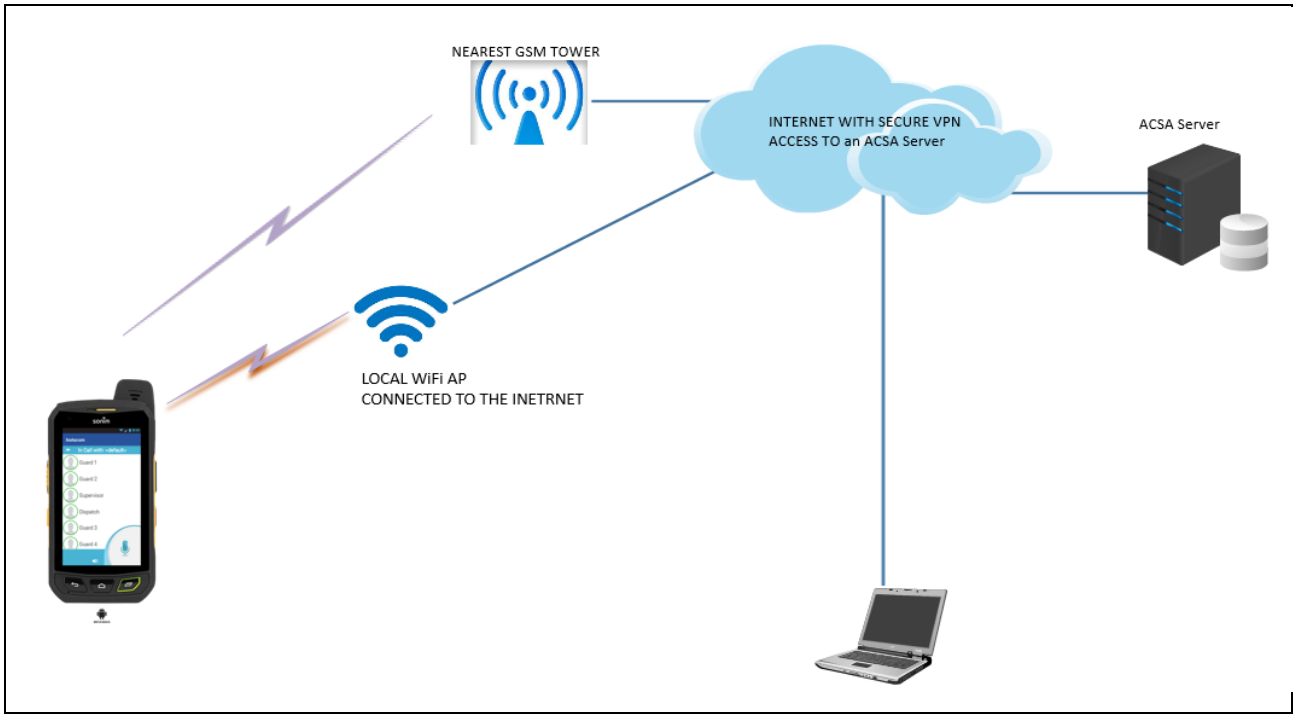

Figure 1 : Semi automated access control solution schematic

3.2. **Main gate structural configuration**

The main gate has three lanes as follow

3.2.1. The first entry lane is for visitors;

3.2.2. The second entry lane is for Staff and permit holders; and

3.2.3. The last lane is exit for all.

Figure 2 is a graphical depiction of the main gate.

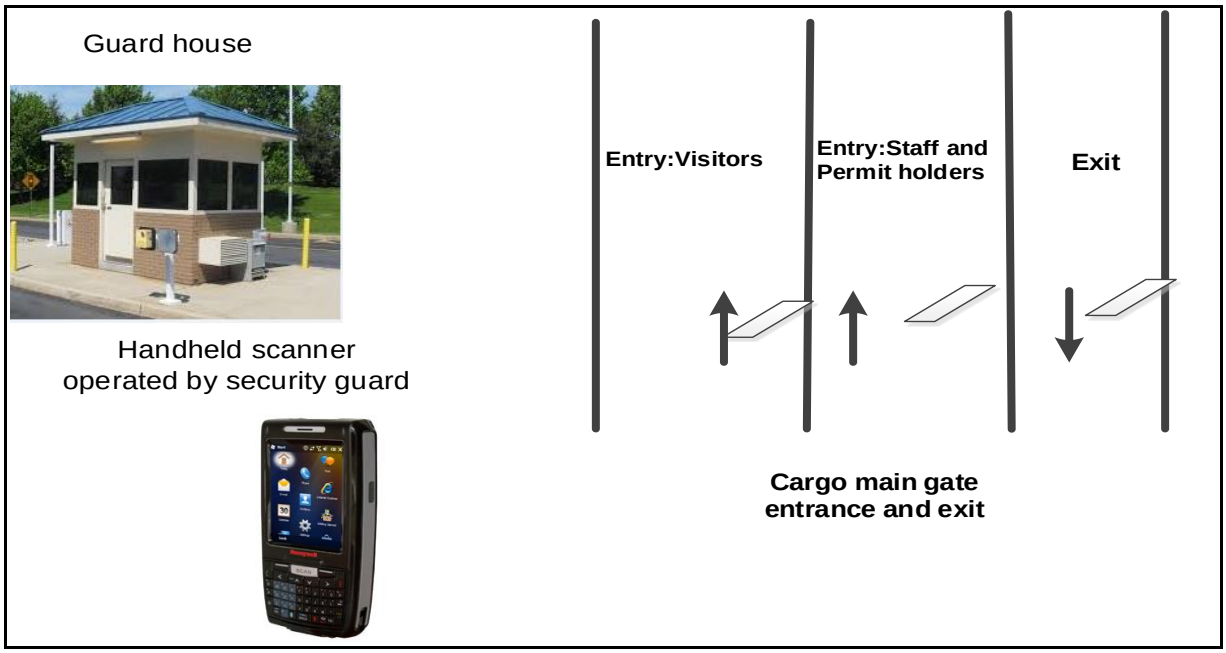

Figure 2 : Cargo main gate entrance and exit

4. BUSINESS RULES

Table 3 is an articulation of applicable high level business rules.

Number		Business Rules
BRL	1	A vehicle's license disc and driver's license should be scanned at point of entry.
BRL	2	All MOTORIST accessing the cargo main gate should have their ID document/card, driver's license or passport scanned at the point of entry.
BRL	3	ACSA Cargo access control standard operating procedures(SOP) should be a adhered to when operating the solution.
BRL	4	Standard operating procedures of cargo main gate shall apply in the case of an emergency (eg ambulance and fire).
BRL	5	The security personnel should revert to manual standard operating procedure in case of downtime.

Table 2 : High level business rules matrix

5. BUSINESS REQUIREMENTS

The solution must comply with minimum requirements articulated in the matrix below.

	Business requirement
BRQ1	**Access control** a. Capture all data; vehicle registration, driver's license, passenger Identification. b. The solution should be able to perform vehicle and driver verification to check that the vehicle is not a stolen vehicle and that the driver is not a wanted person. c. The solution should initiate the creation and maintenance of a comprehensive database of "White List" and "Black list" entries of both vehicles and individuals. d. The solution should be able to record visit statistics of people who go through the gate using ACSA permits or other cards. All statistics should be drawn from the system; no manual intervention should be required. e. The solution should have the capability to capture facial pictures of people and pictures of vehicles visiting the precinct. f. The solution must have an audit functionality whereby all entry activities are electronically captured and stored for a period permissible by the "POPI act". g. The solution must have the ability to eliminate the potential of collusion between staff and visitors.
BRQ 2	**Scanner** The scanner must at minimum comply with the following requirements: a. Quantity: A total of 10 (ten) handheld scanners will be required; b. Data transmission: Must be able to transmit data in real time using 3G, 4G and Wi-Fi communication and network technologies. As soon as a notice is issued at the main gate, the visitor details should be available from the web-based back office system instantly. c. Ease of use: Must be easy to use with simple menu structures and touch functions. d. Multimedia: Must be able take high quality photo, voice and video media and attach them to a motorist profile. Furthermore, it must have the capability to capture the number of occupants per vehicle and any other characteristics that may be necessary to capture. e. Bar code reader: Must incorporate two-dimensional barcode scanning and 128-bit barcode scanning technologies Capable of scanning the registration label in a vehicle, to pre-populate the vehicle license plate number and any other known information.

Business requirement	
	f. Security: Must be able to authenticate a user when login credentials (username and password) are entered prior to establishing communication with a Server. All data communications must take place using SSL which is web security technology. g. Touch screen: The scanner user interface must be a touch screen with keypad size customizable per individual preferences. The preferences to be advised by ACSA at a later stage. h. Real time: All system communications must be in real time. This includes the ability to scan an RFID permit, instantly conduct checks and provide feedback; i. Storage capacity: The device must be shipped with enough memory to allow it to effectively and efficiently perform its functions. Device memory must be at least be 32MB. j. Night operation: Must be able to function at night as per normal. It must therefore incorporate a backlight functionality for low or no light situations. k. Real time uploads: There must be no limitations with the transfer of data. The handheld should be able to communicate the details of each visitor as it is issued using its GPRS connection. l. Blacklist: The handheld must be able to download existing permits, blacklisted vehicles or vehicles of interest. Whenever an officer commences capturing a vehicle data, any offending vehicle registrations from one of the downloaded lists should be flagged when the officer enters it into the relevant field. m. Time: Information must be sent to the Server immediately (real time) after completing a transaction. n. Battery capacity: The scanner battery capacity must last for a minimum of 12 hours on average before charging. In addition, the scanner must be shipped with at least one spare battery. **o.** Customization: All applicable scanner functionality must be customizable as per ACSA requirements;
BRQ 3	**Traffic barrier** The solution must incorporate a traffic barrier or boom gate which is a bar or pole to allow the boom to block vehicular access through a controlled point. The traffic barrier must be designed and fit for purpose for ultra-high traffic flow. It must also be electromechanically designed with battery backup and management override.
BRQ 4	**Spike barriers** Spike barriers at each entrance is a key requirement. Spike grippers are used to enforce one-way traffic in a single traffic lane, such as the entrance or exit to a parking lot. These spikes must be heavy duty spikes, installed to cater for heavy duty vehicles.

Business requirement	
BRQ 5	**Robots** The entry lanes must have two robots that should glow RED by default and should turn GREEN upon entry if the entry transaction is successful. The exit lane must also have two robots that should also be RED by default and should turn GREEN upon exit if the exit transaction is successful.
BRQ 6	**Access control readers and controller** Access control hardware and software is a requirement for the enforcement and control of physical personal and public gaining access to the facility. The solution should thus incorporate access control readers and controllers for each entry and exit. It is recommended that the entry/exit lane should be equipped with a long-range reader with high speed LPR and facial recognition or similar technology, in order to cater for the high demand of vehicles requiring to enter/exit the area during peak times.
BRQ 7	**License plate recognition** LPR is an image processing technology used to identify vehicles by their license plates on entry and at exit time to ensure the car license plate matches the parking ticket. The technology is supported by complimentary processes which match license plate registration, facial image of the motorist and the payment transaction. This makes it difficult for a motorist to drive out of the parking precinct if transaction credentials upon exit do not match the entry ones. In case of a mismatch or discrepancy, an alarm is raised in the control room for attention. The LPR system must at minimum comply with the following minimum requirements: a. The LPR system shall consist of all hardware and software necessary to provide a complete license plate reading system. b. The Service Provider shall be responsible for providing a fully functional LPR system. c. Processing of license plates by the LPR system shall occur in parallel with other functions occurring at exit and entry lanes. d. All Cameras for the LPR system must be digital and IP based; e. The LPR system must have LPR and facial cameras at all entries and exits. f. The facial cameras must be able to capture images of both normal vehicles as well as trucks. Therefore, two facial cameras will be required at each entry and exit as the heights of normal vehicles and trucks are not the same. g. The LPR component must record South African Number plates from all provinces including government, police, military and diplomatic number plates. Recording of number plates from foreign neighboring countries will not be necessary; h. All information within the LPR database shall be accessible for review and printing of reports.

Business requirement	
BRQ 8	**Online integration** The solution must to interface with relevant online databases for the purpose of performing real time checks and validations. These incudes but not limited to the following databases: a. SAPS; b. ENATIS; and c. Any other relevant database deemed necessary by security stakeholders.
BRQ 9	**Data storage, System Backup and Recovery** a. All data collected by the scanner must be encrypted and transmitted wirelessly using secure sockets layer(SSS) technology to the server b. System backup and recovery is a key requirement that should unfold as per ACSA IT backup policy.

Table 3 : Business requirements matrix

6. SERVER REQUIREMENTS SPECIFICATION

6.1. At minimum, the following Servers will be required (refer to 6.5):

6.1.1. One Sever and a backup for the automated access control solution;

6.1.2. One Server and a backup for the LPR system;

6.2. The Service Provider shall utilize premium grade equipment designed to operate reliably within the specified environmental and operating circumstances. All equipment shall be installed and tested by system provider's technicians/personnel complying with manufacturers' recommendations;

6.3. The Severs shall provide capability to expand and upgrade the system to meet future security requirements without having to replace major components;

6.4. The system or solution must be connected to ACSA' network;

6.5. ACSA standards for Severs is Virtual. Furthermore, the Servers will be provided by ACSA's IT Infrastructural team but the Specifications will be furnished by the Service Provider;

6.6. The system will be web accessible and allow Operators and Managers access to the operation and reporting of the system through operator and manager accounts over the internet;

6.7. The system must be flexible and adaptable in order to allow for customization according to ACSA's changing security requirements;

6.8. All central servers shall operate using internationally adopted operating system(s). The database shall be robust, proven, and commercially available (Oracle and Microsoft SQL Server) are examples of such database management systems (DBMS);

6.9. Interoperability, Industry standard SQL databases, commercially available solutions, integrated through open communications protocols, TCP/IP compliant, Hardware and Software reliability and system supportability are the main features, functions and essential requirements for this solution;

6.10. All system transactions shall be recorded in such a manner as to allow an audit to be Conducted on all transactions. The intent is to allow all transactions to be linked back to the master records for reporting, analysis, data retrieval, and legal purposes;

6.11. The system shall be an open system where all interfaces (hardware and software) conform to recognized national and international standards published from organizations such as International Standards Organization (ISO);

6.12. All central servers shall be fault tolerant for all operational functions. There shall be no data loss upon failure of any single component or associated interface. The servers shall be configured at a minimum to:

6.12.1. Maintain twenty-five (25) months of on-line data of all transactions – entry date/time, exit date/time; exit lane identification, parking duration and other information considered as part of the transaction; and

6.12.2. Archive all summary reports for up to sixty (60) months on electronic media with simple retrieval capability.

7. GENERIC REQUIREMENTS SPECIFICATION

7.1. The Service Provider shall provide, install, commission, support and maintain all the required equipment;

7.2. All material housing metals must be weather and rust proof and non-corrosive (IP65 rated);

7.3. A notification must be sent to system users in cases where the main power is down and the system is running on UPS. Minimum required uptime for UPS is 2 hours;

7.4. Owing to the fast pace at which technology evolves, all prospective service providers submitting proposal for the tender should declare all relevant Technology that ACSA has not specifically requested, but could have a significant impact on improving customer service and operating costs;

7.5. From time to time, ACSA may require the Service Provider to perform new Installations, Moves, Additions, Change and De-installation (“IMACD”) as well as tagging of asset as follows

7.5.1. Request installations, change, de-installation or moves of components of the System;

7.5.2. Maintain an asset register indicating the location of all installed equipment;

7.6. The Service Provider shall install all the required equipment, perform on-site inspection of installation work performs initial start-up of equipment and software (including customized equipment and software programming) and test all equipment and software to ensure proper operation;

7.7. All installations shall be complete in all respects and the Service Provider shall allow for the completion and successful operation of the complete installation, irrespective of whether every separate item is specified or not;

7.8. Equipment installation shall include all mounting hardware and all low voltage electrical, fiber optic or other cable or wiring connection required to make the equipment operable;

7.9. The Service Provider shall work with the airport electrician/personnel to direct what necessary low/high voltage hook-ups are necessary;

7.10. If any software is required to be installed on any ACSA-owned computers, such installation shall be done in coordination with the relevant airport's Information Technology Department as necessary.

7.11. The Service Provider shall make available user and maintenance manuals for all equipment and software to ACSA at the time of equipment start-up;

7.12. The solution must at minimum comply with the current ACSA IT Architectural principles;

7.13. All equipment removed from site will be handed over to ACSA immediately after removal. Existing asset management tags must remain on the equipment at all times. Equipment removed will be boxed and transported to a pre-determined location on the airport premises according to ACSA requirements. It is recommended that the supplier keeps a record with serial number information of existing equipment removed and handed over to ACSA;

7.14. All decommissioning of old equipment should follow proper asset decommissioning procedures (for IT equipment) as instructed by ACSA from time to time;

7.15. A Factory Acceptance Test pack will be drafted, and the solution will be tested against the requirements articulated in this document Specification. Any defects will be corrected, and a Factory Acceptance Testing (FAT) report will need to be signed off by the relevant stakeholders' prior to the solution going operational; and

7.16. A thorough system impact assessment will need to be conducted prior to deployment.

8. REPORTING REQUIREMENTS SPECIFICATION

This section specifies customized reports that will be generated by the solution for operational use in addition to already existing standard reports. All reports must be available real-time via a standard PC running a Web Browser such as Microsoft, Chrome or Fire Fox, and can be viewed by lanes daily, weekly, monthly and yearly, or selectable date range formats as selected by the user.

8.1. Visitor reports

Report Name	Visitors report	**Report Owner**	Public safety and security
Report purpose	To report on the number of drivers, cargo drawers and ACSA card users visiting the cargo precinct		
Priority	High	**Preferred Original Source**	From the server
Availability	Always	**History stored**	5 years
Access Method	Report will be emailed to designated security personnel.	**User access**	The server database administrator (DBA) will have access to the server and will be able to access reports on demand.
Data freshness and dependency	Data will be dependent on the accuracy of the source system(server) as well as its availability.	**User Input and Query Method**	• Report must be accessible by relevant security personnel on demand.
Report Detail Format / Layout	The report must at minimum contain the following columns: a. Visitors name b. Visitors car registration number c. Visitors ID number (applicable for South African drivers) d. Cargo stakeholder visited e. Cargo stakeholder contact number f. Date g. Time in h. Time out i. Total duration spent in the precinct j. Total number of visits for a particular driver k. Total number of visits for a particular cargo stakeholder l. Total number of visits for a particular vehicle registration number m. Guard name n. Unique transaction ID		
Report Rules	a. The reports must be able to be filtered by: Day, Week, Month, Year and Stakeholder visited. b. The consolidated report for all visitors must be able to show the total number of visitors filterable as specified above. c. Report must be viewable online on the system as well as exportable in excel and PDF formats.		

Table 4 : Visitor report matrix

8.2. Exception reports

Report Name	Exception report	**Report Owner**	Public safety and security
Report purpose	To report on the number of exceptions.		
Priority	High	**Preferred Original Source**	From the server
Frequency of generating report	Daily	**Update frequency of report data**	Daily
Availability	Always	**History stored**	5 years
Access Method	Report will be emailed to designated security personnel.	**User access**	Designated security personnel should be able to access the system using login credentials.
Data freshness and dependency	Data will be dependent on the accuracy of the source system(server) as well as its availability.	**User Input and Query Method**	Report must be accessible by designated security personnel on demand.
Report Detail Format / Layout	The report must at minimum contain the following columns: a. Number of expired driver's licenses b. Number of expired license discs c. Report must be date and time stamped		
Report Rules	a. The reports must be able to be filtered by: Day, Week, Month and Year. b. The report must be filtered by user card. c. Report must be viewable online on the system as well as exportable in excel and PDF formats.		

Table 5 : Exception report matrix

8.3. Transaction report

Report Name	Transaction report	**Report Owner**	Public safety and security
Report purpose	To report on relevant details pertaining to a particular visitor. A transaction refers to scanning the driver in and out. Therefore, the focus of this report is on the driver.		
Priority	High	**Preferred Original Source**	From the server
Frequency of generating report	Daily	**Update frequency of report data**	Daily
Availability	Always	**History stored**	5 years
Access Method	Report will be emailed to designated security personnel.	**User access**	Designated security personnel should be able to access the system using login credentials.
Data freshness and dependency	Data will be dependent on the accuracy of the source system(server) as well as its availability.	**User Input and Query Method**	Report must be accessible by designated security personnel on demand
Report Detail Format / Layout	The report must at minimum contain the following columns: a. Visitor name b. Cargo stakeholder visited c. Time in d. Time out e. Total duration spent in the precinct f. Vehicle registration number g. Visitor ID number h. Visitor's driver license valid until date i. Visitor type		
Report Rules	Report must be viewable online on the system as well as exportable in excel and PDF formats.		

Table 6 : Transaction report matrix

8.4. License disc report

Report Name	License disc report	**Report Owner**	Public safety and security
Report purpose	To report on relevant details pertaining to a particular vehicle. Therefore, the focus of this report is on the vehicle.		
Priority	High	**Preferred Original Source**	From the server
Frequency of generating report	Daily	**Update frequency of report data**	Daily
Availability	Always	**History stored**	5 years
Access Method	Report will be emailed to designated security personnel.	**User access**	Designated security personnel should be able to access the system using login credentials.
Data freshness and dependency	Data will be dependent on the accuracy of the source system(server) as well as its availability.	**User Input and Query Method**	Report must be accessible by designated security personnel on demand
Report Detail Format / Layout	The report must at minimum contain the following columns: a. Date b. Time in c. Time out d. Vehicle make e. Vehicle colour f. Vehicle model g. Vehicle registration number h. VIN number i. Disc valid until date		
Report Rules	Report must be viewable online on the system as well as exportable in excel and PDF formats		

Table 7 : License report matrix

8.5. Driver change report

Report Name	Driver change report	**Report Owner**	Public safety and security
Report purpose	To report on instances where a driver who is driving out is different from the one that drove the vehicle in.		
Priority	High	**Preferred Original Source**	From the server
Frequency of generating report	Daily	**Update frequency of report data**	Daily
Availability	Always	**History stored**	5 years
Access Method	Report will be emailed to designated security personnel.	**User access**	Designated security personnel should be able to access the system using login credentials.
Data freshness and dependency	Data will be dependent on the accuracy of the source system(server) as well as its availability.	**User Input and Query Method**	Report must be accessible by designated security personnel on demand
Report Detail Format / Layout	The report must at minimum contain the following columns: a. Date b. Time in c. Time out d. Driver name(in) e. Driver ID(in) f. Driver name(out) g. Drive ID(out) h. Vehicle model i. Vehicle make j. Vehicle colour k. Vehicle registration number		
Report Rules	a. The scanner must be able to compare driver and motor vehicle identities upon scanning the driver out and should be able to identify any differences in terms of the driver. b. Report must be viewable online on the system as well as exportable in excel and PDF formats.		

Table 8 : Driver change report matrix

8.6. Shift change report

Report Name	Shift change report	**Report Owner**	Public safety and security
Report purpose	To report shift change for accountability and responsibility purposes and also to compare and contrast individual and team Gate efficiencies and performance. Two shift exist as follows: I. Shift one starts from 6am to 6pm. II. Shift two starts from 6pm to 6am.		
Priority	High	**Preferred Original Source**	From the server
Frequency of generating report	Daily	**Update frequency of report data**	Daily
Availability	Always	**History stored**	5 years
Access Method	Report will be emailed to designated security personnel	**User access**	Designated security personnel should be able to access the system using login credentials.
Data freshness and dependency	Data will be dependent on the accuracy of the source system(server) as well as its availability.	**User Input and Query Method**	Report must be accessible by designated security personnel on demand
Report Detail Format / Layout	The report must at minimum contain the following columns: a. Date b. Shift number (1 or 2) c. Guards names for shift 1 d. Guard starting time for shift 1 e. Guard departure time for shift 1 f. Guards names for shift 2 g. Guard starting time for shift 2 h. Guard departure time for shift 2		
Report Rules	c. The scanner must be able to compare driver and motor vehicle identities upon scanning the driver out and should be able to identify any differences in terms of the driver. d. Report must be viewable online on the system as well as exportable in excel and PDF formats.		

Table 9 : Shift change report matrix

9. NON-FUNCTIONAL SPECIFICATIONS

This section is a high-level exposition of nonfunctional requirements that the system must comply with. Non-functional requirements define the criteria that can be used to judge the operation of a system, in contrast to functional requirements that define specific behavior or functions. Categories of non-functional requirements for the purpose of this solution include the following:

9.1. **Configurability and Flexibility**: The solution must have the ability to handle a wide variety of system configuration sizes. On the other hand, flexibility is applied when the software intends to increase or extend the functionality after its deployment. The solution must able to comply with the latter;

9.2. **Performance**: The performance constraints specify the timing characteristics of the software. efficiency specifies how well the software utilizes scarce resources: CPU cycles, disk space, memory,

bandwidth, etc. System response times must be benchmarked and adhered to;

9.3. **Reliability and Robustness**: Reliability specifies the capability of the software to maintain its performance over time. A robust system is able to handle error conditions gracefully, without failure. This includes a tolerance of invalid data, software defects, and unexpected operating conditions. The system must have a minimum operational and useful life span of 10 (ten) years;

9.4. **Availability**: A system's availability or" uptime" is the amount of time that it is operational and available

for use. Expected system availability Standards at ACSA is 99.8% that the solution must comply with the exception of planned maintenance;

9.5. **Portability**: Portability specifies the ease with which the software can be installed on all necessary platforms and the platforms on which it is expected to run;

9.6. **Usability**: Ease-of-use requirements address the factors that constitute the capacity of the software to be understood, learned, and used by its intended users. The system must be easy to learn and operated by users with minimal training.it must also conform to usability standards for graphical user interfaces;

9.7. **Maintainability**: Refers to the probability of performing a successful repair action within a given time.

In other words, maintainability measures the ease and speed with which a system can be restored to operational status after a failure occurs. The solution must comply with the maintainability and supportability requirements specified in section 23;

9.8. **Operational and environmental**: Refers to wider environmental and operating requirements. The entire solution especially the mechanical dynamics of the booms and other associate components must be able to work within extreme temperature conditions and variations.

9.9. **Security**: Describes functional and non-functional requirements that need to be satisfied in order to achieve the security attributes of an IT system. Security has been further disintegrated into the following requirements:

9.9.1. Authorization:

The solution must restrict the performance of all system use cases to persons who are currently designated as users;

9.9.2. Identification:

The solution must always identify any of its actors before permitting him or her to access the system otherwise access must be denied;

9.9.3. Integrity: The solution must protect of its communications from unauthorized intentional corruption during transit including communications between its users. It must also protect its persistent data from unauthorized intentional corruption;

9.9.4. Privacy: The system shall restrict access to confidential user information, whether communicated or stored to its rightful users and administrators;

9.9.5. Repeated authentication failure: The solution must notify and administrator within one minute if it cannot successfully verify the identity of any user in less than three attempts within anyone-hour period. In addition, the system should hide unauthorized functionality to users according to their user profiles;

9.9.6. Encryption: All data/information transmitted between the various components of the system must be in an encrypted channel. Specifically, all transmitted data must use IPsec-encryption (using a crypto coprocessor) that meets international regulations or standards;

9.9.7. Non-repudiation: All the times that a user performs any updates or changes to profile information, the system shall audit trail the transaction and record the following information:

a. Name of the user;
b. Date and time; and
c. Update or change performed.

Furthermore, the system must maintain an audit log of all security events;

9.10. **Personalization**: Refers to customization of the system according to user personal preferences.

The system must lend itself to all ACSA customization requirements;

9.11. **Compliance**: The solution must comply with all statutory and legislative requirements in the Republic of South Africa;

9.12. **Accessibility**: Refers to the accessibility of a system to all people, regardless of disability type or

severity of impairment; and

9.13. **Innovativeness**: The solution must be a state of the art system surpassing its predecessor in many

novel and innovative aspects and must provide a platform and springboard for innovation and scalability.

10. MAINTENANCE SCOPE OF SERVICES

This section is an enunciation of Support and Maintenance Requirements. The following specifications shall apply to maintenance and support services:

10.1. The Service Provider must provide a detailed proposal and costing on how it will perform this critical

function for ACSA;

10.2. The Service Provider is expected to work in conjunction with ACSA IT and other Service Providers

within ACSA when performing preventative and corrective maintenance;

10.3. The Service Provider will be responsible for the entire solution including hardware, software and all associated applications running on the system as well as adhoc installations;

10.4. The operating hours will be from Monday to Friday, 6h00 to 18h00. The bidder must make provision for a resource to be available at all hours as stipulated in table 10 as well as in the SLA and Contract document to be signed with the Service provider; and

10.5. The Service Provider must ensure that all relevant resources and subject matter experts are available during the entire project duration i.e. from compulsory site inspections, investigations and assessment all the way through to implementation and support.

Coverage parameters are expressed in table 10.

Coverage parameters:

#	Days	Time from	Time to	Standby Times
1.	Monday	06h00	18h00	18h00-06h00
2.	Tuesday	06h00	18h00	18h00-06h00
3.	Wednesday	06h00	18h00	18h00-06h00
4.	Thursday	06h00	18h00	18h00-06h00
5.	Friday	06h00	18h00	18h00-06h00
6.	Saturday	-	-	24 Hours
7.	Sunday	-	-	24 Hours
8.	Public Holiday	-	-	24 Hours

Table 10 : Maintenance timeframe coverage parameters

10.6. The bidder's proposal must make provision for after hours, weekends and public holidays support on a callout basis;

10.7. The proposal must include after hours' telephone numbers, where support personnel are reachable;

10.8. The number of resources allocated for the system should take into account the SLA requirements;

10.9. **Preventative and corrective maintenance requirements**

10.9.1. Preventative maintenance includes planned overhauls, replacements, inspections, tests and any activity aimed at preventing failures and defects through maintaining the condition of the infrastructure or assessing its condition for the purposes of corrective maintenance. Corrective maintenance includes all activities following a preventative maintenance inspection;

10.9.2. Corrective or breakdown maintenance includes maintenance that is unforeseen and is necessary to restore the serviceability of the infrastructure and functionality of the System. Some of this break down maintenance could be requested after hours on weekend and Public holiday. Bidders will be expected to respond and attend to all the faults;

10.9.3. The Service Provider will be held liable for any failure of the System that should have been prevented during preventative maintenance. Therefore, the Service Provider should include any further preventative maintenance recommendations, which in its opinion are necessary for the specific and other failure prevention;

10.9.4. The Service Provider's proposal must make provision for enough personnel at ORTIA during normal working hours (Monday – Friday: 06h00-18h00) to perform maintenance and support

of the systems. The number of resources allocated should take into account the Service Level Agreement ("SLA") requirements as stipulated in Section 4 to ensure that SLA targets are met;

10.9.5. The Bidder's proposal must make provision for after hours, weekends and public holidays support on a callout basis for incidents that impacts the systems. Hourly rates and call-out fees if applicable must be provided in the pricing schedule;

10.9.6. The Service Provider's proposal must also cater for short notice call-out in an emergency situation where the supported system may be affected by other interruptions or change processes within the airport (e.g. power). This Bidders must provide a call-out basis and hour rate at the specific site. For planned activities, advance notice will be given to the service provider. In addition, ACSA will require the Service Provider to be part of disaster recovery efforts and teams in the event of a declared disaster where the solution is also impacted;

10.9.7. As part of bidder's proposals, ACSA expects the Service Provider to put in place a business continuity plan to ensure that if operations are disrupted, services provided to ACSA will not be adversely disrupted. This is over and above disaster recovery/redundancy arrangements; and

10.9.8. It is the responsibility of the Service Providers to ensure their resources are available and reachable at all times and the Services shall be delivered in terms of SABS standards, OHS Act, manufacturer's specifications and other statutory regulations.

10.10. **Preventative maintenance services**

This sub section is an articulation of preventative maintenance services/activities that will be required and they are non-exhaustive. The Bidders must provide a detailed list of maintenance procedures and checks to be performed (Maintenance plan) in addition to the ones listed below and the frequency of such checks or procedures on all the supplied items where applicable.

10.11. **Server activities**

10.11.1. Check and make sure all servers are operational

10.11.2. Do backups

10.11.3. Ensure server's performance (CPU, Memory and HDD space) is within acceptable level.

10.11.4. Make sure that servers are patched (OS patches), If not report to ACSA IT

10.11.5. Make sure that the latest Antivirus is loaded on all systems and If not report to ACSA IT; and

10.11.6. Ensure that all servers and associated equipment are monitored for alerts on ACSA monitoring tool.

10.11.7. Firmware updates on the servers

10.11.8. Event viewer on application and system logs

10.12. **Barriers: Entry and Exit**

10.12.1. Align the booms/barriers;

10.12.2. Check and tighten all nuts and bolts;

10.12.3. Ensure barrier housing is not loose and tighten if necessary;

10.12.4. Ensure the spring is tensioned correctly i.e. boom/barrier opens and closes at the same Speed;

10.12.5. Check the crank arm is securely fitted to motor shaft and the rest of the crank Mechanism;

10.12.6. Replace all worn rubber stoppers;

10.12.7. Clean barrier inside;

10.12.8. Check loop detectors inserted correctly with the correct frequency settings;

10.12.9. Check the cross talks between lanes and adjust if necessary;

10.12.10. Check barrier logic e.g. inserted correctly;

10.12.11. Checks relay e.g. inserted correctly;

10.12.12. Secure incoming mains;

10.12.13. Check barrier drive cable is securely inserted and there are no loose wires; fix all loose wires and report in the monthly report;

10.12.14. Check condition of road surface where loops are and check loop condition; report all findings on the monthly report;

10.12.15. Check barrier arm condition, barrier arm brackets and sheer plates and report all conditions on the monthly report;

10.12.16. Check barrier door locks and secure all locks;

10.12.17. Clean spike grippers and ensure smooth movement; and

10.12.18. Make sure all cables are secured and running in cable trays/conduits.

10.13. **LPR Cameras**

10.13.1. Check picture availability and picture quality, repair where necessary and report all findings in the monthly report;

10.13.2. Check and tighten all nuts and bolts on brackets;

10.13.3. Ensure camera housing and bracket is not loose and tighten if necessary;

10.13.4. Check and adjust camera position for proper picture capturing;

10.13.5. Clean lens, covers and housings;

10.13.6. Check the cross talk between lanes and adjust if necessary;

10.13.7. Secure incoming mains; and

10.13.8. Check camera PSU for correct voltage, rectify where necessary and report findings in the monthly report.

10.14. **Facial Cameras: Entry and Exit**

10.14.1. Check for positioning. Rectify where necessary and report in the monthly report;

10.14.2. Check for picture quality, rectify where required and report findings in the monthly report;

10.14.3. Clean camera lens and housing;

10.14.4. Check and tighten all nuts and bolts;

10.14.5. Check the cross talk between lanes and adjust if necessary.

10.15. **Power Supply Units**

10.15.1. Clean units for dust and dirt;

10.15.2. Check for any ventilation obstructions; and

10.15.3. Check voltage and test for potential overloads.

10.15.4. Check and test UPS and report monthly.

10.16. **Scanner**

10.16.1. Check scanning quality and correct to improve the image quality;

10.16.2. Check batteries and replace if end of life is reached or eminent;

10.16.3. Check and clean scanner lens; and

10.16.4. Clean units for dust and dirt.

10.17. **All Other System Related Devices or Components**

10.17.1. Clean units for dust and dirt; and

10.17.2. Do visual inspections and correct/report irregularities;

11. SUPPORT SERVICES

11.1. Support services refers to day to day support activities performed to resolve incidents that are logged by users of the system or logged by the monitoring tools or alarm and error logs generated by the system's internal monitoring;

11.2. The Service Provider will be required to attend to and resolve all incidents in line with ACSA incident management processes;

11.3. All incidents will be logged on the IT service desk systems. The response and resolution times depicted in table 11 must be adhered to as this will form part of the SLAs that will be agreed to between the Service Provider and ACSA; and

11.4. Penalties will be incurred by the Service Provider if the agreed SLA times are not met.

11.5. **Incident logging procedure**

11.5.1. All incidents must be logged with ACSA service desk via email, telephone or on the self-service web portal;

11.5.2. The incident status must be updated regularly depending on the priority of the incidents until resolution; and

11.5.3. All incidents must be updated with a detailed resolution before closure. The Service Provider must notify the service desk immediately on resolution of the incident.

11.6. **Definition of incident priority**

Table 10 is a disintegration and definition of incident priority levels.

Item #	Priority	Description	Impact
1.	**P1**	Total systems failure/server down or complete loss of system functionality in one or more areas of the airport. The failure has a negative impact to the airports operation.	Critical
2.	**P2**	Multiple devices are down simultaneously however with minimum functionality in the area.	High
3.	**P3**	Failure of single device or components of the systems.	Medium
4.	**P4**	Non-critical fault/failure logged at night or over the weekend. It has no impact on the operations of the airport.	Low

Table 11 : Incident priority definitions

Applicable incident management response as well as resolution times are articulated in table 11.

Incident management response and resolution times (Office hours, After Hours, Weekends and Public Holidays)				
Incident Priority	**Response**	**Restoration**	**Update Feedback**	**Resolution (permanent fix)**
P1	15min	2hrs	15min	Within 6 hours
P2	30min	4hrs	30min	Within 12 hours
P3	60min	4hrs	2hrs	Within 24 hours
P4	4hours	24hrs	6hrs	Within 48 hours

Table 12 : Incident Response and Resolution times

11.7. **Availability requirements**

An ACSA availability requirement for the System is **99.8%** per month. The Service Provider must ensure that the availability targets are met every month. In an event that the target is not met ACSA will impose penalties. The formula for calculation will be provided to the successful Bidder.

11.8. **Penalties**

The Service Provider shall repair all faulty equipment within the times specified in the SLA. The Service Provider will be allowed a grace period of three (3) months to familiarize itself with the operations at all airports before the implementation of penalties can commence.

The following penalties shall apply for failure to resolve incident within the agreed timeline:

Item #	SLA breach	Penalty
1.	P1 Incidents are resolved within one hour after SLA time lapsed for two consecutive times in a measuring period.	20 % of the monthly fee will be deducted per invoice up to 60% in one contractual year thereafter termination procedures will be implemented.
2.	Incidents are resolved within two hours and beyond after SLA time lapsed for three consecutive times.	30 % of the monthly fee will be deducted up to 60% in one contractual year thereafter termination procedures will be implemented.
3.	If a Service Provider misses SLA's in any 3 consecutive months.	50 % of the monthly fee will be deducted.
4.	Fourth missed SLA in one month– 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.

Table 13 : SLA breach and penalty rates

11.8.1. Failure to perform preventative maintenance according to schedule dates shall result in the following penalties.

SLA breach	Penalty
Maintenance not done or proof not submitted.	No payment

Table 14 : SLA Breach and Penalty for Maintenance

12. MEETING AND REPORTING REQUIREMENTS

12.1. Meetings

12.1.1. Project Progress meetings

As part of ongoing performance management, ACSA requires that the Supplier provides the reports articulated in table 15 and attend periodic meetings. These meetings will be

held weekly (every Wednesday), and/or on demand for the duration of the project and arranged by the ACSA Project Management to discuss the following, but not limited to: Project progress delays, risks, issues, financials and all other requirements related to the project.

12.1.2. **Monthly Maintenance meeting**

12.1.2.1. The meetings must be attended by Service Provider's Project Manager as well as ACSA Project Manager;

12.1.2.2. These meetings will be held monthly (during the last week of the month). Purpose of these meetings are to provide the Service Provider a platform to report on their performance for the current month; and

12.1.2.3. If the Service Provider fails to attend any of the scheduled meetings, ACSA will withhold invoice payment for the month.

Table 15 is an articulation of meetings schedule. The project management portion of these meetings will become redundant once the system or solution has been commissioned and handed over to operations. Therefore, the Project board meetings expressed in table 15 will be applicable during the execution part of the project and not during the operational stage.

#	Frequency	Meeting Name	Standing Agenda	Participants and Roles	Documents to be submitted prior to meeting	Documents to be produced after meeting
1.	Monthly (27th or next working day).	SLA meeting.	1. Consumables Usage. 2. Calendar month Incidents (System Availability). 3. Payment. 4. Monthly services deliverables.	1. Service Provider account manager. 2. ACSA representatives. 3. ACSA will chair the meeting.	Maintenance Report.	1. Minutes of meeting. 2. Action items. 3. Penalties. 4. Acceptance of deliverables. 5. Payment status.

			5. Discuss SLA Report. 6. Discuss SLA improvement plan. 7. Discuss penalties.			6. Deliverables for the upcoming month. 7. ACSA will produce minutes and action items.
2.	Monthly - As required.	Project Board meeting.	1. Status. 2. Risks / Issues. 3. Next milestones. 4. Monthly services deliverables.	1. Service Provider account manager. 2. ACSA representatives.	Project Report	1. Minutes of meeting. 2. Action items 3. Acceptance of deliverable. 4. Payment status. 5. Deliverables for the upcoming month.
3.	Adhoc.	Adhoc.	Adhoc.	As and when required.	Either party	Lync (Online) or in Person (Physical).

Table 15 : Meetings schedule

12.2. **Reporting**

Table 16 is an articulation of reports schedule.

#	Frequency	Meeting Name	Standing Agenda	Participants and Roles	Documents to be submitted prior to meeting	Documents to be produced after meeting
1.	Monthly (27th or next working day or date agreed upon by	SLA meeting.	1. Consumables Usage 2. Calendar month Incidents (System Availability).	1. Service Provider account manager. 2. ACSA representatives.	Maintenance Report.	1. Minutes of meeting. 2. Action items. 3. Penalties. 4. Acceptance of deliverables.

	both parties).		3. Payment. 4. Monthly services deliverables. 5. Discuss SLA Report. 6. Discuss SLA improvement plan. 7. Discuss penalties.	3. ACSA will chair the meeting.		5. Payment status 6. Deliverables for the upcoming month 7. ACSA will produce minutes and action items.
2.	Monthly - As required.	Project Board meeting	1. Status 2. Risks / Issues. 3. Next milestones. 4. Monthly services deliverables.	1. Service Provider account manager. 2. ACSA representatives.	Project Report.	1. Minutes of meeting. 2. Action items. 3. Acceptance of deliverables. 4. Payment status 5. Deliverables for the upcoming month.
3.	Adhoc.	Adhoc.	Adhoc.	As and when required.	Either party.	Lync (Online) or in Person (Physical).

Table 16 : Reports schedule

12.2.1. All reports must be submitted three days prior to the meeting day. The meeting will be attended by the Service Provider's account manager, Technical lead, Project manager and ACSA's IT contract management, procurement and end users; and

12.2.2. If reports are not delivered within the stipulated times, ACSA will withhold invoice payment for the month until the reports are submitted and reviewed.

13. DOCUMENTATION

The Service Provider is expected to keep detailed and updated documentation including but not limited to the following.

13.1. Technical architecture diagrams incorporating all architecture domains i.e. Business, Information

(Systems and Technology);

13.2. List of all equipment installed;

13.3. Inventory list of minimum spares required;

13.4. List of decommissioned or old equipment;

13.5. Maintenance report template and schedules;

13.6. Training manual;

13.7. System manual

13.8. Cable route drawings;

13.9. Certifications (electrical, Mechanical and civil)

13.10. Standard operating procedure;

13.11. Daily check list;

13.12. Equipment manuals; and

13.13. Any other relevant documentation

13.14. Prior to the solution going live, the relevant Operational department must ensure that an Operational handover checklist has been duly completed and signed by all relevant stakeholders (Service Provider, Project Team and the applicable Operations department; and

13.15. Accreditation and partnership of OEM. The successful Service Provider is expected to provide written proof of their partnership status with the OEM or any form of accreditation that certifies that the supplier has the necessary resources and skills to work on the specific technologies or devices.