AIRPORTS COMPANY
SOUTH AFRICA

Annexure F:

Service Management, Preventative and Corrective Maintenance Scope of Work – Customer Relationship Management (CRM) Solution.

Tel: +27 (0)11 723 1400 Fax: +27 (0)11 453 9353
The Maples, Riverwoods, 24 Johnson Road, Bedfordview, Gauteng, South Africa, 2007
PO Box 75480, Gardenview, Gauteng South Africa, 2047

www.airports.co.za

Airports Company South Africa SOC Ltd Reg No. 1993/004149/30 VAT no. 4930138393

Contents

List of Tables:

1.0 SERVICE ENVIRONMENT

1.1 Scope of the environment to be Supported

The Scope is directly related to the Scope of Works for the implementation of the CRM Solution

2.0 PERSONNEL

2.1 The provider will be responsible for professional and appropriately certified staffing to meet the Services Roles and Responsibilities and Service Levels set forth in this services specification.

2.2 Suitably certified resources are required onsite at some locations for preventative and corrective maintenance. Airport operating hours will prevail but may extend to after-hours requirements due to window periods of downtime required for specific areas of maintenance and disruptive incidents.

2.3 Providers should adapt their resourcing model to meet the Service Level Agreement which includes either permanent onsite and\or variable offsite resources for preventative and corrective maintenance respectively.

2.4 Dedicated on-site resources for operations to be proposed by the service provider tying up to the stipulated SLA's.

2.5 All resources must sign the ACSA Non-Disclosure Agreement as supplied in this tender. Successful supplier will need to obtain permits (e.g., access control) whereby security vetting and background checks will be a pre-requisite.

2.6 Service provider will provide required resources to meet and deliver on the stipulated SLA's. The following are the minimum functions ACSA requires:

High Level Functions

High Level Function	Coverage
Provide 1st and 2nd Line technical support to troubleshoot complex issues including diagnosing and resolving integration issues, software application issues, network & connectivity issues, hardware and equipment failures etc.	24 x 7
Provide technical support in dealing mostly with IMACD's, fix/ swop equipment on the floors specific reported incidents and service requests and dispatching in-scope hardware related callouts. This function is performed from the service desk and includes 24x7 monitoring of the national infrastructure with senior technical support engineers.	24 x 7

2.7 **The provider will be liable to pay office rental space for any resources that are deemed necessary to be located onsite at any ACSA premises. The applicable rates must be agreed between the provider and ACSA Property Department.**

2.8 The provider will be liable to pay parking fees for any resources that are deemed necessary to be located onsite or perform work under this contract at any ACSA premises.

2.9 The provider will be liable for any fees and training necessary to obtain ACSA Security and Access Permits for any resources that are deemed necessary to be located onsite or perform work under this contract at any ACSA premises.

2.10 Certified resources will be required for support, preventative, and corrective maintenance of the services during below coverage windows.

Service Coverage Windows

<table>
<tr><th>Service Class</th><th>Service Coverage Window</th></tr>
<tr><td>Standard</td><td>Normal Office Hours - 06:00 - 18:00 on Mon - Fri, excluding public holidays</td></tr>
<tr><td>Weekday After Hours</td><td>After Hours – 18:00 – 06:00 on Mon – Fri, excluding public holidays</td></tr>
<tr><td>Weekends</td><td>Weekend and Public Holidays – 24 Hours Saturday and Sunday, including public holidays</td></tr>
<tr><td>Project & IMACD</td><td>All project and IMACD tasks that impact the live environment will take place after the last flight has departed and before the first flight departs/arrives in the morning. These hours vary from airport to airport, but generally the provider can plan to run project tasks between 23h30 and 05h00, times are subject to change and will be communicated timeously

ON SITE SUPPORT - HUB SITES
<table>
<tr><th>Airport</th><th>Weekdays & Weekends</th></tr>
<tr><td>OR Tambo International</td><td>24 hours</td></tr>
<tr><td>Cape Town International</td><td>04:00am – 01:00am</td></tr>
<tr><td>King Shaka International</td><td>05:00am - 22:00pm</td></tr>
</table>
</td></tr>
</table>

Service Coverage Windows

2.11 **T**he provider should ensure a resourcing model is in place that allows achievement of the SLAs and ensure ability to deliver service during the defined Service Coverage Windows. The provider is to ensure a full complement of resources at all times.

2.12 If resources are absent from the site they are assigned to, the provider must replace the said resource for the duration of their absence, with an equally competent and qualified resource. The stand in resource must have the required access permits, training, and site knowledge.

2.13 The provider must have resources dedicated solely to service management and maintenance activities related to the passenger self-service programme.

2.14 The Bidder must complete a safety file in accordance with ACSA standards within the 1st month of commencement of services. This file must be kept up to date always. If this is not necessary communication will be provided

3.0 EQUIPMENT AND SPARES HOLDING REQUIREMENTS

3.1 The provider is required to ensure that all service technicians are equipped with the appropriate tool kits and testing equipment to perform their functions without delay.

3.2 The provider is required to ensure that enough critical spares are available for the maintenance of the environment to meet the SLAs at all locations.

3.3 The provider should honour the SLA and must have its own backup/ loan stock available to restore service within the specified maintenance SLA.

3.4 The replacement and/or repair of faulty or malfunctioning components shall be performed by the provider using original parts and/or components, each guaranteed as new by its manufacturer and of the same grade or release as the part or component which requires replacement; if such a component is not available, it shall be replaced by a component of a higher grade. Any part or component that is replaced shall be certified by the manufacturer of the device.

3.5 The provider shall carry out replacements using its own parts. To ensure that this is possible, The provider undertakes to establish – within sixty (60) days of the notification that it has been awarded this tender – a warehouse or safe capable of storing any such part or component required to ensure full compliance with the SLA, including in-scope devices and equipment declared to be obsolete and no longer supported by the manufacturers' technical maintenance services and for which "end of maintenance" notifications have already been issued (End of SW Maintenance Releases Date: H/W, End of Routine Failure Analysis Date: H/W, End of New Service Attachment Date: H/W, End of Service Contract Renewal Date: H/W, Last Date of Support: H/W and similar).

4.0 PREVENTATIVE AND CORRECTIVE MAINTENANCE

4.1 Preventative Maintenance includes planned overhauls, replacements, inspections, tests, software upgrades, firmware upgrades, patch management and any activity aimed at preventing failures through maintaining the condition of the infrastructure or assessing its condition for the purposes of corrective maintenance.

4.2 Corrective maintenance includes all activities following a preventative maintenance inspection.

4.3 Break/fix includes maintenance that is unforeseen and is necessary to restore the serviceability of the **Intelligent Integrated Security Platform** infrastructure, and functionality of the System. Some of this break/fix maintenance could be requested after hours on weekend and public holiday. Service providers will be expected to respond and attend to all the faults

4.4 The provider must make provision for after hours, weekends and public holidays support, no additional costs will be entertained

4.5 For planned activities, notice will be given to the provider to make available resources as and when required.

4.6 The provider must provide after-hours telephone numbers, where support personnel are reachable. It is the responsibility of the Service providers to ensure that their resources are available and reachable always; and that any changes to after-hours telephone numbers are communicated to ACSA.

4.7 The Preventative Maintenance Schedules table provide a high-level maintenance schedule and tasks/checks.

The provider is expected to provide a detailed preventative and corrective maintenance plan/schedule incorporating the below as a minimum as part of the response to this RFP. In the detailed preventative maintenance schedule, the provider must include all remedial actions to be taken (include what communication will be actioned, which provider resource will be responsible for the communication, to which ACSA resource the communication will be addressed to, in what format, what timelines after the incident is detected and what follow up mechanism will be in place) if any issues are found during the maintenance schedule routine.

5.0 ROLES AND RESPONSIBILITIES

In this SOW, we use the RASCI ("responsible, accountable, supporting, consulted and informed") chart approach for all roles and responsibilities matrices.
The RACI terminology is as follows:

Code	Role	Role Detail Description	
R	Responsible	Individual operationally responsible for performing a sourcing activity. Responsible individuals report to the Accountable individual.	Only one individual is accountable for any given activity. Responsible is a proactive role.
A	Accountable	Individual with final accountability for the results of a sourcing activity. Accountability includes a mandate to dismiss or accept the results by activity as realized by the Responsible individual. This individual also holds the budget to back the mandate.	Only one individual is accountable for any given activity. Accountable is a reactive role.
S	Supporting	Individuals who support the Responsible individual in realizing the sourcing activity. They actively participate in realizing/executing/performing the activity. Supportive individuals report to the Responsible individual.	Multiple individuals can participate in support of the Responsible individual for any given activity. Supporting is a proactive role.
C	Consulted	Individuals who should be consulted in realizing/executing/performing the activity, on the scope, budget, time, and value of the activity.	Multiple individuals can be required to be heard for any given activity. Consulted is a reactive role.
I	Informed	Individuals who need to be informed but have no role in the realization/execution/performance of an activity, other than being informed of the result of the activity.	Multiple individuals can be informed of the results of any given activity. Informed is a passive role.

Table 1 - Definition of RASCI Model

The following table identifies the roles and responsibilities associated with this SOW

5.1 Roles and Responsibilities- General

Sub area	Number	Task/Activity	Provider	ACSA
General	1.	Provide Services and the supporting processes that support ACSA business needs, technical requirements, and End-User requirements	R, A	C
	2.	Approve Services and the supporting processes that support ACSA's business needs, technical requirements and End-User requirements	I	R
	3.	Comply with ACSA policies, guiding principles, standards and regulatory requirements applicable to the ACSA for information, information systems, personnel, physical and technical security	R, A	C
	4.	Develop and maintain an approved comprehensive Standards and Procedures Manual that contains the standards, processes and procedures that will be used in the delivery of all Services. The manual will include clearly delineated roles and responsibilities, touch points and measurements between ACSA and the vendor.	R, A	C
	5.	Approve the comprehensive Standards and Procedures Manual that contains the standards, processes and procedures that will be used in the delivery of all Services. The manual will include clearly delineated roles and responsibilities, touch points and measurements between ACSA and the vendor.	I	R
	6.	Conform to changes in laws, regulations and policies. Major Service Changes shall be proposed on a project-by-project effort basis to alter the environment to conform to the new requirements.	R	C, A
	7.	Report performance against Service-Level Requirements (SLRs)	R, A	I
	8.	Coordinate all Changes to the IT systems that may affect the SLRs of any other Service	R, A	C, I
	9.	Provide timely creation, updating, maintenance and provision of all appropriate project plans, project time and cost estimates, technical specifications, management documentation and management reporting in a form/format that is acceptable to the ACSA for all Service projects and major Service activities	R, A	C
	10.	Adhere to IT service management (ITSM) best practices and Key Performance Indicators (KPIs)	R, A	I
	11.	Approve the use of the ITSM best practices and KPIs	C, I	R
Site Access	12.	Coordinate with site IT staff to schedule On-Site Technical Support visit when using non-regular or 3rd party resources	R, A	C, I
	13.	Ensure that all support staff has valid airside permits for the airports that they support.	R, A	C, I
	14.	Ensure that support staff strictly adheres to the terms and conditions of their permit allowances	R, A	C, I
	15.	Ensure that support staff has access to reliable transport and valid driver's licences. This includes access services provider vehicle that is permitted on airside should there be a requirement to support any device on airside. The operator must have a valid Airport Vehicle Operators Permit (AVOP). The vehicle requires a regulatory permit and must be insured as per ACSA requirements.	R, A	C, I
	16.	Support staff must have the relevant safety certifications, protective wear and equipment to carry out corrective maintenance duties.	R, A	C, I

Sub area	Number	Task/Activity	Provider	ACSA
	17.	Ensure that the provider always has a valid health and safety file	R, A	C, I
	18.	On request from the provider ACSA will provide access to ACSA premises (which will not be unreasonably withheld) to the provider or their 3rd party personnel to effect maintenance and repairs	I	R, A
	19.	Parking fees at ACSA premises	R, A	I
	20.	Rental of office space at ACSA premises	R, A	I
	21.	Any security related training and payments for access to ACSA premises	R, A	I

Table 2 - Roles and Responsibilities - General

5.2 Roles and Responsibilities - Management, Planning, and design

Architecture Planning and Analysis Services are the activities required to assess the requirements for architectural, functional, performance, IT Service Continuity, and security requirements

Activities associated with the documenting the requirements for architectural, functional, performance, IT Service Continuity, and security requirements

Include identifying the opportunities to improve the efficiency and effectiveness of the Service.

Can also help support competitive business advantage and mitigate risks by reducing defects and improving the quality of IT Services look at current and how to bring in efficiencies and improvements

Sub area	Number	Task/Activity	Provider	ACSA
Architecture Planning and Analysis	1.	Adhere to, implement, and ensure alignment to the defined standards, timeframes and reporting requirements for planning, project management and analysis activities.	R, A	C,S,I
	2.	Attend and actively participate in the ACSA scheduled focus groups, stakeholder meetings, project, and technical workshops to provide the required expertise (addressing all tasks pre and post the meeting as required such as requirements gathering activities; solution design options)	R, A	C, S, I
	3.	Provide input into the review of the existing Services, architectural standards and project management practices for Planning and Analysis activities to ensure continuous alignment to best practise.	R, A	C, S, I
	4.	Ensure all documentation remains updated in required ACSA format. Where no existing documentation is available, the standards are to be followed and documentation to be drafted.	R, A	C, I
	5.	Define Services, standards, timeframes and reporting requirements for planning, project management, and analysis activities	C, S, I	R, A
	6.	Schedule the required focus groups and technical workshops for architecture planning and analysis requirements – such as to review the existing infrastructure topologies at an enterprise (e.g., technology strategy, technology architecture, functional, availability, capacity, performance, backup and IT Service Continuity)	S, I	R, A
	7.	Provide ACSA documentation format standards. Review and approve updated documentation presented by Service provider	I	R, A
	8.	Review and update the existing Services, standards and project management practices for Planning and Analysis activities	I	R, A

Sub area	Number	Task/Activity	Provider	ACSA
Technical Architecture	9.	Attend, actively participate in and provide technical assistance and subject matter expertise in technical and business planning sessions to review standards, architecture and project initiatives to align with best practise	R, A	C, S, I
	10.	Document current and future Technical Architecture in the agreed formats and update these throughout the service lifecycle	R, A	C, S, I
	11.	Perform evaluation of new equipment considered for implementation in compliance with the ACSA's security and IT architecture policies, regulations and procedures.	C, S, I	R, A
	12.	Define and approve any new architecture standards	C, S, I	R, A
	13.	Conduct technical and business planning sessions to review standards, architecture and project initiatives to align with best practises	R, A	C, S, I
Continuous Improvement and Innovation Planning	14.	Conduct technical reviews and provide recommendations for improvements that increase efficiency, effectiveness and reduce costs	R, A	C, I
	15.	Perform ad hoc investigations as requested by ACSA and submit recommendations for ACSA's consideration.	R, A	C, I
	16.	Conduct on-going, regular planning and recommendations for technology refresh and upgrades	R, A	C, I
	17.	Showcase new technology enhancements to ACSA hence allowing ACSA the option to upgrade to any new productised technology.	R, A	C, I
	18.	Review and approve any technical improvement recommendations	C, I	R, A
	19.	Review and approve any requested ad hoc investigations	C, I	R, A
	20.	Review and approve recommendations for technology refresh and upgrades	C, I	R, A
	21.	Review any new technology enhancements presented	C, I	R, A
Management and Testing Tools	22.	Use existing System management tools to monitor measure, manage and document the environment.	R, A	C, I
	23.	Provide access to existing System management tools to monitor measure, manage and document environment	C, I	R, A
Research	24.	Provide expert advice and research latest technologies on a constant basis and formally submit these presentations to ACSA IT Infrastructure on a 3-monthly basis.	R, A	C, I
	25.	Together with ACSA-IT perform feasibility studies for the implementation of new and existing technologies that best meet ACSA business needs and meet cost, performance and quality objectives.	R, A	C, I
	26.	Review the latest technologies presented by the Service provider.	C, I	R, A
Design and panning		Provide design documentation for quarterly audits as requested by ACSA	R, A	C, I
	27.	Provide input into design plans through coordination with the appropriate ACSA technology standards groups and design architects	C, I, S	R, A
	28.	Quarterly audit of design documentation	C, I, S	R, A
	29.	Adhere to production acceptance test criteria	R, A	C, I
	30.	Conduct and document test plans and results	R, A	C, I

Sub area	Number	Task/Activity	Provider	ACSA
	31.	Define and document production acceptance test criteria	C, I	R, A
	32.	Review and approve test plans and results	C, I	R, A

Table 3 - Roles and Responsibilities - Management, Planning, and design

5.3 Roles and Responsibilities - Project Management Services

ACSA may from time-to-time request that the provider perform a discrete set of activities in addition to the on-going services obligations. (a "Project").

Sub area	Number	Task/Activity	provider	ACSA
Management Project Approach	1.	Utilise project management methodologies, knowledge, skills, tools, and techniques consistent with leading internationally recognised and accepted project management practices such as those contained in the Guide to the Project Management Body of Knowledge (PMBOK) or Prince2	R, A	C, I
	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	C, I	R, A
Define Project Plan	3.	Provide project definition and plan, identify major critical milestones, ensure delivery within budget and project deliverables aligned and approved by the ACSA Project Manager	R, A	C, I
	4.	Provide, maintain, and update detailed project planning, identify critical path dependencies.	R, A	C, I
	5.	Approve project plan, critical milestones, budget forecast, and project deliverables	C, I	R, A
	6.	Attend scheduled weekly project meetings to review detailed project plan and critical path dependencies	C, I	R, A
Manage Execution of the Project	7.	Manage, follow up and track execution of project plan.	R, A	C, I
	8.	Ensure project plan management activities are carried out and ensure updated communication to project stakeholders is done.	C, I	R, A
Monitor Project Progress	9.	Report on project progress, budget, risk, issues	R, A	C, I
	10.	Review and escalate any issues risk etc. for action to higher governance authorities as required	C, I	R, A

Table 4 - Roles and Responsibilities - Project Management Services

5.4 Roles and Responsibilities - Acquisition and Management

The acquisition and management process include the purchase of all service equipment, including new equipment, upgrades to existing equipment, or purchases resulting from a service or repair request. Also, maintains buying catalogue, execution of purchase orders, provides quotations, deals with goods handling.

Sub area	Number	Task/Activity	provider	ACSA
Policies, Processes, Standards and	1.	When procurement is requested by ACSA-IT, provider to adhere to acquisition/procurement policies	R, A	C, I
	2.	Provide guidance on ACSA acquisition/procurement policies	C, I	R, A
	3.	Develop, document and maintain in the Standards and Procedures Manual Acquisition and Management procedures that meet requirements and adhere to defined policies	R, A	C, I
	4.	Review and approve Acquisition and Management procedures	C, I	R, A

Sub area	Number	Task/Activity	provider	ACSA
	5.	Perform periodic audits of procurement procedures	R, A	C, I
Demand Management	6.	Escalate any acquisition and management issues to ACSA-IT, notify ACSA immediately upon learning of item shortages, and notify ACSA-IT of out-of-line (e.g., out-of-stock occurrences) deliveries.	R, A	C, I
	7.	Attend monthly review sessions to understand estimated consumption forecast where available to ensure achievement of timelines	R, A	C, I
	8.	Address any acquisition and management escalations from Service provider	C, I	R, A
	9.	Quarterly, ACSA shall provide the Service provider with its estimated consumption forecast of all in scope infrastructure equipment. The forecast process will be a joint effort between ACSA and the provider using historical data.	C, I	R, A
Equipment Delivery	10.	Ensure all equipment is delivered as scheduled. No uncommunicated delays in delivery will be accepted by ACSA-IT. Any delays are to be communicated in writing and in the relevant meeting (project meeting) to allow for review and any possible business impacts	R, A	C, I
	11.	Request updates on equipment delivery timelines in the relevant meetings (project meetings etc.)	C, I	R, A
Standards Compliance	12.	Ensure that new equipment/ hardware complies with established ACSA standards and architectures	R, A	C, I
	13.	Ensure all procured hardware and software is listed as part of the ACSA architecture technology standards	C, I	R, A
Goods Handling and Warehousing	14.	Provide facilities for spares holding nationally at the provider's Locations.	R, A	C, I
	15.	Securely store and ensure equipment at designated Service Locations (as agreed with ACSA)	R, A	C, I
	16.	Control and manage the equipment in a secure and auditable manner.	R, A	C, I
	17.	Manage the physical movement (appropriate packing and transportation) of service in scope equipment as required and agreed with ACSA	R, A	C, I
	18.	Allow ACSA audits when requested by ACSA	R, A	C, I
	19.	Inspect provider's location nationally to confirm required security is in place	C, I	R, A
	20.	Provide proof of valid insurance coverage for equipment held by the provider on ACSA behalf	R, A	C, I
	21.	Ad hoc inspections of equipment being moved to insure appropriate packaging and transportation	C, I	R, A
Equipment Inventory Holding	22.	Maintain adequate equipment inventory levels in accordance with SLA obligations.	R, A	C, I
	23.	Report on stock levels quarterly	R, A	C, I

Table 5 - Roles and Responsibilities - Acquisition and Management

5.5 Roles and Responsibilities - Documentation

Documentation Services are the activities associated with developing, revising, archiving, maintaining, managing, reproducing, and distributing information (e.g., project planning materials, System design specifications, Procedures Manuals, operations guides) in hard copy and electronic form.

Sub area	Number	Task/Activity	provider	ACSA

Documentation	1.	Ensure that the entire Intelligent Integrated Security Platform infrastructure is well documented and constantly updated	R, A	C, I
	2.	Compile a checklist and all documentation for carrying out of maintenance tasks related to in scope Intelligent Integrated Security Platform Infrastructure Intelligent Integrated Security Platform (detailed maintenance plan). Provide exception reports where risks and issues cannot be addressed via the maintenance plan	R, A	C, I
	3.	A detailed checklist template will be presented to the ACSA for approval.	R, A	C, I
	4.	Specify the content, purpose, format and production schedule of all documents	R, A	C, I
	5.	Store all copies of documents on ACSA Microsoft Teams sites provided.	R, A	C, I
	6.	Review and approve in scope documentation to ensure the Intelligent Integrated Security Platform infrastructure is well documented and constantly updated	I	R, A
	7.	Review checklist and implement action plans based on any exception reports and recommendations	I	R, A
	8.	Work with provider to specify the content, purpose, format and production schedule of all documents within scope	C, I	R, A
	9.	Provide space to store physical copies of all documents and share folder for digital copies of the documents	I	R, A
	10.	Provide timely creation, updating, maintenance and provision of all documentation, (design documents; architectural diagrams; as built documents; test plans; all ACSA required project documentation; technical specifications, preventative and corrective maintenance plans and checklist; escalation reports; daily service request report; floor layout diagrams; OEM and third party documentation and management reporting in a form/format that is acceptable to ACSA for Service Projects and major Service activities	R, A	C, I
	11.	Manage all documentation in accordance with Configuration Management standards and guidelines	R, A	C, I
	12.	Document standard operating procedures (e.g., boot, failover/disaster recovery/COOP, spool management, batch processing, backup)	R, A	I
	13.	Review and approve standard operation procedures Documentation	I	R, A

Table 6 - Roles and Responsibilities - Documentation

5.6 Roles and Responsibilities - Technology Refresh and Replenishment

Technology Refreshment and Replenishment (TR&R) Services are the activities associated with modernizing the IT environment on a continual basis, to ensure that the system components stay current with evolving industry-standard technology platforms.

Sub area	Number	Task/Activity	provider	ACSA
Technology Refresh and Replenishment	1.	Recommend TR&R life cycle management policies, procedures and plans appropriate for support of ACSA business requirements	R, A	C, I
	2.	Develop, document, and maintain in the Standards and Procedures Manual TR&R procedures, and develop TR&R plans that meet requirements as well as adhere to defined policies and Change and Release Management processes	R, A	C, I
	3.	Review and approve TR&R policies, procedures, and plans	I	R, A
	4.	Perform the necessary tasks required to fulfil the TR&R plans	R, A	I
	5.	Provide management reports on the progress of the TR&R plans	R, A	I
	6.	Periodically review the approved TR&R implementation plans to ensure they properly support ACSA business requirements	I	R, A

Table 7 - Roles and Responsibilities - Technology Refresh and Replenishment

5.7 Roles and Responsibilities - Infrastructure Build and Change

Managing all the Intelligent Integrated Security Platform infrastructure changes [standard, low, med, high risk] within all operations and projects of the airports. This includes initiating change requests and closing out change requests.
IMACDs will be treated as projects when the following is met:

- Ad hoc IT related installation requests from IT Commercial
- Upgrades to any existing or live facility
- Hardware decommissioning
- Hardware installation

Sub area	Number	Task/Activity	provider	ACSA
Installations and Additions	1.	Complete IMACD plan per installation and addition	R, A	C, I
	2.	Present IMACD plan to ACSA for approval	R, A	C, I
	3.	Complete IMACD Installations and additions per approved IMACD plan (timelines / tasks / pre-installation checks / UAT etc.)	R, A	C, I
	4.	Receive and review IMACD plan per installation and addition presented by Service provider	I	R, A
	5.	Approve IMACD plans received from Service provider	I	R, A
	6.	Approve and sign off IMACD installations and additions in alignment with approved plans	I	R, A
Moves	7.	Complete IMACD plan per installation and addition	R, A	C, I
	8.	Present IMACD plan to ACSA for approval	R, A	C, I
	9.	Complete IMACD Installations and additions per approved IMACD plan (timelines / tasks / pre-installation checks / UAT etc.)	R, A	C, I
	10.	Receive and review IMACD plan per installation and addition presented by Service provider	I	R, A
	11.	Approve IMACD plans received from Service provider	I	R, A
	12.	Approve and sign off IMACD installations and additions in alignment with approved plans	I	R, A
Change	13.	Recommend changes to meet service requirements	R, A	C, I

Sub area	Number	Task/Activity	provider	ACSA
	14.	Perform changes to meet business requirements	R, A	C, I
	15.	Review and approve recommended changes presented by the provider where required	I	R, A
	16.	Sign off implemented changes	I	R, A
Decommission	17.	Complete IMACD plan per decommission requirement	R, A	C, I
	18.	Present IMACD plan to ACSA for approval	R, A	C, I
	19.	Complete IMACD decommission per approved IMACD plan (timelines / tasks / pre-decommission checks / UAT etc.)	R, A	C, I
	20.	Disposal of equipment and materials in accordance with ACSA policies upon request.	R, A	C, I
	21.	Receive and review IMACD plan per decommission by Service provider	I	R, A
	22.	Approve IMACD plans received from Service provider	I	R, A
	23.	Approve and sign off IMACD decommission in alignment with approved plans	I	R, A
	24.	Sign off the disposal of equipment and materials in accordance with ACSA policies with Service provider, and ensure financial asset disposal tasks are completed	I	R, A
IMACD Completion Sign-Off	25.	Conduct and document production acceptance tests and provide results to obtain signed completion form (production acceptance) from ACSA	R, A	C, I
	26.	All works must have before, during and after photos taken which will be submitted with the hand over pack. This applies to every task, including removal of old electrical cabling and piping, new installations, upgrades to existing facilities, etc. Photographs may be combined with video recordings. This form of documentation will be required during audits, meetings, etc.	R, A	C, I
	27.	Maintain and update records to ensure baseline CMDB is always up to date	R, A	C, I
	28.	Review acceptance test and results for sign off	I	R, A
	29.	Review before during and after photos taken during changes	I	R, A
	30.	Review CMDB baseline reports quarterly as defined in report schedule	I	R, A

Table 8 - Roles and Responsibilities - Infrastructure Build and Change

5.8 Roles and Responsibilities – Maintenance

Maintenance Services are the activities associated with the maintenance and repair of hardware, software to include "break/fix" Services. Installed platform and product version levels are not to be more than one version behind the current commercial release, unless coordinated with ACSA architectural standards committee.

Sub area	Number	Task/Activity	provider	ACSA
Maintenance	1.	Define Maintenance requirements	I	R, A
	2.	Develop, document and maintain in the Standards and Procedures Manual Maintenance procedures that meet requirements and adhere to defined policies	R, A	I
	3.	Develop Maintenance schedules (OEM recommended preventative maintenance to be considered)	R, A	
	4.	Review and approve Maintenance procedures and schedules	I	R, A
	5.	Ensure appropriate Maintenance coverage for all Service components	R, A	C, I
	6.	Provide Maintenance and break/fix support in ACSA's defined locations, including dispatching repair technicians to the point-of-service location if necessary	R, A	C, I
	7.	Perform (and/or coordinate with Third-Party Maintenance Vendor if applicable) diagnostics and maintenance on Service components, including hardware, software, peripherals and special-purpose devices as appropriate	R, A	C, I
	8.	Perform an analysis of the impact and/or applicability of Vendor-provided (e.g., Omni) patches and/or service packs, in accordance with ACSA policies and requirements	R, A	C, I
	9.	Approve Vendor-provided patches and/or service packs	C, I	R, A
	10.	Review all patches relevant to the IT environment and classify the need and speed at which the Security patches should be installed, as defined by policies and Change Management	R, A	C, I
	11.	Install patches per ACSA's Change Management process and procedures including acquiring required ACSA approval	R, A	C, I
	12.	Install (and/or coordinate with Third-Party Maintenance Vendor if applicable) manufacturer field change orders, service packs, firmware and software maintenance releases, etc.	R, A	C, I
	13.	Perform (and/or coordinate with Third-Party Maintenance Vendor if applicable) product patch, "bug fix," service pack installation or upgrades to the current installed version	R, A	C, I
	14.	Perform Maintenance-related software distribution and version control, both electronic and manual	R, A	C, I
	15.	Replace (and/or coordinate with Third-Party Maintenance Vendor if applicable) defective parts, including preventive Maintenance, according to the manufacturer's published mean-time-between-failure rates	R, A	I
	16.	Conduct (and/or coordinate with Third-Party Maintenance Vendor if applicable) Maintenance and parts management and monitoring during warranty and off-warranty periods	R, A	I

Sub area	Number	Task/Activity	provider	ACSA
	17.	Execute preventative maintenance per the high-level schedule which needs further development by provider responding to this RFP. The following activities will constitute the minimum requirements. • Inspections and alerts investigations • Syslog analysis – Continuous monitoring and responding with corrective actions to warnings and alerts. • Health Checks • Configuration Backups • Log Analysis • Device performance monitoring for high memory and CPU utilization • Software upgrades on management systems • Capacity Management • User Management • Redundancy Testing • Firmware Upgrades • Advise / recommend improvement for the Self-Service infrastructure and identify potential risks within the environment include detailed additional preventative maintenance recommendations which as experts in the field are deemed necessary to prevent system failures	R, A	C, I
	18.	Initiate projects to execute on approved preventative maintenance recommendations	I, C	R, A
	19.	Provide detailed monthly reports on capacity, assets, changes, faults, potential risks, etc. as defined in the report schedule	R, A	C, I

Table 9 - Roles and Responsibilities – Maintenance

5.9 Roles and Responsibilities - Infrastructure Monitoring, Operations and Administration

Monitoring, Operations and Administration are the activities associated with providing a stable environment thus ensuring a proactive approach to risk mitigation and will aid the provider to meet their SLA targets.

Management of the Intelligent Integrated Security Platform infrastructure will always be done in consultation with ACSA-IT Airport Systems and Operations and no decisions can be made without approvals and written consent of ACSA

Sub area	Number	Task/Activity	provider	ACSA
Management and Administration	1.	Utilise ACSA Monitoring tools to monitor the Intelligent Integrated Security Platform infrastructure. ensuring that it meets the monitoring and service level reporting requirements	R, A	C, I
	2.	Implement measures for proactive monitoring to limit Intelligent Integrated Security Platform infrastructure outages.	R, A	C, I
	3.	Manage all in scope Intelligent Integrated Security Platform infrastructure elements in accordance with ACSA's policies (including security oversight and change management policies)	R, A	C, I
	4.	Manage and coordinate provider appointed subcontractors and Third Parties to meet Service and SLA requirements	R, A	C, I
	5.	Suggest any additions or changes to ACSA monitoring tools landscape	R, A	C, I

Sub area	Number	Task/Activity	provider	ACSA
	6.	Install, customise and maintain an Intelligent Integrated Security management system for event monitoring and availability reporting.	I	R, A
	7.	Implement measures for proactive monitoring to limit Intelligent Integrated Security Platform infrastructure outages	I	R, A

Table 10 - Roles and Responsibilities - Monitoring, Operations and Administration

5.10 Roles and Responsibilities - Availability Management

The goal of Availability Management is to understand the overall availability requirements of ACSA's business needs and to plan, measure, monitor and continuously strive to improve the availability of the Intelligent Integrated Security Platform infrastructure, services and supporting IT organization to ensure these requirements are met consistently, with a focus on providing cost-effective availability improvements that deliver measurable ACSA business benefits.

Availability Management covers the evaluation, design, implementation, measurement and management of the Intelligent Integrated Security Platform Infrastructure Availability from a component and an end-to-end perspective (i.e., Services), including new or modified IT Service Management methodologies and tools, as well as technology modifications or upgrades Intelligent Integrated Security Platform infrastructure systems and components. The goal of the Availability Management process is to optimize the capability of the Intelligent Integrated Security Platform infrastructure, services and supporting organization to deliver a cost-effective and sustained level of Availability that enables the business to satisfy its business objectives.

Key activities of the Availability Management process are as follows:

- Determining business requirements for a new or enhanced IT Service and formulating the availability and recovery design criteria for the Intelligent Integrated Security Platform infrastructure to ensure IT Services are designed to deliver the appropriate levels
- Determining the critical business functions and impact arising from IT component failure. Where appropriate, reviewing the availability design criteria to provide additional resilience to prevent or minimize impact to the business.
- Identifying opportunities to optimize the availability of the Intelligent Integrated Security Platform infrastructure to deliver cost-effective improvements that deliver tangible business benefits
- Supporting the targets for availability, reliability and maintainability for the Intelligent Integrated Security Platform infrastructure components that underpin the IT Service, to enable these to be documented and agreed within SLAs and contracts
- Establishing measures and reporting of availability, reliability and maintainability that reflect the business, End-User and IT support organization perspectives
- Monitoring and trend analysis of the availability, reliability and maintainability of IT systems and components
- Reviewing IT Service, system and component availability, identifying unacceptable levels and ensuring appropriate corrective actions are taken to address shortfalls
- Investigating the underlying reasons for unacceptable availability and providing recommendations for resolution
- Producing and maintaining a forward-looking Availability Plan, which prioritizes and plans overall improvements aimed at improving the overall availability of IT Services and Intelligent Integrated Security Platform infrastructure to ensure that existing and future business availability requirements can be met
- Providing reports to ensure that agreed levels of availability, reliability and maintainability are measured and monitored on an ongoing basis

Sub area	Number	Task/Activity	provider	ACSA
Availability Management	1.	Establish criteria and SLRs for Availability Management support requirements, including IT systems and services to be covered	C, I	R, A
	2.	Develop Availability Management policies, process and procedures, and determine appropriate Availability Management tools and methods that support ACSA's Availability Management support requirements	R, A	I
	3.	Participate in the development of Availability Management policies, process and procedures, and identify the tools and availability methods to be used	I	R, A
	4.	Review and approve Availability Management policies, processes and procedures	I	R, A
	5.	Implement agreed-upon Availability Management policies, processes and procedures	R, A	I
	6.	Provide unrestricted read access by ACSA-authorized staff and designated personnel to all current and historical availability knowledgebase data and records	R, A	I
	7.	Ensure that availability requirements are included when requirements are identified, when upgrading and/or designing new IT systems and services to support business users	I	R, A
	8.	Participate in user requirements gathering and analysis when upgrading and/or designing new IT systems and services, to ensure that they are designed to deliver the required levels of availability (mapped to the SLRs) required by the business	R, A	I
	9.	Create availability and recovery design criteria to be applied to upgrades and/or new or enhanced Intelligent Integrated Security Platform design	R, A	I
	10.	Participate in creating availability and recovery design criteria to be applied to upgrades and/or new Intelligent Integrated Security Platform and services design	I	R, A
	11.	Coordinate with the IT service support and IT service delivery process owners and managers from ACSA to research, review and assess Availability issues and optimization opportunities	R, A	C, I
	12.	Define the availability measures and reporting required for the Intelligent Integrated Security Platform infrastructure and its components that underpin an upgraded and/or new IT Service, as the basis for an SLA that reflects business, End-User and IT support organization requirements	I	R, A
	13.	Participate with ACSA in defining the availability measures and reporting requirements	R, A	I
	14.	Recommend appropriate tools and practices to measure and report on agreed-upon availability measures for upgraded and/or enhanced Intelligent Integrated Security Platform infrastructure	R, A	I
	15.	Review and approve availability measurement tools and practices	I	R, A
	16.	Ensure that approved availability measurement tools and practices are implemented	R, A	I
	17.	Monitor and maintain an awareness of technology advancements and IT best practices related to availability optimization, and periodically provide updates to ACSA IT management	R, A	I
	18.	Ensure that all Availability Management improvement initiatives conform to defined Change Management procedures set forth in the Process and Procedures Manual	R, A	I
	19.	Participate in Problem Management review sessions as appropriate, specifically those problems related to outages of critical systems	R, A	C, I
	20.	Monitor actual Intelligent Integrated Security Platform infrastructure achieved versus targets and ensure shortfalls are addressed promptly and effectively	R, A	I

Sub area	Number	Task/Activity	provider	ACSA
	21.	Conduct Availability Assessment review sessions and provide cost-justified improvement recommendations	R, A	I
	22.	Participate in availability improvement review sessions	I	R, A
	23.	Review and approve cost-justifiable improvement recommendations that ACSA deems appropriate to enhance ACSA IT and business performance needs	I	R, A
	24.	Coordinate with ACSA and Third-Party Service Vendors to gather information on IT systems and service availability issues and trends, to be used for trend analysis	R, A	I
	25.	reduce and maintain an Availability Plan that prioritizes, and plans approved Intelligent Integrated Security Platform infrastructure improvements	R, A	I
	26.	Review and approve Availability Plan	I	R, A
	27.	Provide Intelligent Integrated Security Platform infrastructure reporting to ensure that agreed levels of availability, reliability and maintainability are measured, reported and monitored on an ongoing basis	R, A	I
	28.	Promote Availability Management awareness and understanding within all IT support organizations, including Third-Party Service Vendors	R, A	I
	29.	Perform regular (e.g., quarterly) reviews of the Availability Management process and its associated techniques and methods to ensure that all are subjected to continuous improvement and remain fit for purpose	R, A	I
	30.	Periodically audit the Availability Management process to ensure that it continues to deliver desired results in compliance with agreed-upon policies, processes and procedures	I	R, A

Table 11 - Roles and Responsibilities - Project Management Services

5.11 Roles and Responsibilities - Capacity Management

Capacity Management Services are the activities associated with ensuring that the capacity of the Service matches the evolving demands of ACSA business in the most cost-effective and timely manner. The process encompasses the following:

- Monitoring of performance and throughput of IT Services and supporting IT components
- Understanding current demands and forecasting for future requirements
- Developing capacity plans which will meet demand and SLRs
- Developing modelling and conducting simulations to manage capacity
- Conducting risk assessment of capacity recommendations
- Developing and implementing a capacity plan including the financial impact of the Service
- Undertaking tuning activities

Sub area	Number	Task/Activity	provider	ACSA
Capacity Management	1.	Define Capacity Management requirements	I	R, A
	2.	Develop, document and maintain in the Standards, Process and Procedures Manual Capacity Management procedures that meet requirements and adhere to defined policies	R, A	I
	3.	Review and approve Capacity Management process and procedures	I	R, A
	4.	Establish a comprehensive Capacity Management planning process	R, A	I
	5.	Review and approve Capacity Management planning process	I	R, A

Sub area	Number	Task/Activity	provider	ACSA
	6.	Define, develop and implement tools that allow for the effective capacity monitoring/trending of Intelligent Integrated Security Platform infrastructure, applications and IT components	R, A	I
	7.	Identify future business requirements that will alter capacity requirements	I	R, A
	8.	Develop a periodic (usually yearly) capacity plan, including quarterly updates	R, A	I
	9.	Develop and implement capacity models and run simulations to validate the capacity plan	R, A	I
	10.	Participate in all capacity planning activities	I	R, A
	11.	Assess capacity impacts when adding, removing or modifying applications and components of the Intelligent Integrated Security Platform infrastructure.	R, A	I
	12.	Continually monitor IT resource usage to enable proactive identification of capacity and performance issues	R, A	I
	13.	Capture trending information and forecast future ACSA capacity requirements based on ACSA-defined thresholds	R, A	I
	14.	Assess incidents/problems related to capacity and provide recommendations for resolution	R, A	I
	15.	Recommend changes to capacity to improve service performance	R, A	I
	16.	Assess impact/risk and cost of capacity changes	R, A	I
	17.	Approve capacity-related recommendations	I	R, A
	18.	Maintain capacity levels to optimize use of existing IT resources and minimize ACSA costs to deliver Services at agreed-to SLRs	R, A	I
	19.	Ensure adequate capacity exists within the IT environment to meet SLRs and requirements, considering daily, weekly and seasonal variations in capacity demands	R, A	I
	20.	Validate asset utilization and capital efficiency	I	R, A

Table 12 - Roles and Responsibilities - Capacity Management

5.12 Roles and Responsibilities - Performance Management

Performance Management Services are the activities associated with managing and tuning Service components for optimal performance. The process encompasses the following:

- Monitoring of performance and throughput of IT Services and supporting IT components
- Assessing the results of the reports
- Conducting trending analysis
- Providing recommendations to tune
- Performing tuning activities
- Updating on a periodic basis (at least annually)

Sub area	Number	Task/Activity	provider	ACSA
Performance Management	1.	Define Performance Management requirements	I	R, A
	2.	Develop, document and maintain in the Standards, Process and Procedures Manual Performance Management procedures that meet requirements and adhere to defined policies	R, A	I
	3.	Review and approve Performance Management procedures	I	R, A
	4.	Perform Service component tuning to maintain optimum performance in accordance with Change Management procedures	R, A	I
	5.	Manage Service component resources (e.g., devices and traffic) to meet defined Availability and performance SLRs	R, A	I

Sub area	Number	Task/Activity	provider	ACSA
	6.	Provide monitoring and reporting of Tower component performance, utilization and efficiency based on specified time frame and sequence (e.g., monthly)	R, A	I
	7.	Proactively evaluate, identify and recommend configurations or changes to configurations that will enhance performance	R, A	I
	8.	Conduct trending analysis to recommend changes to improve the performance based on specified time frame and sequence (e.g., monthly)	R, A	I
	9.	Develop and deliver improvement plans as required to meet SLRs based on specified time frame and sequence (e.g., monthly)	R, A	I
	10.	Review and approve improvement plans		R, A
	11.	Implement improvement plans and coordinate with Third Parties as required	R, A	I
	12.	Provide technical advice and support to the application maintenance and development staffs as required	R, A	I

Table 13 - Roles and Responsibilities - Performance Management

5.13 Roles and Responsibilities - Configuration Management

Configuration Management Services are the activities associated with providing a logical model of the devices or assets (including software licenses) and their relationships by identifying, controlling, maintaining, and verifying installed hardware, software and documentation (i.e., maintenance contracts, SLA documents, etc.).

The goals are to account for all IT assets and configurations, provide accurate information on configurations, provide a sound basis for Incident, Problem, Change and Release Management, and to verify configuration records against the Intelligent Integrated Security Platform infrastructure and correct any exceptions. The following table identifies the Configuration Management roles and responsibilities that provider and ACSA will perform

Sub area	Number	Task/Activity	provider	ACSA
Configuration Management	1.	Define Configuration Management requirements	I	R, A
	2.	Develop, document and maintain in the Standards Process and Procedures Manual Configuration Management procedures that meet requirements and adhere to defined policies	R, A	I
	3.	Review and approve Configuration Management procedures and processes	I	R, A
	4.	Identify and document the configuration item structure	R, A	I
	5.	Approve the configuration item structure	I	R, A
	6.	Establish Configuration Management database, in accordance with ACSA requirements	R, A	I
	7.	Review and approve Configuration Management database	I	R, A
	8.	Select and provide Configuration Management tools	I	R, A
	9.	Install and maintain Configuration Management tools	R, A	I
	10.	Enter/upload configuration data into configuration database	R, A	I
	11.	Establish process interfaces to Incident and Problem Management, Change Management, technical support, maintenance and Asset Management processes	R, A	I
	12.	Establish appropriate authorization controls for modifying configuration items and verify compliance with software licensing	R, A	I
	13.	Establish guidelines for physical and logical separation between development, test and production and the process for deploying and back-out of configuration items	I	R, A

Sub area	Number	Task/Activity	provider	ACSA
	14.	Develop procedures for establishing configuration baselines as reference points for rebuilds, and provide ability to revert to stable configuration states	R, A	I
	15.	Develop procedures for establishing security baselines as reference points for rebuilds, and provide ability to revert to stable configuration states	I	R, A
	16.	Establish procedures for verifying the accuracy of configuration items, adherence to Configuration Management process and identifying process deficiencies	R, A	I
	17.	Provide a deficiency report and steps taken to address the issues identified	R, A	I
	18.	Provide ACSA Configuration Management reports as required and defined by ACSA	R, A	I
	19.	Audit Configuration Management process and accuracy of configuration data	I	R, A

Table 14 - Roles and Responsibilities - Configuration Management

5.14 Roles and Responsibilities - Asset Management

Asset Management Services are the activities associated with process of the ongoing management and tracking of the life cycle of existing, Service components (e.g., hardware, software and software licenses, maintenance, circuits) and their attributes (i.e., location, costs, depreciation, contracts, vendor, serial numbers, etc.).

Sub area	Number	Task/Activity	provider	ACSA
Asset Management	1.	Define Asset Management requirements	C, I	R, A
	2.	Recommend improvements to Asset Management requirements and policies	R, A	C, I
	3.	Develop, document and maintain in the Standards and Procedures Manual Asset Management process and procedures that meet requirements and adhere to defined policies	R, A	C, I
	4.	Review and approve Asset Management process and procedures	C, I	R, A
	5.	Deploy an Asset Management system that meets ACSA requirements and adheres to defined policies	C, I	R, A
	6.	Maintain and manage an Asset Management system that meets ACSA requirements and adheres to defined policies	R, A	C, I
	7.	Manage life cycle of all assets from identification, requisition ordering, inventory, installation and maintenance to disposal	R, A	I
	8.	Develop asset type list and attributes that would be included in the Asset Management system	I	R, A
	9.	Review asset type list and attributes and maintain asset types and attributes in the Asset Management system	R, A	I
	10.	provide ACSA inquiry and reporting access into the Asset Management system for all assets	R, A	I
	11.	Maintain the accuracy of the data of in-scope assets in the Asset Management system, according to SLRs	R, A	I
	12.	Provide electronic feed file of asset data for various ACSA-defined systems (e.g., financial system, ACSA internal billing system)	R, A	I

Sub area	Number	Task/Activity	provider	ACSA
	13.	Establish, update and maintain the asset database to include, at a minimum, the following asset attributes: • Manufacturer • Model • Serial number • Identification number • Location • Ownership information (provider/ACSA — lease/purchase) • Cost information • Maintenance information and history, including the age of the asset • Warranty information • Other billing information (e.g., lease information, ACSA-specific information) • Transaction edit history (e.g., locations, billing, and user)	R, A	I
	14.	Update in-scope asset records related to all approved change activities (e.g., install/move/add/change activities, break/fix activities, company reorganization and Change Management)	R, A	I
	15.	Perform ongoing physical asset audit, in accordance with Asset Management SLRs, to validate that data in the database is accurate and current	R, A	I
	16.	Provide reports of Asset Management audit results	R, A	I
	17.	Provide and, upon ACSA approval, implement Asset Management remediation plan for Asset Management deficiencies	R, A	I
	18.	Review and approve audit reports and remediation plans of asset inventory management information	C, I	R, A
	19.	Provide reports of ACSA asset financial information including depreciation, maintenance contracts and value of assets	R, A	I
	20.	Affix Asset Tags supplied by ACSA according to the relevant procedures.	R, A	I
	21.	Conduct periodic/ad hoc quality assurance audit of Asset Management system	I	R, A

Table 15 - Roles and Responsibilities - Asset Management

5.15 Roles and Responsibilities - Software License Management

Software License Management Services are the activities associated with the identification, acquisition and disposal as well as ongoing management and tracking of software and their corresponding licenses

Sub area	Number	Task/Activity	provider	ACSA
Software License Management	1.	Define Software License Management requirements	C, I	R, A
	2.	Recommend improvements to Software License Management requirements and policies	R, A	I
	3.	Develop, document and maintain in the Standards and Procedures Manual Software License Management procedures that meet requirements and adhere to defined policies as mapped to Asset Management	R, A	I
	4.	Review and approve Software License Management processes and procedures	I	R, A
	5.	Manage and maintain (e.g., monitor, track status, verify, audit, perform contract compliance, reassign) software licenses and media through software license life cycle	R, A	C, I
	6.	For ACSA-retained contracts, be responsible for procurement, renewal and upgrade costs, and vendor agreements	I	R, A

Sub area	Number	Task/Activity	provider	ACSA
	7.	For non-ACSA-retained contracts, be responsible for procurement, renewal and upgrade costs, and vendor agreements	R, A	C, I
	8.	Develop and maintain inventory of all Software licenses within the Asset Management system	R, A	I
	9.	Report to ACSA on any exceptions to Vendor terms and conditions including license non-compliance	R, A	I
	10.	Periodically (at least yearly), conduct software license and maintenance agreements review, allowing for sufficient time prior to expiration for negotiations	R, A	I
	11.	Participate in software license and maintenance agreements review	I	R, A
	12.	Provide ACSA with reports and recommendations to use in making software acquisition and discontinuance decisions	R, A	I
	13.	Provide recommendations to purchase additional license allocation, recommending alternatives or curtailing usage where necessary and appropriate, to restore or continue to maintain license compliance	R, A	I
	14.	Identify and report license compliance issues to ACSA and provide recommendations to resolve the compliance issue	R, A	I
	15.	Review license compliance issues and document completed resolution	I	R, A
	16.	Manage and perform audits and reconcile the number of licenses to the number of installs, as requested by ACSA	R, A	I
	17.	Provide recommendations to ACSA to resolve any software reconciliation issues	R, A	I
	18.	Report on resolution to software reconciliation issues	I	R, A
	19.	Obtain approval from ACSA for any license change or replacement	R, A	I

Table 16 - Roles and Responsibilities - Software License Management

5.16 Roles and Responsibilities - Change Management

Change Management Services are activities to ensure that standardized methods and procedures are used for efficient and prompt handling of all changes, in order to minimize the impact of change upon Service quality and consequently to improve the day-to-day operations of ACSA.

Change Management covers all aspects of managing the introduction and implementation of all changes affecting all Towers and in any of the management processes, tools and methodologies designed and utilized to support the Service components.

The Change Management processes and activities are inter-related and complementary with Release Management and Configuration Management, as well as Incident Management and Problem Management.

The Change Management process includes the following process steps:

- Determining metrics for measuring effectiveness of a change
- Request for change (**RFC**) process
- Recording/tracking process
- Prioritization process
- Responsibility assignment process
- Impact/risk assessment process
- Participation in IT service continuity and DR planning
- Coordination of the Change Advisory Board (**CAB**)
- Review/approval process
- Establishing and managing the schedule of approved changes
- Implementation process
- Verification (test) process
- Closure process

Sub area	Number	Task/Activity	provider	ACSA
Change Management	1.	Define Change Management policies and requirements, including change priority schema and classifications, per the Change Management process components outlined above	I	R, A
	2.	Develop Change Management procedures and processes per the Change Management process components outlined above	R, A	I
	3.	Review and approve Change Management process, procedures, and policies	I	R, A
	4.	Receive and document all RFCs and classify proposed changes to the Services, which shall include change cost, risk impact assessment and system(s) security considerations	R, A	I
	5.	Review and validate that RFCs comply with Change Management policies, procedures, and processes	I	R, A
	6.	Ensure that appropriate back-out plans are documented and in place in the event of systems failure as a result of the change	R, A	I
	7.	Provide Change Management plan to ACSA for review	R, A	I
	8.	Approve Change Management plan	I	R, A
	9.	Develop and maintain a schedule of planned approved changes (Forward Schedule of Changes [FSC]) for ACSA to review	R, A	I
	10.	Coordinate, schedule, and conduct CAB meetings to include review of planned changes and results of changes made, ensuring that all appropriate parties are invited and represented in accordance with approved CAB policies	R, A	I
	11.	Participate in CAB meetings as ACSA deems appropriate or necessary	I	R, A
	12.	Provide change documentation as required, including proposed metrics as to how effectiveness of the change will be measured	R, A	I
	13.	Review and approve change documentation and change effectiveness metrics	I	R, A
	14.	Review and approve any RFC determined to have a cost, security, or significant risk impact to ACSA's IT systems or business	I	R, A
	15.	Authorize and approve scheduled changes or alter the schedule change requests as defined in the Change Management procedures	I	R, A
	16.	Publish and communicate the approved FSC to all appropriate IT and business unit stakeholders within ACSA of change timing and impact	I	R, A
	17.	Oversee the approved change build, test and implementation processes to ensure these activities are appropriately resourced and completed according to change schedule	R, A	I
	18.	Ensure that thorough testing is performed prior to release and assess ACSA business risk related to any change that is not fully tested prior to implementation	I	R, A
	19.	Participate in business risk assessment for change to be introduced without being fully tested	R, A	I
	20.	Monitor changes, perform change reviews and report results of changes, impacts and change effectiveness metrics	R, A	I
	21.	Verify that change met objectives based upon predetermined effectiveness metrics, and determine follow-up actions to resolve situations where the change failed to meet objects	R, A	I
	22.	Review and approve Change Management results	I	R, A
	23.	Close out RFCs that met the change objectives or changes that were abandoned	R, A	I
	24.	Perform Change Management quality control reviews and audits of Change Management processes and records	c, I	R, A
	25.	Provide ACSA Change Management reports as required and defined by ACSA	R, A	c, I

Table 17 - Roles and Responsibilities - Change Management

5.17 Roles and Responsibilities - Training and Knowledge Transfer

Training and Knowledge Transfer Services consist of the following three types of training provider will provide:

- Training for the improvement of skills through education and instruction for provider's staff. provider will participate in any initial and ongoing training delivered by ACSA as required that would provide a learning opportunity about ACSA's business and technical environment.

- Training for ACSA-retained technical staff for the express purpose of exploiting the functions and features of the ACSA computing environment. Delivery methods may include classroom-style, computer-based, individual or other appropriate means of instruction.

- Selected classroom-style and computer-based training (case-by-case basis) for standard COTS and Software as a Service (SaaS) applications, including new employee training, upgrade classes and specific skills.

Sub area	Number	Task/Activity	Provider	ACSA
Training and Knowledge Transfer	1.	Define Training and Knowledge Transfer requirements	I	R, A
	2.	Develop, document, and maintain in the Standards and Procedures Manual Training and Knowledge Transfer procedures that meet requirements and adhere to defined policies	R, A	C, I
	3.	Review and approve Training and Knowledge Transfer procedures	I	R, A
	4.	Develop and deliver training program to instruct ACSA personnel on the provision of provider Services (e.g., "rules of engagement," requesting Services)	R, A	C, I
	5.	review and approve provider-developed training program	I	R, A
	6.	Develop, implement, and maintain an ACSA-accessible knowledge database/portal	R, A	C, I
	7.	Develop and implement Knowledge Transfer procedures to ensure that more than one individual understands key components of the business and technical environment	R, A	C, I
	8.	anticipate in ACSA-delivered instruction on the business and technical environment	R, A	C, I
	9.	Develop, document, and deliver training requirements that support the ongoing provision of ACSA Services, including refresher courses as needed and instruction on new functionality	R, A	C, I
	10.	Take training classes as needed to remain current with systems, software, features, and functions for which help desk support is provided, in order to improve Service performance (e.g., First-Contact Resolution)	R, A	C, I
	11.	Provide training when substantive (as defined between ACSA and provider) technological changes (e.g., new systems or functionality) are introduced into ACSA environment, in order to facilitate full exploitation of all relevant functional features	R, A	C, I
	12.	Provide training materials for ACSA technical staff for Level 1-supported applications	R, A	C, I
	13.	Provide ongoing training materials for help desk personnel on ACSA business and technical environments, as defined by ACSA	R, A	C, I
	14.	Provide ACSA-selected classroom-style and computer-based training (case-by-case basis) for standard COTS applications, as requested by ACSA	R, A	C, I

Table 18 - Roles and Responsibilities - Training and Knowledge Transfer

5.18 Roles and Responsibilities - Account Management

Account Management Services are the activities associated with the ongoing management of the Service environment.

Sub area	Number	Task/Activity	Provider	ACSA
Management	1.	Define Account Management requirements	I	R, A
	2.	Develop, document, and maintain in the Standards Process and Procedures Manual Account Management procedures that meet requirements and adhere to defined policies	R, A	I
	3.	Review and approve Account Management process and procedures	I	R, A
	4.	Develop a detailed "IT" catalogue that details Services offered, including all Service options, pricing, installation time frames, order process (new, change and remove service) and prerequisites	R, A	I
	5.	Approve Service catalogue	I	R, A
	6.	Develop a Service ordering process that clearly defines how to order, change, or delete Services	R, A	C, I
	7.	Recommend criteria and formats for administrative, Service activity and Service-Level Reporting	R, A	C, I
	8.	Review and approve criteria and formats for administrative, Service activity and Service-Level Reporting	I	R, A
	9.	Develop and implement customer satisfaction program for tracking the Quality of Service (QoS) delivery to End Users	R, A	I
	10.	Review and approve customer satisfaction program for tracking the QoS delivery to End Users	I	R, A
	11.	Provide reporting (e.g., statistics, trends, audits, customer satisfaction results)	R, A	I
	12.	provider to ensure the appropriate resource model is assigned to the account, including relationship manager, project managers, delivery manager, technical managers, etc. The relationship manager will be the single point of contact between the provider and ACSA-IT	R, A	I
Meetings	13.	Actively participate in meetings as defined in the report and meeting schedule.	R, A	I
	14.	Ensure any planning is done prior to the meetings	R, A	I
	15.	Ensure reports and any required documents are circulated prior to the meeting	R, A	I
	16.	Ensure all actions documented from the meetings are addressed	R, A	I
	17.	Produce minutes of the meetings	R, A	I
Risk Management	18.	Participate in regular reviews of the risk exposure of the relationship and overall transaction between ACSA and Service provider.	R, A	I
	19.	Inform ACSA of any immediate risks requiring urgent attention	R, A	I
	20.	Co-develop risk mitigation strategies	R, A	I

Table 19 - Roles and Responsibilities - Account Management

5.19 Roles and Responsibilities - Incident Resolution and Problem Management

The activities associated with restoring normal service operation as quickly as possible and to minimize the adverse impact on ACSA business operations, thus ensuring that the best possible levels of service quality and availability are maintained.

Problem Management also includes minimizing the adverse impact of Incidents and Problems on the business that are caused by errors in the in-scope Intelligent Integrated Security Platform, and to prevent the recurrence of Incidents related to those errors. In order to achieve this goal, Problem Management seeks to get to the root cause of incidents and then initiate actions to improve or correct the situation.

Sub area	Number	Task/Activity	provider	ACSA
Incident Resolution and Problem Management	1.	Adhere to ACSA Problem Management process and procedures	R, A	I
	2.	Provide ACSA Problem Management process and procedures	I	R, A
	3.	If the provider requires calls to be logged to their service desk, an integration between ACSA and provider service desk must be provided by Service provider. All accountability and associated costs are for the Service provider. No manual call logging to provider's Service Desk will be in scope for ACSA. Any failure in communication between ACSA and the provider's service desk does not constitute grounds to miss SLA as the ACSA service desk is the tool to measure SLA	R, A	I
	4.	Accept, update and close calls as per service level agreements using the ACSA_IT call logging system.	R, A	I
	5.	Provide, configure, and operate Incident and Problem Management system that tracks Incidents	I	R, A
	6.	Perform incident and problem management per ACSA process and procedures, which includes, but is not limited to: • Perform event management monitoring of the Services to detect abnormal conditions or alarms, log abnormal conditions, analyse the condition, and take corrective action • Manage entire Incident/Problem life cycle including detection, diagnosis, status reporting, repair, and recovery • Coordinate and take ownership of problem resolution by managing an efficient workflow of incidents including the involvement of Third-Party providers (e.g., vendors). • Assign problems to L2 & L3 technical maintenance and repair staff as required • Review the state of open Problems and the progress being made in addressing these problems. • Interact on a regular basis with the IT service desk to ensure optimised efficient level of service delivery [scheduled meetings, reports, etc.]. • Updates must be provided to the service desk in a professional, timely manner in both verbal and in written formats [using the call logging application] • Manage and coordinate subcontractors and third parties in order to meet resolve Incidents/Problems • Upon rectification of the Incident/Problem, the provider will immediately notify ACSA helpdesk that the Incident/Problem has been Resolved • Update all change configuration data bases prior to closing any call.	R, A	I, C

Sub area	Number	Task/Activity	provider	ACSA
	7.	ASCA IT Engineer to review Incident and Problem management tasks by the provider in Monthly Care Review Meetings to ensure the provider is completing tasks in accordance with ACSA process and procedures	I	R, A
	8.	Provide status report detailing the Incident and Problem Management logs as defined in reporting schedule	R, A	I,

Table 20 - Roles and Responsibilities - Incident Resolution and Problem Management

5.20 Roles and Responsibilities - IT Service Continuity and Disaster Recovery

IT Service Continuity and Disaster Recovery (DR) Services are the activities associated with providing such Services for the Intelligent Integrated Security Platform, and the associated infrastructure (e.g., CPU, servers, data and output devices End-User devices) and associated infrastructure and Services will receive DR Services according to ACSA's Business Continuity Plan. provider must demonstrate that it will consistently meet or exceed ACSA's IT Service Continuity and DR Services requirements.

Sub area	Number	Task/Activity	provider	ACSA
IT Service Continuity and Disaster Recovery	1.	As needed, assist ACSA in other IT continuity and emergency management activities	R, A	I
	2.	Develop and maintain a detailed DR plan to meet IT Service Continuity and DR requirements. Include plans for data, replication, backups, storage management and contingency operations that provide for recovering ACSA's systems within established recovery requirement time frames after a disaster affects ACSA's use of the Services.	R, A	I
	3.	Participate in DR tests	R, A	I, C, S
	4.	Track and report DR test results to ACSA	R, A	I
	5.	Review and approve DR testing results	I	R, A

Table 21 - Roles and Responsibilities - IT Service Continuity and Disaster Recovery

5.21 Roles and Responsibilities - Service-Level Monitoring and Reporting

Service-Level Monitoring and Reporting Services are the activities associated with the monitoring and reporting Service Levels with respect to Service-Level Requirements (SLRs). In addition, provider shall report system management information (e.g., performance metrics and system accounting information) to the designated ACSA representatives in a format agreed to by ACSA.

Sub area	Number	Task/Activity	provider	ACSA
Service-Level Monitoring and Reporting	1.	Define Service-Level requirements	I	R, A
	2.	Define Service-Level Monitoring and Reporting requirements	I	R, A
	3.	Develop, document and maintain in the Standards Process and Procedures Manual Service-Level Monitoring and Reporting procedures that meet requirements and adhere to defined policies	R, A	I
	4.	Review and approve Service-Level Monitoring and Reporting procedures	C	R, A
	5.	Report on SLR performance and improvement results	R, A	I
	6.	Coordinate SLR monitoring and reporting with designated ACSA representative and Third Parties	R, A	I
	7.	Measure, analyse and provide management reports on performance relative to SLRs	R, A	I
	8.	Conduct SLR Improvement Meetings to review SLRs and recommendations for improvements	R, A	I
	9.	Review and approve SLR improvement plans	I	R, A
	10.	Implement SLR improvement plans	R, A	I

Sub area	Number	Task/Activity	provider	ACSA
	11.	Review and approve SLR metrics and performance reports	C, I	R, A
	12.	Provide ACSA access to performance and SLR reporting and monitoring system and data	R, A	I

Table 22 - Roles and Responsibilities - Service-Level Monitoring and Reporting

5.22 Roles and Responsibilities - Financial Management

Manage the financial aspects of the contract. This involves reconciling of billing and internal charge back. This also includes Processes for maintaining financial management of the contract through unnecessary cost elimination

Sub area	Number	Task/Activity	provider	ACSA
Financial Management	1.	Adhere to ACSA Standards and Procedures Manual Financial/Chargeback Management and Invoicing procedures.	R, A	I
	2.	Implement corrective actions for billing disparities	R, A	I
	3.	Provide data to conduct Penalties per ACSA requirements	R, A	I
	4.	Provide timely and correct invoices to ACSA and/or respective ACSA Operating Divisions	R, A	I
	5.	Provide ACSA Standards and Procedures Manual Financial/Chargeback Management and Invoicing procedures.	I	R, A
	6.	Provide such information as it may reasonably request for it to perform Penalty processes	I	R, A
	7.	Identify billing disparities and work with the provider to identify corrective actions	I	R, A
	8.	provide information to be used for budgeting in line with operating plan	R, A	I
	9.	Assist in monitoring and manage charging/invoicing	R, A	I
	10.	Set budgets in line with operating plan		R, A
	11.	Monitor and manage payment against budgets		R, A
	12.	Maintain an audit trail and records of all costs incurred under the Agreement	R, A	I
	13.	Proactively ensure that all unnecessary costs are eliminated, and that costs are managed in an efficient manner	R, A	I
	14.	Participate in financial review meetings	R, A	I
	15.	Identify areas for potential cost savings and provide input for innovation process where appropriate	R, A	I
	16.	Implement ACSA's invoicing and recharge requirements	R, A	I
	17.	Review and approve records of all costs incurred by the provider under the Agreement	I	R, A
	18.	Proactively ensure that all unnecessary costs are eliminated, and that costs are managed in an efficient manner	I	R, A
	19.	Participate in financial review meetings	I	R, A
	20.	Identify areas for potential cost savings and provide input for innovation process where appropriate	I	R, A
	21.	Implement ACSA's invoicing and recharge requirements	I	R, A

Table 23 - Roles and Responsibilities - Financial Management

5.23 Roles and Responsibilities - Human Resources

Human Resource Management Services include the activities associated with the provision and adjustment of appropriate human resources, per workloads, to perform the required Services at the required Service Levels

Sub area	Number	Task/Activity	provider	ACSA
Skills and Staffing	1.	Ensure that staffing and skill levels are adequate to achieve SLA	R, A	I
	2.	Train and up skill staff as required	R, A	I
	3.	Provide ACSA with staff training plans (especially onsite staff)	R, A	I
	4.	Monitor the staff development	I	R, A
Capacity Management	5.	Proactively keep the provider informed of any requirements that would potentially impact on the Service provider's HR resource requirements	I	R, A
	6.	Define any constraints for the use of Subcontractors	I	R, A
	7.	Approve or reject recommended Subcontractors	I	R, A
	8.	Analyse the impact of any new requests made by ACSA to be implemented by the provider and propose HR resources (skills and staffing) solution	R, A	I
	9.	Analyse the impact of enhanced SLAs (if required by ACSA) on the allocated human resources and propose solution	R, A	I
	10.	Recruit and provide the human resources necessary for the performance of required Services in compliance with SLAs	R, A	I
	11.	Manage Employees time off and replacement	R, A	I
	12.	Recommend Subcontractors for delivery of Services, if applicable	R, A	I
Performance Monitoring	13.	Continuously monitor the performance of all the human resources made available to ACSA to ensure that the Services comply with the SLAs	R, A	I
	14.	Perform Annual Employee performance reviews	R, A	I
	15.	Consider ACSA satisfaction a key component of the assigned Employee performance reviews	R, A	I
Change Management	16.	On request by ACSA designate certain members of staff as Key Employees	R, A	I
	17.	Inform ACSA with a minimum of two weeks' notice of any potential Key Employee staffing changes and of any new Employee assignments planned for new projects and Services	R, A	I
	18.	Assign a new provider Relationship Manager as necessary to discharge the Service provider's responsibilities	R, A	I
	19.	Provide staff turnover data relevant to the Agreement when requested by ACSA	R, A	I
	20.	ACSA to nominate key employees where required	I	R, A
	21.	Request provider staff turnover data when required	I	R, A
	22.	Communicate changes to internal ACSA Stakeholders	I	R, A

Table 24 - Roles and Responsibilities - Human Resources

5.24 Roles and Responsibilities - Security

Security Services are the activities associated with maintaining physical and logical security of all Service components (hardware and software) and data, virus protection, access protection and other Security Services in compliance with ACSA's Security requirements.

Physical Security focuses on the physical access controls implemented to ensure the security of ACSA's and provider's data processing equipment, facilities, and its associated management systems

Data Security consists of the activities associated with the classification, management, security and encryption of sensitive/confidential data, and the storage of media containing that data.

Identity and Access Management Services consist of the activities to authorize, authenticate, and provide access control to the Intelligent Integrated Security Platform.

Sub area	Number	Task/Activity	provider	ACSA
General	1.	Install Security patches per ACSA's Change Management process and procedures, including acquiring required ACSA approval	R, A	I
Physical Security	2.	Provide physical security in conformance with policies, procedures and practices	R, A	I
	3.	Physically secure data processing equipment, facilities, and storage media from unauthorized access	R, A	I
	4.	Physically protect and store fixed and portable media (e.g., tape, optical, portable hard drives, flash drives) containing sensitive data	R, A	I
	5.	Ensure only authorized personnel have access to data processing equipment, facilities and storage media	R, A	I
	6.	Track and monitor all physical access and activities performed on data processing equipment and facilities	R, A	I
	7.	Review logs to show the access to data processing equipment was business-justified	R, A	I
	8.	Provide capability to immediately revoke access to data processing equipment, facilities and storage media	R, A	I
	9.	Maintain physical access audit logs	R, A	I
	10.	Physically secure management systems from unauthorized access	R, A	I
	11.	Ensure only authorized personnel have access to management systems	R, A	I
	12.	Track and monitor all changes performed on management systems	R, A	I
	13.	Provide capability to immediately revoke access from management systems	R, A	I
	14.	Maintain change audit logs on management systems	R, A	I
Data Security	15.	Assume custodial responsibility for all storage media Related to services provided	R, A	I
	16.	Protect portable media while in transit and maintain transmittal records	R, A	I
	17.	Eradicate all data from storage media (server memory, disk, tape, optical, other) before redeployment or disposal, in accordance with ACSA's procedures	R, A	I
	18.	Perform periodic (e.g., monthly) reconciliation reporting of all data media and perform annual audit to reconcile all storage media	R, A	I
	19.	Report reconciliation discrepancies to ACSA and take corrective action to address issue	R, A	I
Identity and	20.	Provide Identity and Access Management in conformance with ACSA practices, policies and procedures	R, A	I

Sub area	Number	Task/Activity	provider	ACSA
	21.	Establish roles, authorized activities and minimum rights granted to Service provider personnel (including non-user accounts)	R, A	I
	22.	Establish roles, authorized activities and minimum rights granted to ACSA personnel (including non-user accounts)	I	R, A
	23.	Approve roles and authorization activities performed by provider	I	R, A
	24.	Establish and manage the process for defining, granting, modifying, and revoking user accounts and enforcing role restrictions	R, A	I
	25.	Establish and manage process to support temporary access	R, A	I
	26.	Review and approve user and system user account management process	I	R, A
	27.	Approve Service provider personnel who are authorized to manage user accounts.	I	R, A
	28.	Provide IT Identity and Access Management technology solution that integrates with ACSA systems	I	R, A
	29.	Support and maintain IT Identity and Access Management technology solution for the Intelligent Integrated Security Platform	R, A	I
	30.	Perform engineering, configuration and ongoing management of IT Identity and Access Management technology solution	R, A	I
	31.	Provide and implement a solution to interface ACSA and Service provider's Identity and Access Management processes	R, A	I
	32.	Approve solution to interface ACSA and Service provider's Identity and Access Management processes	I	R, A
	33.	Define logging and archiving policies and requirements	I	R, A
	34.	Provide logging and archiving specifications/design	R, A	I
	35.	Approve logging and archiving specification/design	I	R, A
	36.	Log and archive user/account activity according to approved logging and archiving specification/design	R, A	I
	37.	Monthly audit production system access logs and activities to identify malicious or abnormal behaviour in accordance with established ACSA policies and standards	R, A	I
	38.	Conduct monthly review of all privileged user accounts to ensure the accounts are valid/required, removing inactive and unneeded accounts in accordance with established ACSA policies and standards	R, A	I
	39.	Conduct monthly review of End-User accounts to ensure each user has appropriate minimal permissions required to perform their job function in accordance with established ACSA policies and standards	R, A	I
	40.	Conduct monthly review of privileged user accounts to ensure each user has appropriate minimal permissions required to perform their job function in accordance with established ACSA policies and standards	R, A	I
Configuration Security Management	41.	Certify engineering and Configuration Management are secure	R, A	I
	42.	Review and approve engineering designs and Configuration Management security	I	R, A
	43.	Certify equipment meets ACSA's security requirements and provide evidence of compliance	R, A	I
	44.	Periodically review equipment configurations and address any deficiencies or inconsistencies, and provide ACSA with results with detailed recommendations to remediating issues that are found	R, A	I
	45.	Review and approve remediation approach	I	R, A
	46.	Provide ACSA with secure baselines for standard components (e.g., routers, servers, DBMS, etc.)	R, A	I

Sub area	Number	Task/Activity	provider	ACSA
	47.	Establish a baseline for the secure configuration of Equipment based on ACSA's technical control specifications (e.g., CIS benchmark)	I	R, A
	48.	Recommend changes to baseline to meet ACSA requirements	I	R, A
	49.	Configure equipment to approved security requirements	R, A	I
	50.	provider collaborates with ACSA on plan to implement security patches	R, A	I
	51.	Install security patches per the Change, Configuration and Release Management processes and procedures	R, A	I
	52.	Establish logging and archiving specifications	R, A	I
	53.	Identify logging and archiving specifications in order to support business requirements	I	R, A
	54.	Approve logging and archiving specifications.	I	R, A
	55.	Log and archive user and system activity.	R, A	I
	56.	Provide ACSA with reports on any server logs/intrusion detection activities, anomalies or deficiencies that could result in a compromise of the ecommerce system's data confidentially, integrity or system performance	R, A	I
	57.	Provide ongoing support (patches, upgrades, signatures), tuning and management	R, A	I

Table 25 - Roles and Responsibilities - Security

6.0 SERVICE MANAGEMENT

6.1 Objectives

A key objective of this Managed Service agreement is to attain Service Level Requirements (SLR's).

SLRs applicable are identified in this Service Management SOW below.

Specific Service Management SLRs are specified with Fee Reductions, where business is impacted through failure to meet their respective SLRs. SLRs are detailed in the Service-Level Requirements section, and those associated with Fee Reductions are identified in 7.0 SERVICE CREDITS.

provider shall provide written reports to Airport Systems Management regarding provider's compliance with the SLRs specified.

6.2 Reports

The provider shall report to ACSA its performance of the Services against each SLA monthly beginning on the Effective Date, along with detailed supporting information. As part of the standard monthly Service Level reports, the provider shall notify ACSA of any (i) Service Level Failures, and (ii) Penalties to which ACSA becomes entitled.

The provider shall provide such reports and supporting information to ACSA no later than 5 (five) Business Days following the end of the applicable Measurement Interval. The raw data and detailed supporting information shall be Confidential Information of ACSA.

6.3 Root cause analysis

The provider shall promptly investigate and correct Service Level Failures in accordance with the procedures for Root Cause Analysis

6.4 Support services

This 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.

The provider will be required to attend to and resolve all incidents in line with ACSA incident management processes.

The response and resolution times depicted below must be adhered to. This will form part of the SLAs that will be agreed to between the provider and ACSA.

Penalties will be incurred by the provider if the agreed SLA times are not met.

A good performance on an SLA cannot compensate a bad performance on another one

The fact that an SLA is not associated with a specific service does not mean that this SLA is not important to ACSA.

6.5 SERVICE-LEVEL REQUIREMENTS (SLRs)

The following Service-Level Requirements (SLRs) represent minimum Service levels required. providers must consistently meet or exceed the following SLRs.

Review of Service Levels and KPIS

On an annual basis after the initial start-up (90 days), ACSA can request a change to any service level by providing notice to the provider that a service level needs to be changed.

This change can take effect only after the provider has had sufficient time (maximum 3 weeks) to review the requested change and determine if any modifications are required to the delivery of the support and maintenance services. Should changes be required by the provider, then ACSA must allow the provider reasonable time to make such changes before the service-level change takes place.

Priority levels

Priority Level 1 — Emergency/Urgent *Critical Business Impact*	The incident has caused a complete and immediate work stoppage affecting a critical function or critical Intelligent Integrated Security Platform component, and a primary business process or a broad group of users (an entire department, floor, branch, line of business or external customer). No workaround available.
Priority Level 2 — High *Major Business Impact*	A business process is affected in such a way that business functions are severely degraded, multiple users are impacted, a key customer is affected, or a critical function is operating a significantly reduced capacity or functionality. A workaround may be available but is not easily sustainable.
Priority Level 3 — Medium *Moderate Business Impact*	A business process is affected in such a way that certain functions are unavailable to End Users or a system and/or service is degraded. A workaround may be available.
Priority Level 4 — Low *Minimal Business Impact*	An incident that has little impact on normal business processes and can be handled on a scheduled basis. A workaround is available or there is minimal negative impact on a user's ability to perform their normal daily work.

Table 26 – Priority Levels

Incident management

Time to resolve incidents/problems following responses to different incident priority level classifications.

Each IT Service categorizes incidents/problems according to the incident/problem resolution priorities listed below.

Incident management response and resolution times for International Airports (Office Hours)			
Incident/Problem Resolution	**Service Measure**	**Performance Target**	**SLR Performance %**
Time to Notify ACSA of or to accept/acknowledge a Priority 1	Time to Respond	<10 minutes	99.0%
Time to Notify ACSA of or to accept/acknowledge a Priority 2 Incident	Time to Respond	<20 minutes	99.0%
Time to Notify ACSA of or to accept/acknowledge a Priority 3 or 4 Incident	Time to Respond	<120 minutes	98.0%
Time to Notify ACSA of or to accept/acknowledge a Priority 5 Incident	Time to Respond	<3 hours	98.0%
Priority Level 1	Time to Restore (Not linked to hardware failure)	<2 hours	99.0%
Priority Level 2	Time to Restore (Not linked to hardware failure)	<4 hours	98.0%
Priority Level 3	Time to Restore (Not linked to hardware failure)	<8 hours	98.0%
Priority Level 4	Time to Restore (Not linked to hardware failure)	Next business day or as prioritized by provider	98.0%
Priority Level 5	Time to Restore (Not linked to hardware failure)	To be agreed	98.0%
Priority Level 1	Resolution (permanent fix)	To be agreed	99.0%
Priority Level 2	Resolution (permanent fix)	To be agreed	99.0%
Priority Level 3	Resolution (permanent fix)	To be agreed	98.0%
Priority Level 4	Resolution (permanent fix)	To be agreed	98.0%
Priority Level 5	Resolution (permanent fix)	To be agreed	98.0%
Priority Level1-5 Hardware Failure	Fix/replacement	In line with the hardware support procured by ASCA	99.0%
Root-Cause Analysis	Time to Report	Within 48 hours of incident resolution	98.0%
	Formula	Number of requests completed within Performance Target ÷ Total of all requests occurring during Measurement Interval	
	Measurement Interval	Weekly	
	Reporting Period	Monthly	

Incident management response and resolution times for International Airports (Office Hours)		
	Measurement Tool	Data from ACSA Service management Tool (Service NOW) complimented with other provider tools if applicable
	SLR Element Weighting Factor Allocation	50%

Table 27 - Incident Response and Resolution time (Office Hours)

Incident management response and resolution times for International Airports (After hours Hours) and regional airports.			
Incident/Problem Resolution	**Service Measure**	**Performance Target**	**SLR Performance %**
Time to Notify ACSA of or to accept/acknowledge a Priority 1	Time to Respond	<15 minutes	99.0%
Time to Notify ACSA of or to accept/acknowledge a Priority 2 Incident	Time to Respond	<20 minutes	99.0%
Time to Notify ACSA of or to accept/acknowledge a Priority 3 or 4 Incident	Time to Respond	<160 minutes	98.0%
Time to Notify ACSA of or to accept/acknowledge a Priority 5 Incident	Time to Respond	<3 hours	98.0%
Priority Level 1	Time to Restore (Not linked to hardware failure)	<3 hours	99.0%
Priority Level 2	Time to Restore (Not linked to hardware failure)	<5 hours	98.0%
Priority Level 3	Time to Restore (Not linked to hardware failure)	<10 hours	98.0%
Priority Level 4	Time to Restore (Not linked to hardware failure)	Next business day or as prioritized by provider	98.0%
Priority Level 5	Time to Restore (Not linked to hardware failure)	To be agreed	98.0%
Priority Level 1	Resolution (permanent fix)	To be agreed	99.0%
Priority Level 2	Resolution (permanent fix)	To be agreed	99.0%
Priority Level 3	Resolution (permanent fix)	To be agreed	98.0%
Priority Level 4	Resolution (permanent fix)	To be agreed	98.0%
Priority Level 5	Resolution (permanent fix)	To be agreed	98.0%
Priority Level1-5 Hardware Failure	Fix/replacement	In line with the hardware support procured by ASCA	99.0%
Root-Cause Analysis	Time to Report	Within 48 hours of incident resolution	98.0%
	Formula	Number of requests completed within Performance Target ÷ Total of all requests occurring during Measurement Interval	

Incident management response and resolution times for International Airports (After hours Hours) and regional airports.		
	Measurement Interval	Weekly
	Reporting Period	Monthly
	Measurement Tool	Data from ACSA Service management Tool (Service NOW) complimented with other provider tools if applicable
	SLR Element Weighting Factor Allocation	50%

Table 28 - Incident Response and Resolution time (After Hours) (and Regional airports)

Service Availability

Availability SLR	
Component	**Explanation of Component**
Definition	Based on the availability of specifically identified managed objects. Total availability of the Service is based on the number of managed objects and the number of hours within the reporting time period. Downtime is subtracted from the total availability time to determine Availability The following downtimes are excluded from the adjusted calculation: • Prescheduled outages for MACs of routers and/or preventative maintenance • Time required for third-party vendors to resolve hardware/software problems when the ESP is not directly contracted with the vendor (the customer holds the contract with the vendor) • Downtime caused by customer facility power and/or HVAC outages or malfunctions • Downtime attributed directly to customer personnel (such as relocating or reconfiguring devices without prior coordination, hardware negligence or abuse) • Time where the customer is responsible for providing resolution. • Acts of nature (such as lightning and floods)
Requirement	24 hours per day, 7 days per week (365 days a year)
Measurement Range	Priority 1 Objects = 99,999% Priority 2 Objects = 99,9% Priority 3 Objects = 99% Priority 4 Objects = 98%
Measurement Tool	ACSA supplied Enterprise monitoring tools
Frequency	Monthly
Calculation Formula	Performance is calculated as follows: Dl = Total downtime hours Al = Adjusted downtime hours based on exceptions H = Hours in the month Ol = Total number of managed objects in the Priority El = Expected availability = H x Ol Report Only: **Availability %** = (El — Dl)/El x 100 SLA: **Adjusted Availability** % = (El — Al)/El x 100
SLR Element Weighting Factor Allocation	50%

Table 29 Availability SLR

Resource Availability

NOTE: This SLR's is only applicable to pricing option 1 and 2

Availability SLR	
Component	**Explanation of Component**
Definition	Based on the availability of minimum specified Resources.
Coverage	As per resource table
Measurement Range	98%
Frequency	Monthly
Measurement Tool	provider Automated Time and attendance tool
Calculation Formula	Performance is calculated as follows: Dl = Total "downtime" hours Al = Adjusted downtime hours based on exceptions H = Hours in the month (adjusted according to resource type and availability requirements) Ol = Total number of resources per type El = Expected availability = H x Ol Report Only: **Availability %** = (El — Dl)/El x 100 SLA: **Adjusted Availability** % = (El — Al)/El x 100
SLR Element Weighting Factor Allocation	30%

Table 30 Resource availability SLR

Service requests for Intelligent Integrated Security Platform

Intelligent Integrated Security Platform, Service-Level Requirements			
System Administration Task	**Service Measure**	**Performance Target**	**SLR Performance %**
Create user account for administration software	Elapsed Time	request acknowledgement within 1 Business Day	99.0%
Replacement of peripherals or components, i.e., scanner, display, keyboard, mouse, scale, ups, printer, reader, motor, belt, door\ panel, camera, sensor, speaker and lights	Response Time	As per SLA according to priority	99.0%
OS and software updates\ upgrades and general software maintenance	Elapsed Time	Within 30 days after Software vendor announcement	99.0%
General hardware maintenance	Elapsed Time	Monthly unless requested otherwise	
Capacity/Performance Trend Analysis and Reporting across all platforms	Monthly measurement/analysis and periodic notification on resource utilization and trends for critical system resources	Monthly analysis reports Interim reports on rapidly developing events and trends identification	99.0%
	Formula	Number of requests completed within Performance Target ÷ Total of all requests occurring during Measurement Interval	
	Measurement Interval	Measure Weekly	
	Reporting Period	Report Monthly	
	Measurement Tool	TBD	

Table 31 Service requests SLR

IMACDs

Any physical installation, dismantlement, relocation of hardware, and any hardware or software installation, upgrade, or update in accordance with Change Management policies. IMACDs are usually planned and scheduled in advance.

Should The provider not be able to fulfil the IMACD requirement, in the required timeline The provider must provide ACSA with a proposal stating the committed time to complete the IMACD. ACSA, has based on their sole discretion, the right to accept the proposal or engage an alternative (internal or external) provider to provide the service.

Service Measure:	Performance Target:	SLR Performance %
Receipt of IMACD the installation / decommission / move / change plan According to ACSA standards.	IMACD plan to be received by ACSA within 5 days of request. No IMACD plan or written confirmation that the provider cannot achieve the required timelines will be deemed as a missed SLA	98%
On receipt of approval to proceed with IMACD, the provider is to complete the IMACD on time as per the approved plan	Each IMACD milestones not delivered on time as per the approved IMACD plan will be deemed a missed SLA	98%
	SLR Element Weighting Factor Allocation	50%

Table 32 IMACD SLR

Asset management

NOTE: This SLR's is only applicable to pricing option 1 and 2

Within five days after the first day of each calendar quarter, provider shall select a statistically valid sample, in accordance with the agreed process, to measure provider's compliance with the following SLRs pertaining to the accuracy of individual data elements in the asset tracking database. Accuracy of data shall adhere to the following SLR.

Asset Tracking SLR			
Accuracy of Data in Asset Tracking Database	Accuracy	Accuracy percentage of each of the following data elements as determined by audit:	
		Data Element	**Accuracy Percentage**
		ACSA asset tag number, Serial Number, Model number, PO number, Invoice number	99%
		Location (Airport, terminal, floor, counter, gate)	99%
	Formula	Number of tracked assets where data element is determined to be correct ÷ Total number of tracked assets audited	
	Measurement Interval	quarterly as of Effective Date	
	Measurement Tool	Physical Audit.	
	SLR Element Weighting Factor Allocation	30%	

Table 33 Asset Tracking SLR

Configuration management

Configuration Management Services are the activities associated with providing a logical model of the passenger self-service solution by identifying, controlling, maintaining, and verifying installed hardware, software and utility versions.

Within five (5) days after the first day of each calendar quarter, the provider shall select a statistically valid sample for assessment and SLA review.

Configuration Management SLR	
Service Measure:	**Performance Target:**
Configuration Record Accuracy: Data accuracy – chosen sample of all configurations (hardware and software) tracked by the ACSA NMS tools	98%
Timelines of updates: Time to update configuration records	1 day after change to configuration
Measurement Interval:	Electronic audit, conducted quarterly from date of contract commencement
Measurement Tool:	ACSA NMS Tools
SLR Element Weighting Factor Allocation	20%

Table 34 Configuration Management SLR

Overall service satisfaction

Where The provider receives feedback through client surveys and end user feedback, where satisfaction is measured on scale of 1 to 5, with 1 being lowest and 5 being highest.

End-User Satisfaction SLR			
End-User Satisfaction	**Service Measure**	**Performance Target**	**SLR Performance %**
Scheduled Survey (conducted semi-annually by ACSA or its designated Third-Party agent)	End-User Satisfaction rate	clients surveyed should be very satisfied or satisfied	90%
	Formula	1. Sum of survey result from each participant ÷ Total number of participants responding to scheduled survey	
	Measurement Interval	Quarterly	
	Reporting Period	Quarterly	
	Measurement Method/Source Data	ACSA Service management Tool, or results from special survey	
	SLR Element Weighting Factor Allocation	20%	

Table 35 Overall satisfaction SLR

Software/Firmware Refresh

Software refresh for all upgrades and new releases.

Software /firmware Refresh Service-Level Requirements			
Software Refresh	**Service Measure**	**Performance Target**	**SLR Performance %**
Notification of vendor Software upgrades and new releases	Response Time	Within 30 days after Software vendor announcement	95.0%
Implementation of service packs and updates to "dot" releases	Response Time	Within 60 days after approved by Client	95.0%
Implementation of version or major release updates	Response Time	Within 120 days after approved by Client	95.0%
	Formula	Number of requests completed on time ÷ Total of all requests occurring during Measurement period	
	Measure Interval	Measure Monthly	
	Reporting Period	Report Monthly	
	Measurement Tool	TBD	

Table 36 Software/Firmware Refresh SLR

Service level agreement measurement exclusions

The following table provides a list of events that should they occur will not impact on the measurement of the Service Level Agreements.

Number	Service Level Measurement Exclusions
1.	The connection of ancillary equipment, not supplied by the Service provider, or not approved by the manufacturer of the equipment and software;
2.	The negligent use, abuse or misuse of equipment and software by ACSA;
3.	Damage during any transportation of equipment and software by ACSA;
4.	Electrical work, not performed by the Service provider;
5.	Causes external to the equipment such as failure or proven fluctuation of electrical power;
6.	Any authorised / unauthorised changes not communicated to the Service provider
7.	Failure of equipment or services not directly under the control of, or within the responsibility of the Service provider.

Table 37 SLA Measurement Exclusions

7.0 SERVICE CREDITS

The Service Credit Methodology aims to be an appropriate and adequate remedy for non-performance by the Service provider. The philosophy of the Service Credit Methodology is such that it should drive positive behaviour by encouraging compliance with the Service Level Requirements (SLRs) and be consistent with the outcomes required by ACSA. The Service Credit Methodology has been designed recognizing this philosophy and incorporates:

- the need to match Service Credit payments to the severity of the failure/defect.
- the need to provide appropriate incentives based on regimes to cure any defect or failure as quickly as possible.
- the need to avoid an inappropriate impact on Service provider funding.
- the need to be easily understood and unambiguous.
- the need to be administratively manageable; and
- the need to avoid consistent non-performance.

7.1 Principles

The principles for the calculation of the credits are described below:

Service Credits only occur as a result of Service Level Failures.

The Service Levels are calculated for each SLR according to the measurement interval specified in each SLR table (monthly by default),

The Service Credits are calculated according to the formula associated with the SLR as specified in each SLR table.

The Service Credits are totalled for each SLR and valued using the contractual value of a Service Credit.

A good performance on a SLR cannot compensate a bad performance on another one

The SLRs that are considered as critical by ACSA will always be associated with Service Credits assigned. The other set of SLRs can be subject to Service Credits mechanisms, if they are included in a quality improvement plan, or if the Service Levels attained are periodically below requirements.

The fact that an SLR is not associated with a Service Credit does not mean that this SLR is not important to ACSA.

ACSA reserves the right to associate Services Credit mechanism to SLRs where the Service provider would have been in failure over several consecutive months.

ACSA reserves the right to not apply some or any Service Credits that may occur at its sole discretion.

The provider will be allowed a grace period of three ninety (90) Days (to familiarise itself with the operations at all airports) before the implementation of service credits will commence. SLA's will be measured and reported on during the grace period, however, no credits will apply

7.2 Definitions

Total Per Site Monthly Fee - means the monthly service fixed fee per ACSA Site payable by ACSA to the Service provider for the Services.

At Risk Amount - means, for any month during the Term, fifty percent (30%) of the monthly fixed Service Fees per ACSA Site.

Weighting Factor - means, for a particular Service Level Requirement (SLR), the portion of the At-Risk Amount used to calculate the Service Credit payable to ACSA in the event of a Service Level Failure with respect to that SLR.

Monthly Service Credit Pool - means two hundred percent (200%).

Service Level Failure(s) - means whenever the Service provider actual level of performance for a particular Service Level metric (as calculated by that metrics service level calculation) is worse than the Target Performance adjusted by the Minimum Performance Percentage (%) for that Service Level.

Service Credit - means a calculated value based on the percentages in Weighting of Monthly Service Credit Pool in Section 3 of this document.

Service Level Requirement Categories – SLRs are allocated against the following categories:

Primary Category: Has a direct impact on ACSA business. Service Credits will be applied.

Secondary Category: Has some direct impact on ACSA business, no service credits are applicable to these SLRs which have a Weighting Factor of zero percent (0%).

7.3 Methodology

Monitoring; reports; root cause analysis.

Monitoring

The Service provider shall implement measurement and monitoring tools and produce the metrics and reports necessary to measure its performance against the Service Levels. Upon request in connection with an audit, and at no additional charge to ACSA, Service provider shall provide ACSA or its designees with information and access to the tools and procedures used to produce such metrics.

Reports

The Service provider shall report to ACSA its performance of the Services against each SLR on a monthly basis beginning on the Effective Date, along with detailed supporting information. As part of the standard monthly Service Level reports, the Service provider shall notify ACSA of any (i) Service Level Failures, and (ii) Service Credits to which ACSA becomes entitled. The Service provider shall provide such reports and supporting information to ACSA no later than 5 (five) Business Days following the end of the applicable Measurement Interval. The raw data and detailed supporting information shall be Confidential Information of ACSA.

Root cause analysis

The Service provider shall promptly investigate and correct Service Level Failures in accordance with the procedures for Root Cause Analysis set forth in the Agreement.

Calculating service credits

For each Primary Service Level Failure, the Service provider shall pay or credit to ACSA a Service Credit that will be computed by multiplying (a) the Weighting Factor Allocation for such Service Level by (b) the At-Risk Amount. For example, assume for purposes of illustration only, that the Service provider fails to meet a Service Level with a Weighting Factor of 10% (ten percent) and that the monthly Fees equal

R100,000 (one hundred thousand rand) and the At-Risk Amount is 20% (twenty percent). The Service Credit due to ACSA for such Service Level Failure would be: 10% * (20% * R100,000.00) = R2,000.

Special service credit calculation

If the Service provider commits, in a given month, Service Level Failures with respect to three (3) or more Secondary Category Service Levels whose then-current Weighting Factor equals 0% (zero percent) then the Service provider shall pay or credit to ACSA a Service Credit that will be computed according to the formula set forth in Section 0 above, but using the product of (i) 2% (two percent) multiplied by (ii) the number of such Service Levels for which a Service Level Failure occurred in the given month, as the Weighting Factor for purposes of such calculation.

For avoidance of doubt, the table below provides an example calculation to determine the Service Credit payable for failed Secondary Service Levels.

Assume:		**At Risk Amount**	**Secondary SLRs**
Tower	**Monthly Charges**	**10% x Monthly**	**missed in Month**
1	200 000.00	20 000.00	2
2	100 000.00	10 000.00	5
3	50 000.00	5 000.00	6
Total Missed Secondary SLRs			**13**
Then:			
Derived Weighting Factors			
Tower 1	2% x 2	**4%**	
Tower 2	2% x 3	**6%**	
Tower 3	2% x 4	**8%**	
Therefore:			
Tower 1 Service Credit		-	i.e. <4 SLR's failed
Tower 2 Service Credit		600.00	i.e. 10,000 x 6%
Tower 3 Service Credit		400.00	i.e. 5,000 x 8%
Service Credit		**1 000.00**	

Service breach

If a Service Level Failure with respect to a Primary Service Level recurs in more than four consecutive Measurement Intervals, then such Service Level Failure shall constitute a material breach entitling ACSA to the rights set out in clause 51.2.1 of the Agreement.

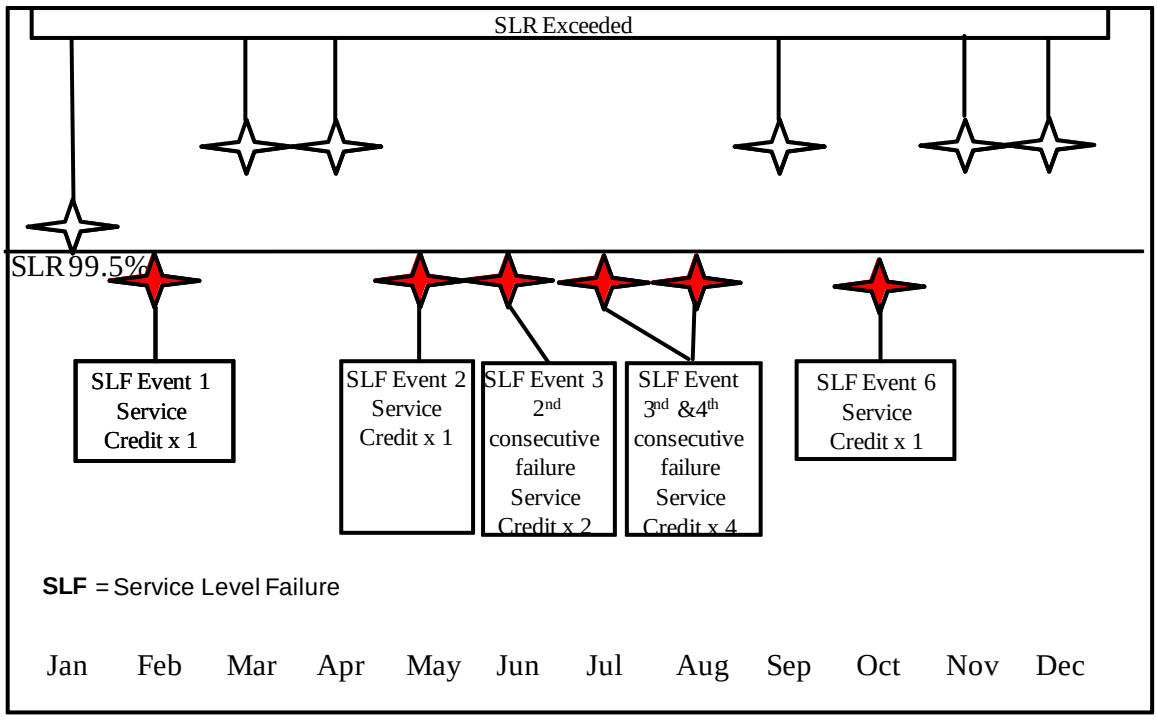
Several service level failures

Subject to Section 0, if more than one Service Level Failure with respect to Service Levels has occurred in a single month, the sum of the corresponding Service Credits shall be credited or paid to ACSA.

Successive service level failures

If a Service Level Failure with respect to a given Service Level recurs in consecutive Measurement Intervals, the amount of the applicable Service Credit payable to ACSA shall be multiplied by the following factors for subsequent Measurement Intervals: (i) Service Level Failure in two consecutive Measurement Intervals, then twice the amount of the Performance Credit as originally calculated; and (ii) Service Level Failure in three or more consecutive Measurement Intervals, then four times the amount of the Service Credit as originally calculated. The Service Credit for any given Service Level shall only be increased as described above, and such increase shall be payable for all consecutive Service Level Failures with respect to such Service Level.

Figure 1. Service Credit for Successive Failures Example



Service credits cap

In no event shall the aggregate amount of Service Credits credited or paid to ACSA with respect to all Service Level Failures occurring in a single month exceed the At-Risk Amount.

Payment/credit of service credits

The Service provider shall itemise the total amount of Service Credits it is obliged to credit to ACSA with respect to Service Level Failures occurring in a given month on the invoice that contains charges for such month. The Service provider shall credit the total amount of such Service Credits related to a given month in the subsequent monthly invoice after ACSA signoff of the Service Credits for the applicable Measurement Interval. Upon termination or expiration of the Term, the Service provider shall pay to ACSA the amount of any Service Credits not so paid or credited to ACSA's account or any unused portion of such Service Credits.

Non-exclusive remedy

The Service provider acknowledges and agrees that the Service Credits shall not be deemed or construed to be liquidated damages or a sole and exclusive remedy or in lieu of any other rights and remedies ACSA has under the Agreement, at law or in equity.

Earn-Back

Following any service-level failure, ACSA may allow the provider the opportunity to earn back the service credits charged in one or more measurement period.

If all the service levels for the relevant service and any others agreed to be associated with that service are exceeded, during each of the **three** measurement periods following the service-level failure, ACSA may, at its sole discretion, return half of the service credits paid to the provider.

If all the service levels for the relevant service and any others agreed to be associated with that service are exceeded, during each of the **six** measurement periods following the service-level failure, ACSA may, at its sole discretion, return the remaining half of the service credits paid to the provider.

The provider may, where the requisite levels of performance are exceeded, make representations to the Company in this regard.

7.4 Changes to performance measurements

Changes to weighting factors

ACSA may request changes to the Weighting Factors for any Service Level by sending written notice to the Service provider. These requested changes will be negotiated through the appropriate Relationship Management structures to gain mutual agreement on such changes prior to them taking effect during the next full measurement interval pertaining to such changed metrics.

Additions

No more than once quarterly, ACSA may add Service Levels by sending written notice to the Service provider at least 30 (thirty) days prior to the date that such added Service Levels are to be effective. The target performance levels for such additional Service Levels shall be determined by mutual agreement of the Parties using industry standard measures.

Deletions

ACSA may delete Service Levels by sending written notice to the Service provider at least thirty (30) days prior to the date that such deletions are to be effective.

8.0 MEETINGS AND REPORT REQUIREMENTS

8.1 The following section defines the meeting and report requirements for all services.

All reports must be submitted as defined in the below table. If reports are not delivered within the stipulated times, ACSA will withhold invoice payment for the month until the reports are submitted

Project meetings: Will be held weekly at ACSA and/or on demand for the duration of the project and arranged by the ACSA Project Manager. The meeting will be attended by the Service providers' Project Manager, as well as the ACSA Project Manager. The agenda for the meeting shall include but not be limited to project progress; project delays; risks & issues and project financials

Maintenance and Support Meetings: These meetings will be held as defined in the below table. ACSA and provider will ensure the required attendees are present at the meetings for the duration of the contract. The purpose of these meetings is to provide The provider a platform to report on their performance.

Meeting's definitions

Meeting Name and frequency	Participants and roles	Documents to be produced after meeting by Service provider
Weekly Service Review	• ACSA-IT PM (chair) • ACSA Technical Lead • ACSA Project Administrator	• Minutes of meeting • Running Action register for any open actions to be addressed
Weekly Project status update	• ACSA-IT PM (chair) • ACSA Business Analyst • ACSA Technical Lead • ACSA Project Administrator • Service Provider • ACSA Enterprise Security	• Minutes of meeting • Updated project schedule • Action register for any open actions to be addressed • Risks and Issues register
Monthly Care Review	• ACSA-IT PM (chair) • ACSA IT Operations • ACSA Enterprise Security • ACSA Security Services • Service Provider • ACSA Project Sponsor • ACSA Technical Lead	• Minutes of meeting • Action register for any open actions to be addressed • Risks and Issues register • Service Credit Report

Meeting Name and frequency	Participants and roles	Documents to be produced after meeting by Service provider
Quarterly review meeting	• ACSA-IT PM (chair) • ACSA Project Administrator • ACSA IT Operations • ACSA Enterprise Security • ACSA Security Services • Service Provider • ACSA IT Infrastracture	• Minutes of meeting • Action register for any open actions to be addressed • Risks and Issues register
Annual review meeting	• ACSA-IT PM (chair) • ACSA Airports Systems • ACSA Enterprise Security • ACSA Security Services • Provider Relationship Manager • ACSA Project Administrator • ACSA IT Infrastracture	• Minutes of meeting • Action register for any open actions to be addressed • Risks and Issues register

Reporting definitions

Frequency	Report Name	Report Content	Due date	Submit to	Format	Meeting Name and frequency
Daily	Fault Summary	Reported faults summary (resolved and outstanding) Weekly to review previous weeks' reports	Start of business every date	ACSA Technical Lead	Email written report summary with supporting tables.	Weekly Service Review
	Fault Summary escalation	Outstanding faults and notification Weekly to review previous weeks' reports	Start of business every date	ACSA Technical Lead	Email written report summary with supporting tables.	Weekly Service Review
	Re-opened fault summary	Re-opened reported faults Weekly to review previous weeks' reports	Start of business every date	ACSA Technical Lead	Email written report summary with supporting tables.	Weekly Service Review
Weekly	Summary Care Report	Summarized report weekly	COB every Friday	ACSA Technical Lead	Email written report summary with supporting tables.	Weekly Service Review

Frequency	Report Name	Report Content	Due date	Submit to	Format	Meeting Name and frequency
	Project and IMACD updates	Installations completed including relocations and projects. Present detailed job cards.	One day before project status update meeting	ACSA Technical Lead & ACSA Project Manager	Email written report summary with supporting tables.	Weekly Project status update
	Data/wire centre areas of concern	Testing done on data/core/wire centres highlighting areas of concern Weekly to review previous weeks' reports	3 days before meeting	Datacentre and Storage Operations Manager	Email written report summary with supporting tables.	Weekly Service Review
Monthly	Consolidated Care Report	Monthly consolidated report · Spares Usage · Calendar month Incidents · Payment · Monthly services deliverables · SLA Report (performance against SLR's) · SLA improvement plan ·Service Credits	3 days before meeting	Datacentre and Storage Operations Manager	Email presentation with attached supporting information	Monthly Care Review
	Preventative maintenance	Schedule of preventative maintenance for the following month for all sites	3 days before meeting	ACSA Technical Lead	Email Excel schedule document	Monthly Care Review
	Asset Data	Asset Register	3 days before monthly account meeting	ACSA Technical Lead	Email Excel document	Monthly Care Review
Quarterly	Stock levels	BOM register documenting stock levels on hand	3 days before quarterly review	ACSA Technical Lead	Email Excel document	Quarterly review meeting
	Contract appendix review	Review updates to contract appendixes are completed	3 days before Quarterly review meeting	ACSA Technical Lead	Email PDF document	Quarterly review meeting
	Baseline (CMDB) information	Review updates to Baseline CMDB	3 days before Quarterly review meeting	ACSA Technical Lead	Email Excel document	Quarterly review meeting

Frequency	Report Name	Report Content	Due date	Submit to	Format	Meeting Name and frequency
	Design documents for audit	Design document audit	3 days before Quarterly review meeting	ACSA Technical Lead	Email Word document on ACSA template	Quarterly review meeting
	Transformation	Performance, financial and development report of all transformation partners	3 days before Quarterly review meeting	ACSA Technical Ops manager	Presentation detailing performance and transformation progress, financial report	Quarterly review meeting
Annual	Proposed improvements report	Proposed improvements or enhancement report	3 days before annual review meeting	ACSA Technical Lead	Email Word document	Annual review meeting
	Annual performance SLA report	Consolidation of previous 12 months SLA performance	3 days before annual review meeting	Datacentre and Storage Operations Manager	Email PDF document	Annual review meeting
	Contract adherence review	Summary of contract requirements and adherence thereof	3 days before annual review meeting	Datacentre and Storage Operations Manager	Email PDF document	Annual review meeting

Table 38 Reporting table

9.0 SPECIAL TERMS

To preserve the integrity of the ACSA infrastructure the following special terms and conditions must be adhered to for the services described in this SOW

9.1 COMMON

Rate of exchange

The following terms will be used to deal with Rate of exchange during the term of the awarded contract for items affected by rate of exchange as per the pricing files.

All initial Quotations for engagements will use a Fixed Rate of exchange. This rate will be communicated by ACSA to the provider on a 3 Monthly basis. This rate will not be used for placing an order

Once scoping for an engagement is completed and funds secured. The provider will provide a final quote for the scope. This quotation must be fixed for a period of 7 days.

The final Quotation will be reviewed by the ACSA internal treasury department to approve the quoted rate of exchange.

ACSA will proceed with the order issuing process after treasury approval

Should a Purchase order not be provided during the quote validity period (as per 0) the provider must supply ACSA with a Variance order quote once the Purchase order is received. This Quote must clearly show the original Rate of Exchange and the actual rate of exchange.

The Variance order quotation will also be approved by the ACSA treasury department before any orders should be placed with the provider's suppliers