Annexure A - Scope of Work

For

Virtual and Physical Compute Infrastructure

Bid Number COR8097/2025/RFP

Description:

Request for Proposal for the supply, installation, commissioning, support, maintenance, decommissioning, and disposal of Virtual and Physical compute infrastructure for 60 months to Airports Company South Africa

CONTENTS

TABLES

FIGURES

1.0 INTRODUCTION

ACSA requires the services of a suitable, qualified, and certified provider to supply, install, commission, support, maintain, decommission, and dispose of Virtual and Physical compute infrastructure at all ACSA sites

1.1 High-Level Scope of Work Required

The list below covers the high-level of scope included in this RFP.

1.1.1 **Supply -** The provisioning of infrastructure-related hardware, cabling and related software licensing.

1.1.2 **Installation -** Installation of the procured equipment into the ACSA environment, including assembling, rack mounting and all cabling connections.

1.1.3 **Commissioning -** The configuration of the new equipment to the OEM and agreed standards, as well as the migration of all data and configurations from the existing infrastructure

1.1.4 **De-Commissioning -** The decommissioning of old equipment once all migrations are done, including removing any configuration and data, removing from racks, removing any redundant cabling, and moving old equipment to designated storerooms. Removal of data from devices should adhere to ACSA decommissioning standards and should produce a data removal certificate, using sanitisation tools that are NIST SP 800-8 compliant/certified.

1.1.5 **Disposal -** The disposal using possible sale or physical destruction of decommissioned equipment following ACSA processes

1.1.6 **Warehousing -** Provide off-site storage for ordered equipment and ensure the equipment is always fully insured. ACSA will request proof of insurance and occasionally require amendments to the insurance provisions to align with ACSA's insurance requirements.

1.1.7 **Asset Management -** Create and manage an Asset Register and Asset Tagging of all newly purchased equipment as per the ACSA standard template. Asset tagging shall be done as per specifications and instructions from ACSA.

1.1.8 **Maintenance and support -** Provide corrective and preventative maintenance as well as support per the defined SLRs

1.2 Service Objectives

The following are the critical high-level Service objectives ACSA expects to achieve through this RFP.

1.2.1 Provide a uniform, reliable, scalable, and resilient IT Server and Virtualisation infrastructure to ACSA.

1.2.2 Acquire services with service quality guarantees backed by Service-Level Agreements (SLAs) as well as the OEM.

1.2.3 Achieve the Service Level Agreement (SLAs) specified.

1.2.4 Provide ACSA with a high-quality, uniform, stable, flexible, managed, monitored and sustainable compute infrastructure as determined by the service level requirements and key performance indicators.

1.2.5 Provide ACSA with the ability to expand its service delivery and support services to ACSA business, subsidiaries, and stakeholders.

1.2.6 Continually reduce the cost-of-service delivery, and the cost of ownership through the re-use or transition of existing infrastructure, and through the effective utilisation of existing licensing agreements.

1.2.7 Dispatch and monitor break/fix repairs, including services performed by other suppliers within SLA

1.2.8 Perform approved Infrastructure Moves Adds, Changes and Decommissions/Disposals (IMACD) Services for Hardware and Software.

1.2.9 Track the inventory of in-scope software and hardware as required.

1.2.10 Technical orientation/training for existing/new employees on existing and new systems.

2.0 Service Environment

2.1 The current infrastructure

The following subsections and related appendices further describe and scope the hardware and software currently deployed.

Category	Service	Description
Hardware	**BladeSystem Chassis**	HP BladeSystem Enclosure C7000 HP Synergy 12000 Frame
	BladeSystem Interconnects	HP BladeSystem Virtual Connect VC Flex-10/100
		HP BladeSystem Virtual Connect 16 Gb FC module
	BladeSystem, Rack Mount and IBM Servers	HP BL 460C Gen 5 to 10
		HP BL 660 Gen 7 to 9
		HP DL 380 Gen1 to 9
		HPE Synergy 480 Gen10
		IBM Power 770 servers
		IBM Power S824
		IBM DataPower
		IBM Message Queuing (MQ)
	Hyperconverged	Dell EMC VXRail S670
Software	**HP**	HP Virtual Storage Software, OneView
	Microsoft	Microsoft Windows Hyper-V
	VMware	VMware Suite of software, including VSAN
	IBM Power System Firmware	IBM Power System Firmware Software & Updates
	IBM AIX Operating System	IBM AIX Operating System Software & Updates

Table 1 - High-Level List of Existing Infrastructure and Software

2.2 Service locations.

2.2.1 A description and location of all ACSA facilities and office locations requiring in-scope services.

Cluster	Airports in the regions	Site Code
Cluster 1	• OR Tambo International Airport	JNB
	• Aviation Park	AVP
	• Bram Fischer International Airport	BFN
Cluster 2	• Cape Town International Airport	CPT
	• George Airport	GRJ
	• Kimberley Airport	KIM
	• Upington International Airport	UTN
Cluster 3	• King Shaka International Airport	DUR
	• King Phalo Airport	ELS
	• Chief Dawid Stuurman International Airport	PLZ

Table 2 - ACSA Clusters

SITE CODE	ADDRESS
JNB	OR Tambo International Airport, Airport Rd, Johannesburg, 1627
AVP	Aviation Park Building OR Tambo International Airport, Airport Rd, Johannesburg, 1627
CPT	Cape Town International Airport, Matroosfontein, Cape Town, 7490
DUR	King Shaka International Airport, La Mercy, 4407
PLZ	Port Elizabeth Airport, Allister Miller Drive, Walmer, 6070
GRJ	George Airport, Old Mosselbay Road, George, 6529
ELS	East London Airport, Settlers Way, East London, 5200
KIM	Kimberly Airport, Compound Patterson Road, Kimberly, 8300
BFN	Bram Fischer International Airport, Bloemfontein, 9300
UTN	Upington International Airport, Diedericks Street, Upington, 8801

Table 3 - Detailed site schedule

2.2.2 This Site Schedule will be revised by agreement between the ACSA and the service provider Account Manager/Service Manager from time to time to meet the ACSA's requirements at additional locations.

3.0 PRICING NOTES

The following notes should be considered when pricing services for this tender.

3.1 USD-influenced items can be adjusted with the Rate of exchange during the contract term, according to the process and terms in Section 4.

3.2 Bidder quotations can be added as additional information, but the pricing file must be filled in in the format provided.

3.3 Only fill in columns in green in the pricing file.

3.4 **NOTE that ACSA reserves the right to reduce the scope depending on business needs. There is no guarantee that the full bill of materials will be executed. Pricing will not be changed due to less bill of materials**

4.0 RATE OF EXCHANGE, QUOTATIONS, AND INVOICES

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

4.1 Rate of exchange for the offer validity period

4.1.1 Pricing must be valid for 120 days from the RFP closing date.

4.1.2 The exchange rate is provided in the pricing file.

4.2 Quotations and Rate of Exchange during the execution phase

4.2.1 All initial quotations for engagements will use a fixed rate of exchange. This rate must be requested by the Service provider on a 3-month basis. This rate will not be used to place an order.

4.2.2 Once scoping for an engagement is completed and funds are secured. The provider will provide a final quote for the scope. This quotation must be fixed for 14 days.

4.2.3 The ACSA internal treasury department will review the final quotation to approve the quoted exchange rate.

4.2.4 ACSA will proceed with the order-issuing process after treasury approval.

4.2.5 Should a purchase order not be provided during the quote validity period (as per 4.2.2The provider must supply ACSA with a Variance order quote once the Purchase order is received.

4.2.6 This Quote must clearly show the original Rate of Exchange and the actual exchange rate (the spot rate for the day the order is placed with the provider's supplier).

4.2.7 ACSA will proceed with obtaining approval of the Variance order quotation RoE.

4.2.8 Once approved, a variance order will be processed.

4.2.9 Pricing is based on a fixed markup % per item type. ACSA may, at its own discretion, ask for the supplier's quote to be provided for every engagement. This will be used to verify the landed cost and to audit if the % mark-up as quoted for the type of device is upheld as per the pricing schedule.

4.2.10 If products were previously procured by the provider for stock, then the original invoice for that stock should be provided as proof against the quotation.

4.2.11 All quotations to be provided in PDF and Excel format (editable). And must have all relevant fields as per the Pricing schedule.

4.3 Additional Quotations

4.3.1 All initial quotations for engagements will use a fixed rate of exchange. This rate must be requested by the Service provider on a 3-month basis. This rate will not be used to place an order.

4.3.2 Once scoping for an engagement is completed and funds are secured. The provider will provide a final quote for the scope. This quotation must be fixed for 14 days.

4.3.3 Pricing is based on a fixed markup % per item type; ACSA may, at its discretion, ask for the supplier quote to be provided for every engagement. This will be used to verify the landed cost and to audit if the % markup quoted for the type of device is upheld per the pricing schedule.

4.3.4 If the provider previously procured products for stock, the original invoice for that stock should be provided as proof against the quotation.

4.3.5 All quotations will be provided in PDF and Excel format (editable). It must have all relevant fields as per the pricing schedule.

4.4 Invoices

4.4.1 All invoices to be accompanied by:

I. Copy of purchase order
II. Proof of delivery, signed by the provider and an ACSA representative, includes the relevant serial numbers.
III. The asset list is in Excel format according to the template provided by ACSA.
IV. Proof of automated asset tracing activation.
V. Invoice to have the ACSA purchase order number coded on it.

4.4.2 All invoices not in dispute will be paid according to payment terms in the final agreement.

5.0 ASSET MANAGEMENT, TRACKING and LOSSES

Due to the nature of the equipment related to the services covered by this RFP, the following should be noted for special attention.

5.1 Asset management

5.1.1 ALL devices (new and returned) remain in the provider's control until handed over to an ACSA user/representative. This handover needs to be recorded officially with a signed handover form by an **ACSA employee**. The record must be attached to the ASSET record for future reference.

5.1.2 For approved disposals, the provider must wipe the device; certified proof must be provided and included in the service cost.

5.1.3 The history of every device must be kept in the asset register or system provided.

5.1.4 An ACSA resource or representative and a provider representative must sign for all deliveries. Planning should consider this when deliveries to the onsite are arranged, as this will affect the Service levels.

5.1.5 On-site stock should be kept to the required levels to ensure service delivery according to SLRs.

5.1.6 The monthly storeroom stock count is to be completed, with updated stock sheets to be submitted to ACSA and reported on in the monthly SLA meeting. Movements in the month to be accounted for in the summary schedule (listing device info, detail of asset move (i.e. end user it was moved to / new store or location it was moved to) and service request number supporting the move).

5.2 Asset Tags and Tracking

5.2.1 ACSA will provide financial asset tags to the provider for affixing to the devices. Devices must be asset-tagged before being installed.

5.3 Asset movement

5.3.1 Any asset that must be transferred to another ACSA site by the provider for whatever reason must follow the ACSA asset transfer process before the movement.

5.3.2 NO device covered under the **onsite repair SLA** can be removed from an ACSA site. The device must be repaired onsite as per the SLA.

5.4 Losses

5.4.1 Any loss needs to be formally reported to ACSA within 2 days of the loss being detected.

5.4.2 Any device, whether new, decommissioned, operational or damaged, that is lost, for whatever reason, that is in the control of the provider must be replaced at the provider's cost.

5.4.3 The process of replacement must be actioned within 5 days after the loss is detected by either party.

5.4.4 Any loss where the provider does not have enough proof that the device was NOT in their control (Issue forms, transfer forms) will be deemed in their control.

5.4.5 The following table lists the value and terms of the replacements:

Device Age	Replacement Terms
<=12 months	Replacement of the device with a new device at the current prevailing ACSA standard
12 to < 18 months	Monetary Replacement of 90% of the original device's cost
18 to < 24 months	Monetary Replacement of 70% of the original device's cost
24 to < 30 months	Monetary Replacement of 60% of the original device's cost
30 to < 36 months	Monetary Replacement of 50% of the original device's cost
36 to < 42 months	Monetary Replacement of 30% of the original device's cost
42 to < 54 months	Monetary Replacement of 15% of the original device's cost
54+ months	Monetary Replacement of 10% of the original device's cost

Table 4 – Loss replacement terms and values

5.4.5.1 Monetary values must be credited to ACSA's account and will be used to procure new devices.

5.4.5.2 Monetary values cannot be allocated to outstanding monies for other invoices.

5.5 **Replacement due to damage/malfunctions (in warranty)**

5.5.1 If a device needs to be replaced during its life due to damage or malfunction, the provider must inform the ACSA representative and follow the provided asset disposal process for damaged/malfunctioning devices.

5.6 **Equipment Ownership Transfer**

5.6.1 Any equipment procured under the agreement only transfers ownership when delivered to an ACSA site, with the approved ACSA resource signature confirming receipt.

5.6.2 The provider must ensure off-site storage is available for the bulk of the equipment until site preparation is concluded.

5.6.3 All warranties and licenses of equipment only "start" when the equipment transfers ownership and must be activated with the OEM.

5.6.4 Although equipment ownership transfers, it is still the responsibility and accountability of the provider to manage the on-site equipment. Until such time, a transfer form is obtained from an ACSA resource or representative, and the equipment is in the provider's control.

5.6.5 Any losses before obtaining the issue forms are for the provider's account.

5.7 Equipment Storage

5.7.1 All equipment is to be warehoused by the provider at no cost to ACSA until it is delivered.

5.7.2 Equipment delivered to the site will be installed in its final location, where possible

6.0 PERSONNEL

6.1 **Qualified Staffing -** 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.

6.2 **Certification Compliance** - The Provider will be required to meet all ACSA-IT requirements for certification during the term of the contract. All additional certification requirements will be communicated by ACSA and must be fulfilled within 4 months of the request. The relevant onsite personnel, if any, are listed in **Table 7 - Resource Requirements**

6.3 **Onsite Resource Availability** - Suitably certified personnel must be available onsite at designated locations for preventative and corrective maintenance. While normal working hours apply, after-hours availability may be required to accommodate maintenance windows or resolve disruptive incidents, ensuring minimal service disruption.

6.4 **Flexible Resourcing Model** - The provider must adapt its resourcing model to meet the Service Level Requirements (SLRs) outlined in 14.0 SERVICE MANAGEMENT, utilising permanent onsite resources for preventative maintenance and variable offsite resources for corrective maintenance to ensure efficient and compliant service delivery.

6.5 **Restricted Resource Use** - Onsite resources may not be reassigned to projects without prior written approval from the ACSA Technical Operations Manager: DataCenter and Storage or Senior Manager: IT Infrastructure, ensuring dedicated support for operational needs.

6.6 **Security Vetting** - All resources must undergo security vetting by the state security agency at a secret level. Required forms and documentation must be submitted within the first month of the contract. Any resource failing the vetting process must be replaced immediately to maintain security compliance.

6.7 **NDA Compliance** - All resources must sign the ACSA Non-Disclosure Agreement (NDA) provided in this tender, ensuring confidentiality and protection of sensitive information.

6.8 **Service Coverage Windows -** Most commissioning and migration activities will be done after operational hours (between 22:00 and 5:00. Refer to Table 5 - Service Coverage Window Definitions. Please consider this in the proposal

6.9 The table below indicates the minimum expectation for resources, whether on-site or variable. Please increase as necessary.

Most commissioning and migration activities will be done after operational hours (between 22:00 and 5:00. Refer to Table 6 - Service Coverage Window Definitions. Please consider this in the proposal

Role	Location	High-Level Function	Minimum Resources Required and Coverage Window
Senior Site Manager	JNB	• Senior Site Manager based at ORTIA and accountable for all sites	JNB: Onsite 1 resource Standard Office Hours

Role	Location	High-Level Function	Minimum Resources Required and Coverage Window
		• Attend SLA meetings, ITAC, and general meetings with IT Operations and stakeholders • Report to the IT Technical Operations Manager, Data Centre and indirectly to the Senior Manager: IT Infrastructure • Project and contracts management experience coupled with a minimum of 5 years of IT infrastructure exposure • Manage Service Provider staff, • Represent the Service Provider in project requests and project meetings • Monitor the environment • IMACD plans • Resource and stock planning • Reporting • Expert advice on managing the infrastructure • Co-ordinate new requests, change requests, drawings, documentation, and quality control • Co-ordinate new permit, application, logical and elevated rights access applications • Assist with IT commercial initiatives and manage all site installations/projects/maintenance • Ensure that all safety requirements are strictly complied with – this includes updating safety files, acquiring approvals for hot works/airside works, the use of the correct safety equipment for all installations, as well as the use of correct signage. • The site manager will be utilised within the operations and project environments. •	Ad-hoc: Weekday After Hours and Weekends as per the standby schedule / as required

Role	Location	High-Level Function	Minimum Resources Required and Coverage Window
Expert Technicians Server and Virtualisation (3rd Level)	All sites	Assist with escalations from Senior engineers	All sites: Remote 1 resource Level 3 remote support whenever necessary, office hours, after hours and over weekends
Senior Technicians Server and Virtualisation	JNB CPT DUR	• OEM accreditation and certified installers with a minimum of 2 years' experience and professional knowledge to support the environment • Responsible for installations, maintenance, Corrective Maintenance, monitoring the environment, testing, temporary resolutions and advanced 3rd line diagnosis. • May be required to travel to the associated airports when required. • Attend meetings with ACSA and other stakeholders at the airports. • Responsible for drawings, documentation, change requests, quality control and planning before the commencement of any works. • To be primarily utilised within the operational environment and may be used within the project's environment only upon written approval from the ACSA Infrastructure engineer.	JNB: Onsite Min 1 resource Standard Office Hours Ad-hoc: Weekday After Hours and Weekends as per the standby schedule / as required CPT: Onsite Min 1 resource Standard Office Hours Ad-hoc: Weekday After Hours and Weekends as per the standby schedule / as required DUR: Onsite Min 1 resource Standard Office Hours Ad-hoc: Weekday After

Role	Location	High-Level Function	Minimum Resources Required and Coverage Window
			Hours and Weekends as per the standby schedule / as required
Technicians Server and Virtualisation	JNB **Local representation per site** (to be on-site on an ad-hoc basis within SLA when required) PLZ ELS BFN KIM GRJ UTN	• OEM accreditation and certified installers with professional knowledge to support the environment • Monitor incidents by using the monitoring tools that were installed at ACSA • Escalate the incidents to the correct team member • Provide 1st line information to assist with troubleshooting the call • Escalate incidents to other ACSA departments if required • Follow the change process to assist the operational team	JNB: Onsite Min 1 resources must be on-site 24/7/365 Regional Sites: Ad-hoc as required per SLA
Senior Technicians IBM Power Series and AIX	JNB	**Software Support Services** • Support the in-scope server operating system, system management software and operating system utilities, including minor upgrades (such as a release upgrade) • Manage the operating system configuration, including initial server configuration, modifying configuration files, system configuration documentation and access to system configuration files • Manage the operating system file systems, including creating, maintaining, and deleting volumes and directory structures, modifying file system sizes, verifying mount point availability, repairing defective file systems and modifying file system permissions	JNB: Onsite Min 1 resource Standard Office Hours Ad-hoc: Weekday After Hours and Weekends as per standby schedule / as required

Role	Location	High-Level Function	Minimum Resources Required and Coverage Window
		• Monitor and reduce operating system log files to prevent file systems from overfilling • Manage Operating System Processes (e.g., investigate continuously running system subtasks, or daemons), including refreshing processes as required, establishing start-up sequences, maintaining system clock synchronisation, and changing process priorities as appropriate. • Recommend operating system updates and configuration modifications to ACSA's Point of Contact, as required • Apply operating system patch set updates, as required • Maintain tools for remote management and alert monitoring • Maintain operational support procedures • Maintain the hardware and software configuration server information • Manage System IDs and domain structure • Evaluate planned changes to the server environment and advise of any requirements to support such changes • Enable passwords for servers to use to connect with other servers on the network • Adhere to standard security processes and procedures (Does not include User ID Admin) • Support trusted third-party security server authentication • Synchronise security information among servers • Create and modify system login/logon scripts	

Role	Location	High-Level Function	Minimum Resources Required and Coverage Window
		• Assign account, workgroup and print managers • Provide health check and trending reports that include CPU, Memory (RAM), Disk and Server Red • Action List (servers that have gone above the defined set thresholds) • Assist with AIX version upgrades on the in-scope servers and migration of the data associated with the in-scope LPARs from one (1) IBM storage device to another **Performance Management** • Manage queues for incidents, problems, changes and other service requests about performance. • Manage thresholds and alerts for usage of IT resources; • Analyse performance service level breaches, alerts, trends, and root causes to restore service; • Track and tune proactively performance through trend and exception reporting to avoid possible service level breaches; • Tune reactively to restore service for performance incidents and root causes; • Provide corrective action to resolve system performance problems and provide recommendations to prevent possible future incidents; • Recommend changes to maintain agreed-upon system performance levels; • Implement performance changes as approved through a formal change management process; • Define performance-related metrics and data collection,	

Role	Location	High-Level Function	Minimum Resources Required and Coverage Window
		summarisation, and storage requirements; • Collect, summarise and store performance data (Standard Performance Data Management); • Define performance alert thresholds to support agreed-upon service levels; • Provide Standard Performance Reporting; • Provide Ad hoc Performance Reporting for analysis of incidents to restore service. • Determine policies for use within Performance tooling, and recommend customisation and maintenance of standard Performance Management tooling to maximise productivity benefits. • Provide administrative services, but do not take control of your day-to-day operational activities, assist with the following: o Adding, modifying, or deleting User IDs; o Adding, modifying, or deleting user access rights; o Adding, modifying, or deleting user groups; o Adding, modifying, or deleting user policies; and o Authenticating existing users and access rights.	
Technical Specialists/Commissioning engineers	All sites	• OEM accreditation and certified installers with a minimum of 2 years of experience and professional knowledge to support the environment. • Responsible for installations, commissioning and migration • May be required to travel to the associated airports when needed. • Attend project meetings. • Responsible for drawings, documentation, quality control and	As required by the project schedule.

Role	Location	High-Level Function	Minimum Resources Required and Coverage Window
		planning before the commencement of any works.	
Project Manager	JNB	• Project planning, scheduling, and coordination • Resource allocation and management. • Risk assessment and mitigation. • Communication management. • Documentation management • Stakeholder engagement. • Budget management. • Quality assurance. • Change management. • Issue resolution.	In accordance with the project plan

Table 7 - Resource Requirements

6.10 The provider will be liable to pay parking fees for any necessary resources to be located on-site or perform work under this contract at any ACSA premises.

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

6.12 Resources are required to keep their permits valid and available for the duration of the contract.

6.13 The provider will be liable for any fees for renting office space for any resources required at each site for the duration of the contract.

6.14 Please refer to **Annexure G - Parking,Permits** and Office space for rates.

<table>
<tr><th>Service Class</th><th>Service Coverage Window</th></tr>
<tr><td>Airport Operating Hours</td><td>
<table>
<tr><th>Airport</th><th>Earliest opening hour</th><th>Latest closing Hour</th></tr>
<tr><td>ORTIA and AVP</td><td>24-hour operation</td><td>24-hour operation</td></tr>
<tr><td>CTIA</td><td>05:00</td><td>23:00</td></tr>
<tr><td>KSIA</td><td>04:00</td><td>22:00</td></tr>
<tr><td>PLZ</td><td>05:00</td><td>22:00</td></tr>
<tr><td>ELS</td><td>05:00</td><td>21:30</td></tr>
<tr><td>GRJ</td><td>06:00</td><td>20:00</td></tr>
<tr><td>BFN</td><td>05:30</td><td>20:00</td></tr>
<tr><td>KIM</td><td>06:00</td><td>20:00</td></tr>
<tr><td>UTN</td><td>06:00</td><td>18:00</td></tr>
</table>
</td></tr>
<tr><td>Standard Office Hours</td><td>Normal Office Hours - 08:30 - 17:00 on Mon - Fri, excluding public holidays</td></tr>
<tr><td>Extended Office Hours</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 impacting the live environment will occur 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.</td></tr>
</table>

Table 8 - Service Coverage Window Definitions

6.15 **Robust Resourcing Model -** The provider must implement a resourcing model that ensures compliance with Service Level Agreements (SLAs) and supports service delivery during defined Service Coverage Windows, always maintaining a full complement of resources to avoid service disruptions.

6.16 **Resource Replacement -** In the event of an assigned resource's absence, the provider must promptly replace them with an equally qualified and competent resource who possesses the necessary access permits, training, and site-specific knowledge to maintain service continuity.

6.17 **Restricted Resource Allocation -** The provider must not deploy support resources to projects or Install, Move, Add, Change, Dispose and Delete / Dispose (IMACD) activities, ensuring focus on core operational support.

6.18 **Safety Compliance -** The provider must compile and maintain a safety file following ACSA standards within the first month of service commencement. This file must be kept current, unless ACSA communicates that it is not required, ensuring adherence to safety protocols.

7.0 EQUIPMENT AND SPARES HOLDING REQUIREMENTS

7.1 **Technician Equipment -** The provider must equip all service technicians with appropriate tool kits and testing equipment to perform their duties efficiently, ensuring no delays in service delivery.

7.2 **ACSA-Provided Devices -** ACSA will supply laptops or desktops for permanent onsite resources, with the device type determined during the enablement request stage, ensuring compatibility with operational needs.

7.3 **Critical Spares Availability -** The provider must maintain sufficient critical spare parts at all locations to support maintenance activities and meet Service Level Agreements (SLAs), minimising downtime.

7.4 **Backup Stock for SLA Compliance -** If the provider's back-to-back agreement with the OEM cannot meet SLA requirements, the provider must maintain its own backup or loan stock to restore services within the specified maintenance SLA, ensuring uninterrupted operations**.**

7.5 **Quality Replacement Parts -** The provider must replace or repair faulty components using original, manufacturer-guaranteed new parts of the same or higher grade as the original. If an exact match is unavailable, a higher-grade component must be used. Replaced parts must be certified by the device manufacturer to ensure reliability and compatibility.

7.6 **Parts Storage and Obsolescence Management -** Within 60 days of contract award notification, the provider must establish a warehouse or secure storage facility to stock all necessary parts and components, including those for in-scope devices declared obsolete or no longer supported by manufacturers (e.g., post End of SW Maintenance Releases, End of Routine Failure Analysis, End of New Service Attachment, End of Service Contract Renewal, or Last Date of Support). This ensures full SLA compliance and uninterrupted service for all equipment

8.0 PREVENTATIVE AND CORRECTIVE MAINTENANCE

8.1 **Preventive Maintenance Scope -** Preventive 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.

8.2 **Corrective Maintenance Scope -** Corrective maintenance includes all activities initiated following a preventative maintenance inspection to address identified issues, ensuring continued system reliability and performance.

8.3 **Break/Fix Maintenance -** Break/fix maintenance addresses unforeseen issues requiring urgent repairs to restore infrastructure serviceability and system functionality. This may include after-hours, weekend, or public holiday requests, and the provider must respond promptly to all faults.

8.4 **After-Hours Support -** The provider must provide callout-based support for incidents impacting systems during after-hours, weekends, and public holidays. Applicable hourly rates and callout fees must be detailed in the pricing schedule to ensure transparency.

8.5 **Emergency Callouts -** The provider must accommodate short-notice callouts for emergencies caused by system interruptions or airport change processes, providing site-specific callout rates and hourly fees to ensure rapid response and minimal disruption.

8.6 **Planned Activity Coordination -** For planned maintenance activities, ACSA will provide advance notice, and the provider must ensure resource availability as required to execute tasks efficiently.

8.7 **Accessible Support Contacts -** The provider must supply after-hours telephone numbers for reachable support personnel, ensuring constant availability. 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.

8.8 **Maintenance Schedule Overview -** The Preventive Maintenance Schedules table outlines high-level maintenance tasks and checks to guide the provider's planning and execution of maintenance activities.

8.9 **Detailed Maintenance Plan -** The Service 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 Work Order. In the detailed preventative maintenance schedule, The Service Provider must include all remedial actions to be taken (include what communication will be actioned; which Service 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.

9.0 Baseline Information

9.1 Information supplied in these tables is accurate as of the time of this tender's publishing. Additions or subtractions could have been affected since then.

9.2 The quantities in this list are to be entirely replaced by the new infrastructure as part of this Tender and **should be included for physical decommissioning and disposal**.

Site Code	BladeSystem Enclosures	Blade Servers	Rack Mount/tower Servers
JNB	15	160	30
KIM	0	0	6
BFN	0	0	6
CPT	5	30	30
GRJ	0	0	6
UTN	0	0	6
DUR	4	13	15
ELS	0	0	6
PLZ	0	0	6

Table 9 - IT Server Baseline

10.0 Detailed Technical Scope

This section provides the detailed technical requirements for the services required.

The current virtual infrastructure landscape ACSA has in place is disjointed, and most of the hardware support has reached the end of its life, except for the infrastructure at the PLZ site.

The aim is to replace all this old infrastructure and reuse the equipment at PLZ for a dev testing environment in the new design and architecture.

It is required to have only three main virtual data centre implementations at JNB, DUR and CPT. The regional sites (PLZ, ELS, GRJ, BFN, UTN and KIM) require very little infrastructure for local high network utilisation systems like CCTV and Parking management, as well as other local services like DHCP, printing, imaging of end-user equipment, and caching of patches.

10.1 **Virtualisation infrastructure**

10.1.1 The solution must be primarily based on a HCI/dHCI Software-designed data centre architecture. However, additional traditional clusters can be added for workloads that cannot function in this manner (e.g. requirements to connect to external physical storage)

10.1.2 Only one OEM for hardware and one for software can be used.

10.1.3 Hardware should be fully certified by the OEM of the virtualisation software.

10.1.4 The certification testing frequency should be at least 4 times per year. Testing must validate the compatibility of software, firmware, and driver components.

10.1.5 The solution must have full update automation that includes software, firmware, and driver components.

10.1.6 Full integration of the Hardware and software OEM support structures.

10.1.7 Local availability of hardware spares and services

10.1.8 The solution must be capable of using a Software-based SAN as well as a Physical SAN. There is a requirement for all hosts to be able to connect to external DELL Unity SAN devices via 32Gbit FC connectors. This requirement is specifically for the CCTV system. **If this requirement is not possible using ONE cluster per Site**, then it can be achieved by adding a secondary cluster. It is understood that a one-click upgrade (automation) will not be possible for the clusters that are connected to the Physical SAN.

10.1.9 The regional sites (smaller airports) only one cluster is allowed.

10.1.10 LiveOptics scans were concluded for 7 days for the three central sites; the scans also include the regional sites that each relevant central site will support. The Hyper-V hosts and some current physical servers were included, some of which will be virtualised.

10.1.11 The scans exclude any physical CCTV servers, but these servers must be catered for in the proposal as per the specifications provided.

10.1.12 Additional projects require capacity in the clusters; these specifications are also provided in section 10.5 **New/additional Virtual Machine Specifications**.

10.1.13 The node failure tolerance should be N+2 for the main centre clusters

10.1.14 Two-node clusters are acceptable for the regional sites. Witness appliances can be hosted at a central site

10.1.15 It is important to note that there is a requirement for the infrastructure to support full Windows Server Failover Clustering (WSFC).

10.1.16 Migration of workloads must be possible, live and offline VMs as well as migrating storage

10.1.17 Must support virtual networking and VLANs (802.1q)

10.1.18 Role-based access control (RBAC) for administrators and users, with granular permissions. (RBAC)

10.1.19 Must integrate to Azure/Local AD

10.1.20 Must support containers (Kubernetes)

10.1.21 Ability to deploy virtual machines with a virtual Trusted Platform Module (vTPM)

10.1.22 Must integrate into the major hyperscalers in the market seamlessly. (Hybrid cloud connectivity)

10.1.23 Support for encryption of data at rest (e.g., VM disks) and in transit (e.g., VM migration, management traffic).

10.1.24 Support for VM-level snapshots, cloning, and cross-node or cross-site replication for backup and disaster recovery.

10.1.25 Isolation of network traffic for different departments or workloads sharing the same environment.

10.2 Physical Servers

10.2.1 All current physical servers have reached the end of life.

10.2.2 The objective is to migrate the majority of these physical servers to the new virtualised infrastructure. The list of physical servers is supplied in Appendix A.

10.2.3 The LiveOptics scans of most of these servers are included in the scans mentioned above.

10.2.4 The quantity of the physical server hardware is not guaranteed to be executed. During the project, each Physical server will be evaluated to determine the possibility of

virtualisation. Only if a server cannot be virtualised physical hardware devices will be procured. Should more servers be added to the virtual cluster than the initial capacity caters for, additional capacity will be added to the cluster.

10.3 **Monitoring and Management**

10.3.1 **Virtualisation**

10.3.1.1 A unified interface or dashboard for managing VMs, hosts, storage, and networking across the platform. All aspects must be included in the management system from Virtual Machines, Kubernetes clusters, as well as the physical infrastructure that supports the solution. The use of AI is encouraged.

10.3.1.2 Real-time monitoring of performance, resource usage, and system health, with customizable alerts and reporting.

10.3.1.3 scripting support (e.g., PowerShell, Python) and orchestration tools (e.g., Ansible, Terraform) to automate deployment and management tasks.

10.3.1.4 Comprehensive logging of system events and user actions for troubleshooting and audit purposes.

10.3.1.5 The system must support an Application Programming Interface (API) for accessing data.

10.3.1.6 The system should be able to set reports and automate them as well.

10.3.1.7 Tagging of resources must be possible. Tagging involves attaching descriptive metadata to resources in the SDDC (compute, storage, networking, or management objects). These tags categorise resources based on attributes like purpose, environment, owner, or application type, making it easier to manage complex, virtualised environments.

10.3.1.8 All clusters across the country must be incorporated into the central system.

10.3.1.9 If the virtualisation is achieved via separate HCI and standard clusters, the standard clusters must also be incorporated into the management system centrally.

10.3.1.10 The solution must have full update automation that includes software, firmware, and driver components (“one-click updates”)

10.3.2 **Physical Servers**

10.3.2.1 A Central system is required to manage and monitor the infrastructure/Solution.

10.3.2.2 Must be able to do firmware updates from the system centrally across the country.

10.3.2.3 The system must support an API for accessing data.

10.3.2.4 The system should be able to set reports and automate them as well.

10.3.2.5 Tagging OR annotating of resources must be possible.

10.4 Hardware Maintenance and Warranties

10.4.1 All hardware must be supplied with a 5 year warranty that includes a maximum of 4 hours of hardware fix 24x7x365. This will be referred to as the initial period. In the initial period, no additional costs will be incurred for hardware fixes.

10.5 New/additional Virtual Machine Specifications

The following section provides the specifications for virtual machines to be added over and above the results of the Liveoptic scans. The projects requiring additional capacity are:

- E-Gates System
- CCTV System
- FIDS System
- Baggage System
- Parking System
- SharePoint 2019
- Oracle Business Intelligence Enterprise Edition (OBIEE)
- Oracle E-Business Suite (OEBS)
- Enterprise Services Bus (ESB)
- SQL Cluster Hardware
- IBM Hardware
- Additional Information

10.5.1 **E-gates**

10.5.1.1 This is a new System, and no Virtual Machines have been created for it yet. The Specifications for the required Virtual Machines are included in the table below.

10.5.1.2 The system will be deployed at JNB for Production and pre-production. DR to implement a CPT

10.5.1.3 **Assume a constant 80%+** resource utilisation for the new Virtual Machines.

10.5.1.4 Virtual Machine Requirements

10.5.1.4.1 **Production (JNB)**

	VM HW Resource allocation							
	Service	**Host**	**vRAM (GB)**	**vCores**	**Storage (GB)**			**OS**
					System	**Swap**	**Data**	
Tier1	Node 1	1	16	8	80	16	0	Linux
	Node 2	2	16	8	80	16	0	Linux
Tier 2	App 1 Node 1	1	12	8	80	12	0	Linux
	App 1 Node 2	2	12	8	80	12	0	Linux
	App 2 Node 1	3	32	10	80	32	50	Linux
	App 2 Node 2	4	32	10	80	32	50	Linux
	App 3 Node 1	3	16	6	80	16	0	Linux
	App 3 Node 2	4	16	6	80	16	0	Linux
	App 3 Node 3	5	16	6	80	16	0	Linux
	LB Tier 2 - Node 1	6	16	8	80	16	0	Linux
	LB Tier 2 - Node 2	7	16	8	80	16	0	Linux
	Analytics - node 1	6	96	14	80	96	3 000	Linux
	Analytics - node 2	7	96	14	80	96	3 000	Linux
	Analytics - node 3	8	96	14	80	96	3 000	Linux
Tier 3	Tier3 - node 1	9	16	8	80	16	23	Linux
	Tier3 - node 1	10	16	8	80	16		Linux

Table 10 – e-Gate Server Requirements - Production

10.5.1.4.2 Pre-Production (JNB)

	Service	Host	VM HW Resource allocation					
			vRAM (GB)	vCores	Storage (GB)			OS
					System	Swap	Data	
Tier1	Node 1	1	16	8	80	16	0	Linux
	Node 2	2	16	8	80	16	0	Linux
Tier 2	App 1 Node 1	1	12	8	80	12	0	Linux
	App 1 Node 2	2	12	8	80	12	0	Linux
	App 2 Node 1	3	32	10	80	32	50	Linux
	App 2 Node 2	4	32	10	80	32	50	Linux
	App 3 Node 1	3	16	6	80	16	0	Linux
	App 3 Node 2	4	16	6	80	16	0	Linux
	App 3 Node 3	5	16	6	80	16	0	Linux
	LB Tier 2 - Node 1	6	16	8	80	16	0	Linux
	LB Tier 2 - Node 2	7	16	8	80	16	0	Linux
	Analytics - node 1	6	96	14	80	96	3 000	Linux
	Analytics - node 2	7	96	14	80	96	3 000	Linux
	Analytics - node 3	8	96	14	80	96	3 000	Linux
Tier 3	Tier3 - node 1	9	16	8	80	16	23	Linux
	Tier3 - node 1	10	16	8	80	16		Linux

Table 11 – e-Gate Server Requirements – Pre-Production

10.5.1.4.3 DR (CPT)

	Service	Host	VM HW Resource allocation					
			vRAM (GB)	vCores	Storage (GB)			OS
					System	Swap	Data	
Tier1	Node 1	1	16	8	80	16	0	Linux
	Node 2	2	16	8	80	16	0	Linux
Tier 2	App 1 Node 1	1	12	8	80	12	0	Linux

	App 1 Node 2	2	12	8	80	12	0	Linux
	App 2 Node 1	3	32	10	80	32	50	Linux
	App 2 Node 2	4	32	10	80	32	50	Linux
	App 3 Node 1	3	16	6	80	16	0	Linux
	App 3 Node 2	4	16	6	80	16	0	Linux
	App 3 Node 3	1	16	6	80	16	0	Linux
	LB Tier 2 - Node 1	2	16	8	80	16	0	Linux
	LB Tier 2 - Node 2	3	16	8	80	16	0	Linux
	Analytics - node 1	4	96	14	80	96	3 000	Linux
	Analytics - node 2	1	96	14	80	96	3 000	Linux
	Analytics - node 3	2	96	14	80	96	3 000	Linux
Tier 3	Tier3 - node 1	3	16	8	80	16	23	Linux
	Tier3 - node 1	4	16	8	80	16		Linux

Table 12 – e-Gate Server Requirements – DR

10.5.1.5 **It is important to note that host affinity MUST be in place according to the tables above. The Host Affinity column in the above table indicates how VM's can be grouped/split Virtual Machines can be spread more than indicated. Each VM node to be deployed in different Host server.**

10.5.2 **CCTV**

10.5.2.1 The CCTV System utilises two server functions, a "Directory Server" and an "Archiver Server."

10.5.2.2 The JNB Site already has virtual machines for the CCTV system, but additional equipment is required, and the existing servers are not being utilised fully yet. Therefore, the Performance data in the Live Optic scans is not totally usable. The quantity in the table below includes the unused servers to allow for capacity.

10.5.2.3 **It is important to note that host affinity MUST be in place for the CCTV systems. A maximum of three archivers and two directory servers may be hosted on a single host.**

10.5.2.4 The Directory Server specification must be based on an existing server in the live optic scans, namely "**JNBVMCCTVDIR01**".

10.5.2.5 The Directory Server specification must be based on an existing server in the live optic scans, namely "**JNBVMCCTVARC01**".

10.5.2.6 Quantities per Site (total including existing deployed)

Site Name	Environment	System Name/Function	Qty	Description and Model	vCPUs	Memory (GB)	Disk (GB)	OS Type
JNB	Production	CCTV Directory Servers	7	Virtual Server	4	32	150	Windows Server 2019
KIM	Production	CCTV Directory Servers	1	Virtual Server	4	32	150	Windows Server 2019
BFN	Production	CCTV Directory Servers	1	Virtual Server	4	32	150	Windows Server 2019
CPT	Production	CCTV Directory Servers	8	Virtual Server	4	32	150	Windows Server 2019
GRJ	Production	CCTV Directory Servers	1	Virtual Server	4	32	150	Windows Server 2019
UTN	Production	CCTV Directory Servers	1	Virtual Server	4	32	150	Windows Server 2019
DUR	Production	CCTV Directory Servers	6	Virtual Server	4	32	150	Windows Server 2019
ELS	Production	CCTV Directory Servers	1	Virtual Server	4	32	150	Windows Server 2019
PLZ	Production	CCTV Directory Servers	1	Virtual Server	4	32	150	Windows Server 2019
JNB	Production	CCTV Archiver Servers	18	Virtual Server	4	16	97280	Windows Server 2016
KIM	Production	CCTV Archiver Servers	2	Virtual Server	4	16	97280	Windows Server 2016
BFN	Production	CCTV Archiver Servers	2	Virtual Server	4	16	97280	Windows Server 2016
CPT	Production	CCTV Archiver Servers	18	Virtual Server	4	16	97280	Windows Server 2016
GRJ	Production	CCTV Archiver Servers	2	Virtual Server	4	16	97280	Windows Server 2016
UTN	Production	CCTV Archiver Servers	2	Virtual Server	4	16	97280	Windows Server 2016
DUR	Production	CCTV Archiver Servers	12	Virtual Server	4	16	97280	Windows Server 2016
ELS	Production	CCTV Archiver Servers	2	Virtual Server	4	16	97280	Windows Server 2016
PLZ	Production	CCTV Archiver Servers	2	Virtual Server	4	16	97280	Windows Server 2016

Table 13 – CCTV Server Qty

10.5.3 JNB Baggage System

10.5.3.1 This is a new System, and no Virtual Machines have been created for it yet. The Specifications for the required Virtual Machines are included in the table below.

10.5.3.2 The system will be deployed at JNB.

10.5.3.3 Assume a constant 80%+ resource utilisation for the new Virtual Machines.

10.5.3.4 It is important to note that host affinity MUST be in place. The Host Affinity column in the above table indicates how VM's can be grouped/split. Virtual Machines can be spread more than indicated.

10.5.3.5 Storage must be able to deliver minimum of 3,500 IOPS per VM at average latency of 1-2 ms and minimum throughput of 1GB/s.

Site Name	Environment	System Name/Function	Qty	Host	Description and Model	vCPUs	Memory (GB)	Disk (GB)	OS Type
JNB	Production	SRV-CSC01	1	1	Virtual Server	4	8	332	Windows Server
JNB	Production	SRV-CSC02	1	2	Virtual Server	4	8	372	Windows Server
JNB	Production	SRV-CSC03	1	3	Virtual Server	4	8	330	Windows Server
JNB	Production	SRV-CSC04	1	4	Virtual Server	4	8	330	Windows Server
JNB	Production	SRV-CSC05	1	5	Virtual Server	4	8	330	Windows Server
JNB	Production	SRV-CIS01	1	4	Virtual Server	4	12	560	Windows Server
JNB	Production	SRV-SAC01	1	1	Virtual Server	4	12	330	Windows Server
JNB	Production	SRV-SCA01	1	2	Virtual Server	4	12	280	Windows Server
JNB	Production	SRV-DOM1	1	3	Virtual Server	2	8	110	Windows Server
JNB	Production	SRV-DOM2	1	4	Virtual Server	2	8	110	Windows Server
JNB	Production	WKS-BIGBEN	1	2	Virtual Server	2	8	120	Windows Server
JNB	Production	WKS-Siemens PC S7	1	5	Virtual Server	2	4	120	Windows Server

Table 14 – JNB Baggage Server requirements

10.5.3.6 It is important to note that host affinity MUST be in place. The Host Affinity column in the above table indicates how VM's can be grouped/split. Virtual Machines can be spread more than indicated.

10.5.4 **Parking Management**

10.5.4.1 Assume a constant 80%+ resource utilisation for the new Virtual Machines.

Site Name	Environment	System Name/Function	HOST	Qty	Description and Model	vCPUs	Memory (GB)	Disk (GB)	OS Type
JNB	Production	JMS Server1	1	1	Virtual Server	8	64	840	Windows Server
JNB	DR	JMS Server2	2	1	Virtual Server	8	64	840	Windows Server
JNB	Production	LPR Server	3	1	Virtual Server	8	64	36100	Windows Server
CPT	Production	JMS Server1	1	1	Virtual Server	8	64	840	Windows Server
CPT	DR	JMS Server2	2	1	Virtual Server	8	64	840	Windows Server
CPT	Production	LPR Server	2	1	Virtual Server	8	64	36100	Windows Server
CPT	Production	LPR Server	3	1	Virtual Server	8	64	36100	Windows Server
CPT	Production	VMS Server	1	1	Virtual Server	4	32	800	Windows Server
CPT	Production	Voice Recorder Server	2	1	Virtual Server	4	16	1024	Windows Server
DUR	Production	JMS Server1	1	1	Virtual Server	8	64	840	Windows Server
DUR	DR	JMS Server2	2	1	Virtual Server	8	64	840	Windows Server
PLZ	Production	JMS Server	1	2	Virtual Server	4	32	840	Windows Server
GRJ	Production	JMS Server	1	2	Virtual Server	4	32	840	Windows Server
KIM	Production	JMS Server	1	2	Virtual Server	4	32	840	Windows Server
ELS	Production	JMS Server	1	2	Virtual Server	4	32	840	Windows Server
BFN	Production	JMS Server	1	2	Virtual Server	4	32	840	Windows Server
UTN	Production	JMS Server	1	2	Virtual Server	4	32	840	Windows Server

Table 15 – Parking management Server requirements

10.5.4.2 It is important to note that host affinity MUST be in place. The Host Affinity column in the above table indicates how VM's can be grouped/split. Virtual Machines can be spread more than indicated.

10.5.5 **SharePoint 2019**

10.5.5.1 Assume a constant 80%+ resource utilisation for the new Virtual Machines.

Site Name	Environment	System Name/Function	Host	Qty	Description and Model	vCPUs	Memory (GB)	Disk (GB)	OS Type
JNB	Production	SP Internet	1	1	App Server	8	32	300	Windows Server 2022
JNB	Production	SP Intranet	2	1	App Server	8	32	300	Windows Server 2022
JNB	Production	SP Internet	3	1	Web Front End Server	8	32	300	Windows Server 2022
JNB	Production	SP Intranet	4	1	Web Front End Server	8	32	300	Windows Server 2022
JNB	DEV	SP DEV	1	1	App Server	8	32	300	Windows Server 2022
JNB	Production	SQL	3	1	SQL Server	32	128	3450	Windows Server 2022
JNB	Production	SQL	4	1	SQL Server	32	128	3450	Windows Server 2022
JNB	DEV	SQL DEV	1	1	SQL Server	32	128	2450	Windows Server 2022
JNB	QA	SQL QA	2	1	SQL Server	32	128	2450	Windows Server 2022
JNB	DEV & QA	SP Intranet	3	1	App Server	8	32	900	Windows Server 2022
JNB	DEV & QA	SP Intranet	4	1	Web Server	8	32	700	Windows Server 2022
JNB	Production	SP Intranet	1	1	App Server	8	32	900	Windows Server 2022
JNB	Production	SP Intranet	2	1	App Server	8	32	900	Windows Server 2022
JNB	Production	SP Intranet	3	1	Web Server	8	32	700	Windows Server 2022
JNB	Production	SP Intranet	4	1	Web Server	8	32	700	Windows Server 2022
JNB	Production	SP Intranet	5	1	Office Web Apps Server	8	32	700	Windows Server 2022
JNB	Production	SP Intranet	6	1	Workflow Server	8	32	700	Windows Server 2022
JNB	Production	SP Intranet	5	1	Distributed Cache Server	8	32	700	Windows Server 2022
JNB	DEV & QA	SP Internet	3	1	App Server	8	32	900	Windows Server 2022
JNB	DEV & QA	SP Internet	2	1	Web Server	8	32	700	Windows Server 2022
JNB	Production	SP Internet	4	1	App Server	8	32	900	Windows Server 2022
JNB	Production	SP Internet	5	1	App Server	8	32	900	Windows Server 2022
JNB	Production	SP Internet	6	1	Web Server	8	32	700	Windows Server 2022
JNB	Production	SP Internet	1	1	Web Server	8	32	700	Windows Server 2022

Table 16 – SharePoint Server requirements

10.5.5.2 It is important to note that host affinity MUST be in place. The Host Affinity column in the above table indicates how VM's can be grouped/split. Virtual Machines can be spread more than indicated.

10.5.6 **Oracle Business Intelligence Enterprise Edition (OBIEE)**

10.5.6.1 Assume a constant 80%+ resource utilisation for the new Virtual Machines.

Site Name	Environment	System Name/Function	Qty	Description and Model	vCPUs	Memory (GB)	Disk (GB)	OS Type
JNB	Production	JMS	1	JMS Server	8	64	840	Windows Server 2022
JNB	Production	OBIEE	1	App Server	8	32	1000	Linux 8
JNB	Production	OBIEE DB Server	1	DB App Server	8	32	2500	Linux 8

Table 17 - Oracle Business Intelligence Enterprise Edition (OBIEE) Server requirements

10.5.7 **Oracle E-Business Suite (OEBS)**

10.5.7.1 Assume a constant 80%+ resource utilisation for the new Virtual Machines.

Site Name	Environment	System Name/Function	Qty	Description and Model	vCPUs	Memory (GB)	Disk (GB)	OS Type
CPT	DR	Oracle Database Server	1	Virtual Server	28	32	4000	Linux 8
CPT	DR	Oracle Database Server	1	Virtual Server	28	32	3000	Linux 8
CPT	DR	Oracle Database Server	1	Virtual Server	28	32	100	Linux 8
CPT	DR	Oracle Database Server	1	Virtual Server	28	32	200	Linux 8
CPT	DR	Oracle Database Server	1	Virtual Server	28	32	3000	Linux 8
CPT	DR	Oracle Application Server	1	Virtual Server	28	32	1000	Linux 8
CPT	DR	Oracle Application Server	1	Virtual Server	28	32	750	Linux 8

Table 18 – 10.5.8 Oracle E-Business Suite (OEBS) Server Requirements

10.5.8 **Enterprise Services Bus (ESB)**

10.5.8.1 Assume a constant 80%+ resource utilisation for the new Virtual Machines.

Site Name	Environment	System Name/Function	Qty	Description and Model	vCPUs	Memory (GB)	Disk (GB)	OS Type
JNB	Production	Prod ESB	1	Virtual Server	5	32	300	Linux 8
JNB	Production	Pre Prod ESB	1	Virtual Server	2	32	300	Linux 8
JNB	Production	DEV ESB	1	Virtual Server	2	32	300	Linux 8
JNB	Production	DB Prod Server	1	Virtual Server	20	32	300	Linux 8
JNB	DEV	DB Pre Prod	1	Virtual Server	20	32	300	Linux 8
JNB	Production	DB Dev Server	1	Virtual Server	10	32	3450	Linux 8

Table 19 – 10.5.8 Enterprise Services Bus (ESB)Server Requirements

10.5.9 **SQL Cluster**

10.5.9.1 Assume a constant 80%+ resource utilisation for the new Virtual Machines.

Site Name	Environment	System Name/Function	Host	Qty	Description and Model	CPUs	Memory (GB)	Disk (GB)	OS Type
JNB	Production	Shared SQL Cluster Node 1	1	1	Virtual Server	4	128	2 000	Windows Server
JNB	Production	Shared SQL Cluster Node 2	2	1	Virtual Server	4	128	2 000	Windows Server
JNB	Production	Shared SQL Cluster Node 3	3	1	Virtual Server	4	128	2 500	Windows Server
JNB	Production	Shared SQL Cluster Node 4	4	1	Virtual Server	4	128	2 500	Windows Server
JNB	Production	SharePoint SQL Cluster Node 1	2	1	Virtual Server	4	128	20 000	Windows Server
JNB	Production	SharePoint SQL Cluster Node 2	3	1	Virtual Server	4	128	20 000	Windows Server
JNB	Pre-Production	SharePoint SQL Cluster Node 1	4	1	Virtual Server	2	24	450	Windows Server
JNB	Pre-Production	SharePoint SQL Cluster Node 2	5	1	Virtual Server	2	24	450	Windows Server
CPT	Production	Shared SQL Cluster Node 1	1	1	Virtual Server	4	128	1000	Windows Server
CPT	Production	Shared SQL Cluster Node 2	2	1	Virtual Server	4	128	1000	Windows Server
DUR	Production	Shared SQL Cluster Node 1	1	1	Virtual Server	4	128	1000	Windows Server
DUR	Production	Shared SQL Cluster Node 2	2	1	Virtual Server	4	128	1000	Windows Server

Table 20 – 10.5.8 SQL Cluster Hardware Server Requirements

10.5.9.2 It is important to note that host affinity MUST be in place. The Host Affinity column in the above table indicates how VM's can be grouped/split. Virtual Machines can be spread more than indicated.

10.5.10 **IBM Hardware**

Site Name	Environment	System Name/Function	Qty	Description and Model	vCPUs	Memory (GB)	Disk (GB)	OS Type	Serial Number
JNB	Production	MQ Hardware Appliance	1	IBM MQ Appliance M2001	N.A.	N.A.	N.A.	N.A.	7803517
JNB	Production	MQ Hardware Appliance	1	IBM MQ Appliance M2002	N.A.	N.A.	N.A.	N.A.	7804383
JNB	Production	DP Hardware Appliance	1	DataPower Appliance	N.A.	N.A.	N.A.	N.A.	7800112
JNB	Production	DP Hardware Appliance	1	DataPower Appliance	N.A.	N.A.	N.A.	N.A.	7800201
CTIA	Production	DP Hardware Appliance	1	DataPower Appliance	N.A.	N.A.	N.A.	N.A.	7801710
CTIA	Production	IBM Power System	1	Power 8 S824	16	512		N.A.	2138ACW
JNB	Production	IBM Power System	1	Power 8 870C	32	2048		N.A.	78FAE17
JNB	Production	IBM Power System	1	Power 8 870C	32	2048		N.A.	78FAE27
JNB	Production	IBM HMC	1	Hardware Management Console	N.A.	N.A.	N.A.	N.A.	786EBAD
JNB	Production	IBM HMC	1	Hardware Management Console	N.A.		N.A.	N.A.	786EB9D
CTIA	Production	IBM HMC	1	Hardware Management Console	N.A.	N.A.	N.A.	N.A.	212A2ED
JNB	Production	Hardware Appliance	1	IBM MQ Appliance M2003B	N.A.	N.A.	N.A.	N.A.	7801645
JNB	Production	Hardware Appliance	1	IBM MQ Appliance M2003B	N.A.	N.A.	N.A.	N.A.	7801648
JNB	Production	Hardware Appliance	1	IBM DataPower Gateway X3 Appliance	N.A.	N.A.	N.A.	N.A.	7801847
JNB	Production	Hardware Appliance	1	IBM DataPower Gateway X3 Appliance	N.A.	N.A.	N.A.	N.A.	7801861
CTIA	Production	Hardware Appliance	1	IBM DataPower Gateway X3 Appliance	N.A.	N.A.	N.A.	N.A.	7801862

Table 21 – 10.5.8 IBM Hardware Server Requirements

10.5.11 **General Supply**

10.5.11.1 During the execution of the contract there might be a requirement to increase capacity even further over and above the included 20% spare capacity.

10.5.11.2 Include the cost for a Standard host in the various clusters in the pricing file

10.5.11.3 Include the cost of the highest specification Physical server in the pricing file

10.5.12 **Other information**

10.5.12.1 Additional Spare capacity of **>=20%** must be incorporated for growth across the full cluster at each site this is for ALL resources.

10.5.12.2 Physical Servers included in the LiveOptics Scan will be virtualised and should be included in the capacity for the clusters.

10.5.12.3 **Please take note that in some tables there is a quantity column, and the resources required should be multiplied by that quantity.**

10.5.12.4 SQL servers will be virtualised on this platform in a Microsoft failover cluster configuration. None of the SQL servers to be virtualised are in high-performance clusters; therefore, no special consideration should be taken.

10.5.12.5 A Conceptual diagram of the envisaged implementation of the clusters is depicted in the figure below.

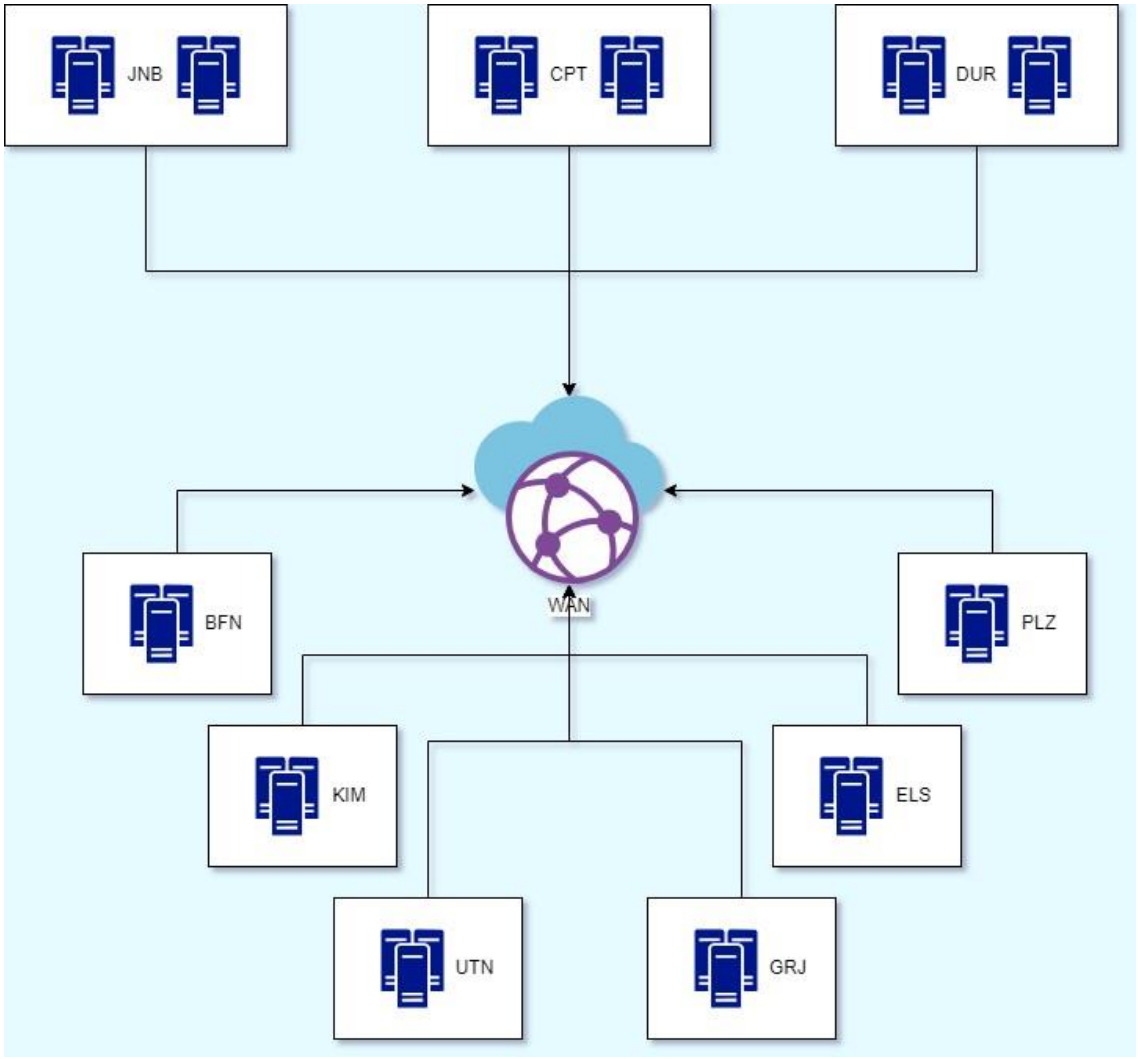


Figure 1 – Conceptual cluster diagram.

10.6 Migration

10.6.1 All migration services must be included in this submission.

10.6.2 Migration can be in multiple formats, for example.

- Inter-cluster movement.
- Export and import.
- Pysical2Virtual import.
- Virtual2Virtual import
- Complete reinstallation of the VM (OS only included in this SOW)

10.6.3 Migration via complete reinstallation will involve some 3rd parties to install the application and migrate data. Third-party migration tasks are to be included in the project schedule for dependency tracking. But will only be known at project start. Costing for this is outside of this SOW.

10.6.4 Most migrations will involve changing IP addresses.

10.6.5 Migration must be completed within 12 months of starting the 1st migration task.

10.6.6 Delays due to ACSA or its 3rd party contractors not to impact SLA, any delays must be communicated timeously.

10.6.7 Note that virtual machines from the regional sites must be migrated to the central site it is allocated to (where applicable), and therefore the central site should have enough capacity for this.

10.7 Decommissioning and disposal

10.7.1 All old equipment replaced by this proposal must be decommissioned (removed from racks), and equipment must be disposed of in an environmentally safe and friendly way.

10.7.2 All disks must be cleansed of all data using the minimum standard DoD 5220.2-m.

10.7.3 Any ACSA branding/references/stickers and asset tags must be removed from decommissioned equipment before being removed from the site.

10.7.4 Certificates must be provided for all data cleansing and disposal.

10.7.5 An electronic asset list of all decommissioned and disposed of equipment must be provided by the Provider.

10.7.6 No storage space will be provided for any equipment.

10.7.7 Any potential “buy-back” must be indicated in the proposal, but not to be factored into any costing

10.8 **Licencing**

10.8.1 Although VMware is active in the environment, it is currently covering the existing installation; therefore, it cannot be factored into the proposal as usable licences should this be the virtualisation solution proposed.

10.8.2 It should be noted that ACSA already owns 465 Core licences for Windows DataCenter, and it can be assumed that these are available to be used against the AZURE hybrid benefit. The cost of any additional licences must be included for evaluation purposes, but the procurement of these licences will be done via ACSA's existing Microsoft agreement.

10.9 **Cabling**

10.9.1 The provision and installation of all cabling requirements must be included in the pricing.

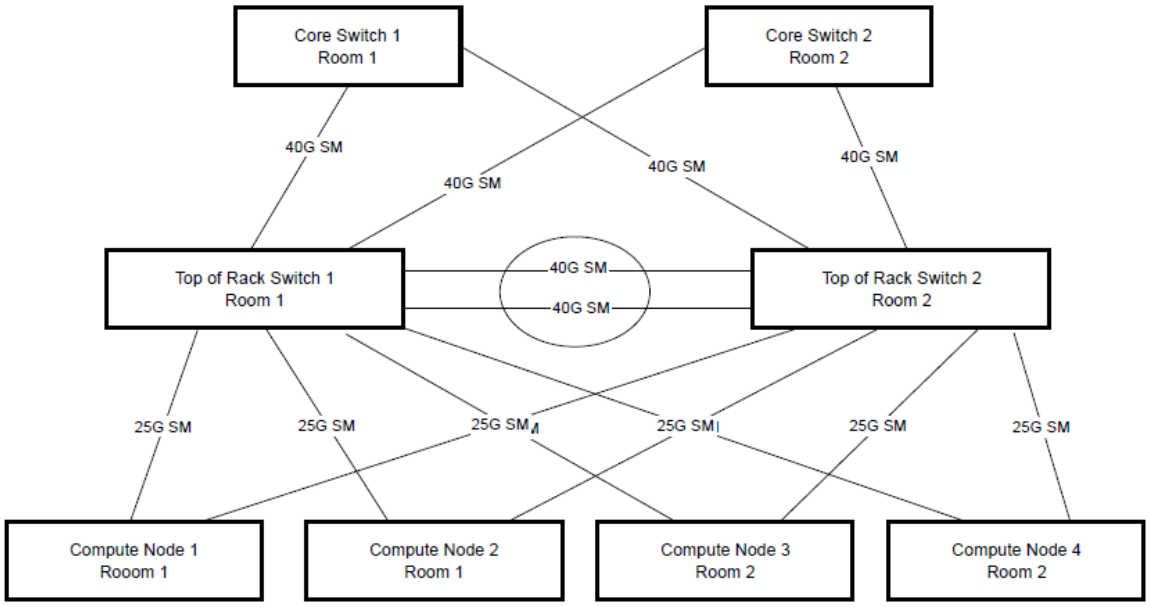
10.9.2 **Any maintenance requirements for cabling must be transferred to the current IT Physical infrastructure vendor.**

10.9.3 Typical network connectivity (therefore fibre requirements) is depicted in the figures below (host counts are not a true reflection per site; it is just used for illustration)

10.9.4 Subcontracting for cabling is allowed, should the Service provider not have the required certifications as required in the evaluation criteria.

10.9.5 All cabling installations to conform to ACSA physical infrastructure standards. (Please refer to Appendix E)

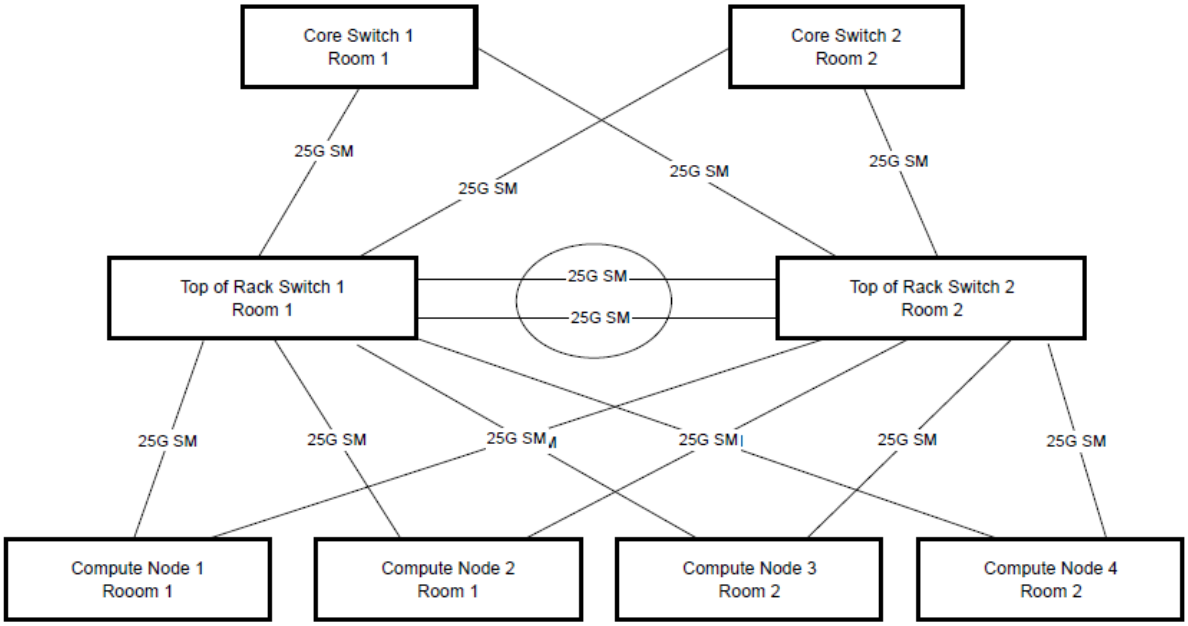
10.9.6 **As mentioned, ACSA reserves the right not to execute the cabling scope**



COMPUTE FIBRE REQUIREMENT @ JNB

Devices shown are split across 2 rooms. Compute node quantities may vary

Figure 2 – Fibre reticulation for JNB



COMPUTE FIBRE REQUIREMENT @ ELS, CPT and DUR

Devices shown are split across 2 rooms. Compute node quantities may vary

Figure 3 – Fibre reticulation for DUR,ELS,CPT and PLZ

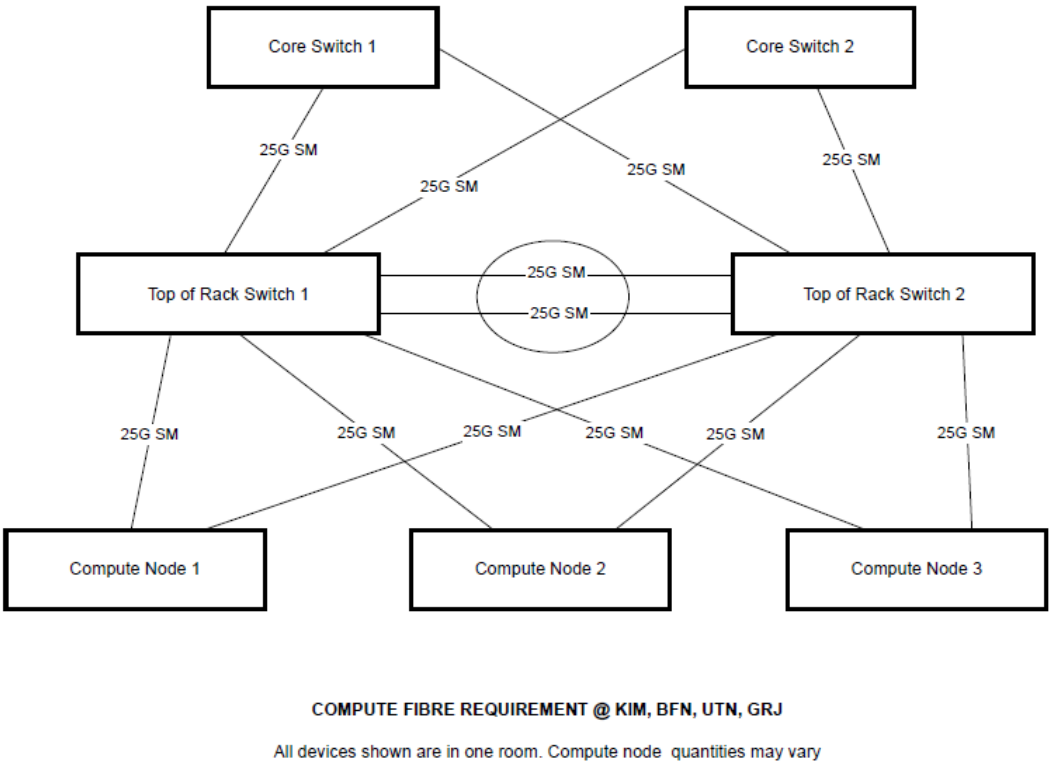


Figure 4 – Fibre reticulation for Regionals

10.10 Network Connectivity

10.10.1 The provision and installation of all networking requirements must be included in the pricing.

10.10.2 **Any maintenance requirements for Networking must be transferred to the current IT Network infrastructure vendor.**

10.10.3 Network connectivity must be provided by dedicated “Top of Rack switches”

10.10.4 Network connectivity to the Nodes must be 25 Gbit for all sites.

10.10.5 Network connectivity between the top-of-rack switches must be 25 Gbit for all sites except JNB which should be 100 Gbit.

10.10.6 **As mentioned, ACSA reserves the right not to execute the Network scope**

10.10.7 Typical network connectivity (therefore fibre requirements) is depicted in the figures below (host counts are not a true reflection per site; it is just used for illustration)

10.10.8 Subcontracting for Networking is allowed, should the Service provider not have the required certifications as required in the evaluation criteria.

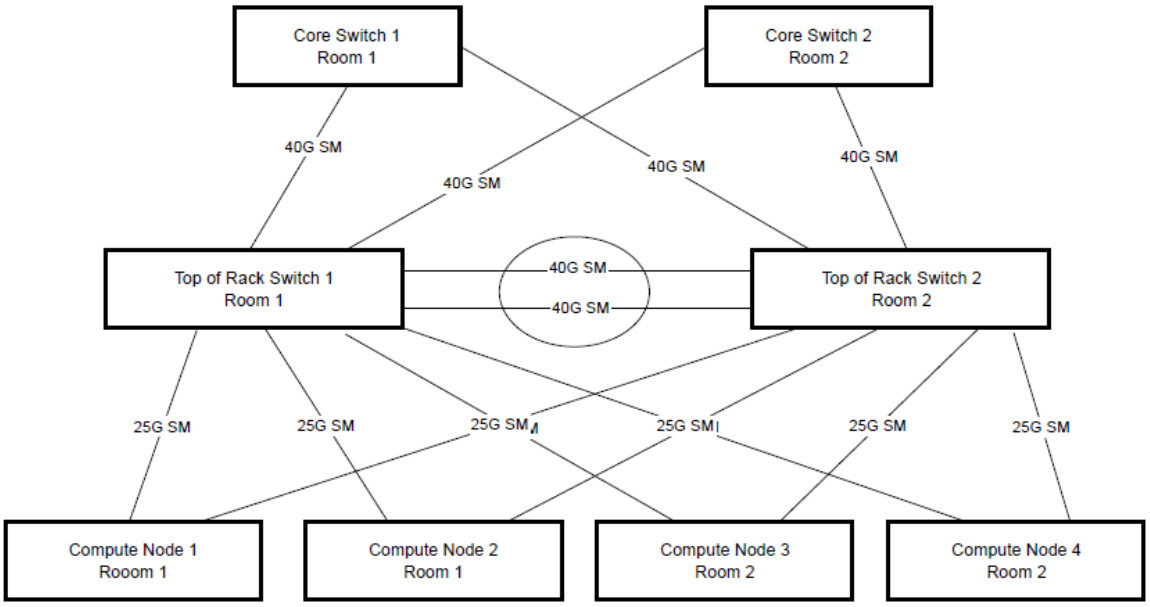


Figure 5 – Fibre reticulation for JNB

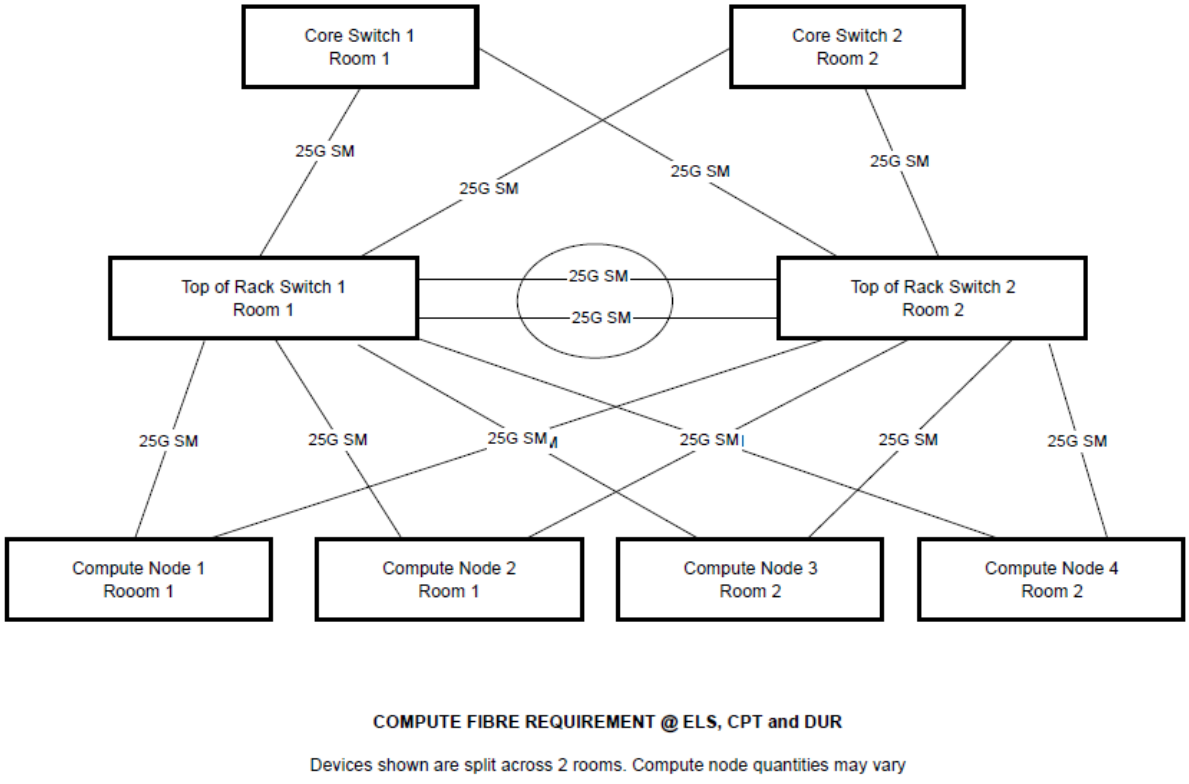
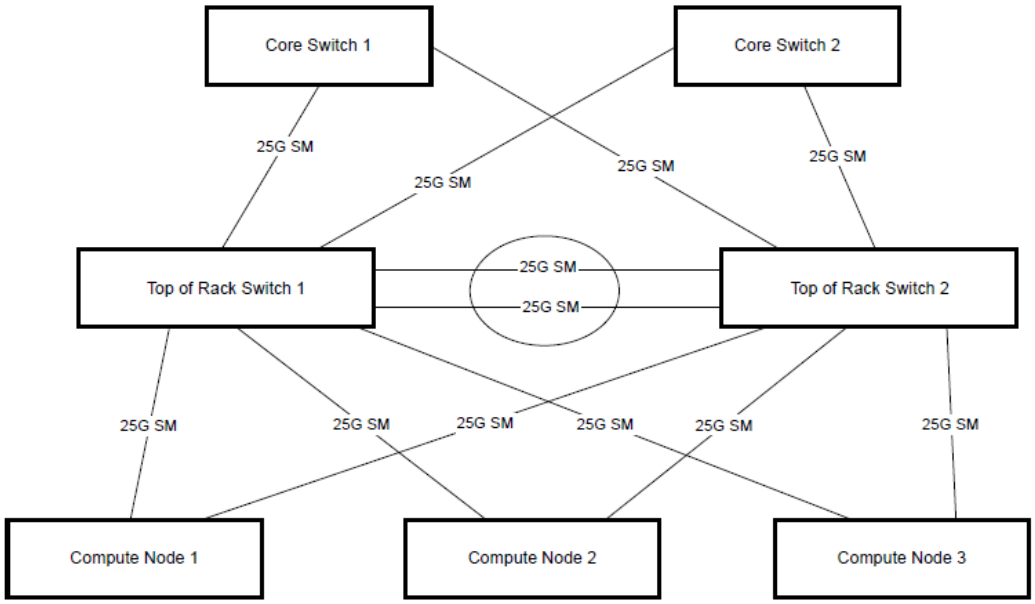


Figure 6 – Fibre reticulation for DUR,ELS,CPT and PLZ



COMPUTE FIBRE REQUIREMENT @ KIM, BFN, UTN, GRJ

All devices shown are in one room. Compute node quantities may vary

11.0 Out of Scope

The following items are exclusively excluded from the scope of work:

11.1 Provisioning of the network equipment

11.2 Cooling and Power Infrastructure within the IT Facilities

13.0 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	An 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	An individual with final accountability for the results of a sourcing activity. Accountability includes a mandate to dismiss or accept the results by activity as realised 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 realising the sourcing activity. They actively participate in realising/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 realising/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. Consulting is a reactive role.
I	Informed	Individuals who need to be informed but have no role in the realisation/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 22 - Definition of RASCI Model

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

13.1 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

Sub area	Number	Task/Activity	provider	ACSA
	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.	Ensure that support staff is capable of supporting infrastructure that is located at above normal height, such as indoor Access Points or external Access Points located on Airside. Support staff must have the relevant safety certifications, protective wear and equipment to carry out corrective maintenance duties.	R, A	C, I
	17.	Ensure that the provider has a valid health and safety file at all times	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 23 - Roles and Responsibilities – General

13.2 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	R,A	C,S,I

Sub area	Number	Task/Activity	provider	ACSA
		post the meeting as required such as requirements gathering activities; solution design options)		
	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. (including but not limited to upgrade requirements, conversion requirements, design schematics, WC/CR/DC floor plans, design diagrams). 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
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	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

Sub area	Number	Task/Activity	provider	ACSA
	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.	Participate in in-scope IT-Commercial initiatives as requested ACSA-IT – this includes understanding the required solution and outcome, provide solution design and architecture documentation relating to this service towner	C,I	R,A
	26.	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
	27.	Review the latest technologies presented by the Service provider.	C,I	R,A
	28.	Request provider to participate in in-scope IT-Commercial initiatives.	C,I	R,A
Design and panning	29.	Develop, document and maintain detailed technical design/engineering plans and environment configuration based on ACSA's business requirements	R,A	C,I
	30.	Provide design documentation for quarterly audits as requested by ACSA	R,A	C,I
	31.	Provide input into design plans through coordination with the appropriate ACSA technology standards groups and design architects	C,I,S	R,A
	32.	Quarterly audit of design documentation	C,I,S	R,A
	33.	Adhere to production acceptance test criteria	R,A	C,I
	34.	Conduct and document test plans and results	R,A	C,I
	35.	Define and document production acceptance test criteria	C,I	R,A
	36.	Review and approve test plans and results	C,I	R,A

Table 24 - Roles and Responsibilities - Management, Planning and design

13.3 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
Project Management 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 risks etc. for action to higher governance authorities as required	C,I	R,A

Table 25 - Roles and Responsibilities - Project Management Services

13.4 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, Proc	1.	When procurement is requested by ACSA-IT, provider to adhere to acquisition/procurement policies	R,A	C,I

Sub area	Number	Task/Activity	provider	ACSA
	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
	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 insure 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

Sub area	Number	Task/Activity	provider	ACSA
	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 26 - Roles and Responsibilities - Acquisition and Management

13.5 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 in scope 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 infrastructure (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 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 document 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	R,A	C,I

Sub area	Number	Task/Activity	provider	ACSA
		reporting in a form/format that is acceptable to ACSA for Service Projects and major Service activities		
	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 27 - Roles and Responsibilities - Documentation

13.6 Roles and Responsibilities - Technology Refresh and Replenishment

Technology Refreshment and Replenishment (TR&R) Services are the activities associated with modernising 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 28 - Roles and Responsibilities - Technology Refresh and Replenishment

13.7 Roles and Responsibilities - Infrastructure Build and Change

Managing all 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 (including but not limited to, appliances, switches, fibre link etc. 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 (including but not limited to, appliances, switches, fibre link etc. 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
Changes	13.	Recommend changes to meet service requirements	R,A	C,I
	14.	Perform changes to meet business requirements (including but not limited to e.g., switch replacement, Ethernet and fibre modules etc.)	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

Sub area	Number	Task/Activity	provider	ACSA
	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 29 - Roles and Responsibilities - Infrastructure Build and Change

13.8 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 taken into account)	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	R, A	C, I

Sub area	Number	Task/Activity	provider	ACSA
		Service components, including hardware, software, peripherals and special-purpose devices as appropriate		
	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
	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. o Inspections and alerts investigations o Syslog analysis – Continuous monitoring and responding with corrective actions to warnings and alerts. o Health Checks o Configuration Backups o Log Analysis o Device performance monitoring for high memory and CPU utilization o Software upgrades on management systems o Capacity Management o User Management o Redundancy Testing o IOS and Firmware Upgrades o Fibre Connectivity Performance Testing	R,A	C,I

Sub area	Number	Task/Activity	provider	ACSA
		o Advise / recommend improvement for the 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		
	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 30 - Roles and Responsibilities – Maintenance

13.9 Roles and Responsibilities - Infrastructure Monitoring, Operations and Administration

Monitoring, Operations and Administration Services of all in scope infrastructure 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 Infrastructure will always be done in consultation with ACSA-IT Infrastructure 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 infrastructure that will meet the monitoring and service level reporting requirement	R,A	C,I
	2.	Implement measures for proactive monitoring to limit infrastructure outages.	R,A	C,I
	3.	Manage all in scope infrastructure elements in accordance with ACSA's policies (including security oversight and change management policies)	R,A	C,I
	4.	Manage and coordinate provider 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
	6.	Install, customise and maintain the infrastructure management system for event monitoring and availability reporting.	I	R,A
	7.	Implement measures for proactive monitoring to limit infrastructure outages	I	R,A

Table 31 - Roles and Responsibilities - Infrastructure Monitoring, Operations and Administration

13.10 **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 IT 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 IT 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 of IT Infrastructure systems and components. The goal of the Availability Management process is to optimize the capability of the IT 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 unit availability requirements for a new or enhanced IT Service and formulating the availability and recovery design criteria for the IT 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 IT Infrastructure to deliver cost-effective improvements that deliver tangible business benefits

- Supporting the targets for availability, reliability and maintainability for the IT 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 IT availability 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 IT availability improvements aimed at improving the overall availability of IT Services and Infrastructure components to ensure that existing and future business availability requirements can be met

- Providing IT availability 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 infrastructure design	R, A	I
	10.	Participate in creating availability and recovery design criteria to be applied to upgrades and/or new IT Infrastructure system 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 IT 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 IT 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	R, A	I

Sub area	Number	Task/Activity	provider	ACSA
		optimization, and periodically provide updates to ACSA IT management		
	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.	Coordinate and take ownership of Availability Management across all IT service areas within ACSA and Third-Party Service Vendors (e.g., public carriers, Internet service providers, Third-Party providers, etc.)	R, A	I
	20.	Participate in Problem Management review sessions as appropriate, specifically those problems related to outages of critical systems	R, A	C, I
	21.	Monitor actual IT availability achieved versus targets and ensure shortfalls are addressed promptly and effectively	R, A	I
	22.	Conduct Availability Assessment review sessions and provide cost-justified improvement recommendations	R, A	I
	23.	Participate in availability improvement review sessions	I	R, A
	24.	Review and approve cost-justifiable improvement recommendations that ACSA deems appropriate to enhance ACSA IT and business performance needs	I	R, A
	25.	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
	26.	reduce and maintain an Availability Plan that prioritizes and plans approved IT availability improvements	R, A	I
	27.	Review and approve Availability Plan	I	R, A
	28.	Provide IT availability reporting to ensure that agreed levels of availability, reliability and maintainability are measured, reported and monitored on an ongoing basis	R, A	I
	29.	Promote Availability Management awareness and understanding within all IT support organizations, including Third-Party Service Vendors	R, A	I
	30.	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
	31.	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 32 - Roles and Responsibilities - Project Management Services

13.11 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
	6.	Define, develop and implement tools that allow for the effective capacity monitoring/trending of IT 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 infrastructure components	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, taking into account daily, weekly and seasonal variations in capacity demands	R, A	I
	20.	Validate asset utilization and capital efficiency	I	R, A

Table 33 - Roles and Responsibilities - Capacity Management

13.12 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
	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 34 - Roles and Responsibilities - Performance Management

13.13 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 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
	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 35 - Roles and Responsibilities - Configuration Management

13.14 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
	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

Sub area	Number	Task/Activity	provider	ACSA
	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 36 - Roles and Responsibilities - Asset Management

13.15 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
	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

Sub area	Number	Task/Activity	provider	ACSA
	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 37 - Roles and Responsibilities - Software License Management

13.16 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

Sub area	Number	Task/Activity	provider	ACSA
	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 38 - Roles and Responsibilities - Change Management

13.17 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

Sub area	Number	Task/Activity	provider	ACSA
	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 39 - Roles and Responsibilities - Training and Knowledge Transfer

13.18 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

Sub area	Number	Task/Activity	provider	ACSA
	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 40 - Roles and Responsibilities - Account Management

13.19 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 Infrastructure, 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]	R, A	I,C

Sub area	Number	Task/Activity	provider	ACSA
		• 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.		
	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 41 - Roles and Responsibilities - Incident Resolution and Problem Management

13.20 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 ACSA applications, and their associated infrastructure (e.g., CPU, servers, network, data and output devices, End-User devices). ACSA 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 42 - Roles and Responsibilities - IT Service Continuity and Disaster Recovery

13.21 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
	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 43 - Roles and Responsibilities - Service-Level Monitoring and Reporting

13.22 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 44 - Roles and Responsibilities - Financial Management

13.23 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	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

Sub area	Number	Task/Activity	provider	ACSA
	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 45 - Roles and Responsibilities - Human Resources

13.24 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 IT Infrastructure

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

Sub area	Number	Task/Activity	provider	ACSA
	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 Access Management	20.	Provide Identity and Access Management in conformance with ACSA practices, policies and procedures	R, A	I
	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 infrastructure	R, A	I

Sub area	Number	Task/Activity	provider	ACSA
	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
Security Configuration 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 ACSAs 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
	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. This is something	R, A	I

Sub area	Number	Task/Activity	provider	ACSA
	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 46 - Roles and Responsibilities - Security

14.0 SERVICE MANAGEMENT

14.1 Objectives

14.1.1 A key objective of this Managed Service agreement is to attain SLRs.

14.1.2 SLRs applicable are identified in this Service Management SOW below.

14.1.3 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 15.0 SERVICE CREDITS.

14.1.4 provider shall provide written reports to Technical Operations Manager: Datacentre and Storage regarding provider's compliance with the SLRs specified.

14.2 Reports

14.2.1 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.

14.2.2 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.

14.3 Root cause analysis

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

14.4 Support services

14.4.1 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.

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

14.4.3 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.

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

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

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

14.5 SERVICE-LEVEL REQUIREMENTS (SLRs)

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

14.5.1 Review of Service Levels and KPIS

14.5.1.1 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.

14.5.1.2 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 Priority levels

14.5.2 **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 infrastructure 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. Examples: • Blade Enclosure Failure, • IBM Failure • Virtual Host Failure • Critical Server Failure • Critical Service Failure
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. Examples: • Blade enclosure redundancy failure • Redundant part failure • Service reduction of availability,
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. Examples: • Noncritical server not available • Noncritical redundant part failure • Service not available for small non-operational application
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. Example: • Service available but slow response
Priority Level 5 — Low Impact that will take a week or two to resolve	Any services or equipment that has a low impact that will require a week or two to fix

Table 47 – Priority Levels

14.5.3 **Incident management**

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

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

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

Table 48 - Incident Response and Resolution time (Operational Hours)

Incident management response and resolution times for International Airports (Outside Operational Hours) and regional airports operational 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	<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	
	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 49 - Incident Response and Resolution time International Airports (outside of operational hours) and Regional airports (Operational Hours)

14.5.4 **Resource Availability**

Resource 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: DI = Total "downtime" hours AI = Adjusted downtime hours based on exceptions H = Hours in the month (adjusted according to resource type and availability requirements) OI = Total number of resources per type EI = Expected availability = H x OI Report Only: **Availability %** = (EI — DI)/EI x 100 SLA: **Adjusted Availability** % = (EI — AI)/EI x 100
SLR Element Weighting Factor Allocation	30%

Table 50 Resource availability SLR

14.5.5 **Requests**

System Administration Service-Level Requirements			
	Service Measure	**Performance Target**	**SLR Performance %**
Advise Client of need to allocate additional processing resources based on predefined parameters and observed growth patterns	Proactive monitoring and reporting to Client of need to increase capacity	Sustained average daily CPU utilisation approaches 80% of installed processor capacity—Inform Client within 1 Business Day	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	ACSA Service Desk Stats/ Provider request schedule	
	SLR Element Weighting Factor Allocation	20%	

Table 51 Service requests SLR

14.5.6 **IMACDs**

14.5.6.1 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.

14.5.6.2 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 52 IMACD SLR

14.5.7 **Asset management**

14.5.7.1 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.

14.5.7.2 Historic information may not be available, and exclusion of certain data elements will be granted at the discretion of ACSA

Asset Tracking SLR			
	Service Measure	**Performance Target**	**SLR Performance %**
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 (Wirecenter, position in Cabinet, Room tag number, Site)	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 53 Asset Tracking SLR

14.5.8 Configuration management

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

14.5.8.2 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 Configuration management Tools
SLR Element Weighting Factor Allocation	30%

Table 54 Configuration Management SLR

14.5.9 Overall service satisfaction

14.5.9.1 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			
	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	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 55 Overall satisfaction SLR

14.5.10 Software/Firmware Refresh

Software refresh for all upgrades and new releases.

Software /firmware Refresh Service-Level Requirements			
	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 or to be agreed time by ACSA	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	
	SLR Element Weighting Factor Allocation	30%	

Table 56 Software/Firmware Refresh SLR

14.5.11 Resource Certifications and experience

Resource Availability SLR	
Component	**Explanation of Component**
Definition	Based on the minimum certified resources and years' experience as per the tender evaluation
Coverage	As per tender evaluation
Measurement Range	98%
Frequency	Monthly
Measurement Tool	Copy of response sheet as in tender, together with a summarised report
Calculation Formula	As per tender evaluation sheet/
SLR Element Weighting Factor Allocation	30%

Table 57 Resource Certifications and experience SLR

14.5.12 **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 58 SLA Measurement Exclusions

15.0 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 recognising 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.

15.1 **Principles**

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

15.1.1 Service Credits only occur because of Service Level Failures.

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

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

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

15.1.5 A good performance on an SLR cannot compensate for a bad performance on another one.

15.1.6 The SLRs that are considered 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.

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

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

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

15.1.10 The provider will be allowed a grace period of 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

15.2 **Definitions**

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

15.2.2 **At Risk Amount -** means, for any month during the Term, fifty percent (50%) of the monthly fixed Service Fees per ACSA Site.

15.2.3 **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.

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

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

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

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

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

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

15.3 **Methodology**

15.3.1 **Monitoring; reports; root cause analysis.**

15.3.1.1 **Monitoring**

The Service provider shall utilise ACSA measurement and monitoring tools and produce the metrics and reports necessary to measure its performance against the Service Levels.

Additional Tools may be implemented by the provider at its own cost should the ACSA tools not be enough.

Upon request and at no additional charge to ACSA, the Service provider shall provide ACSA or its designees with information and access to the tools and procedures used to produce such metrics.

15.3.1.2 **Reports**

The Service provider shall report to ACSA its performance of the Services against each SLR every month 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.

15.3.1.3 **Root cause analysis**

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

15.3.2 **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.

15.3.3 **Service breach**

If a Service Level Failure 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 the Agreement.

15.3.4 **Several service level failures**

Subject to Section 15.3.5If 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.

15.3.5 **Successive service level failures**

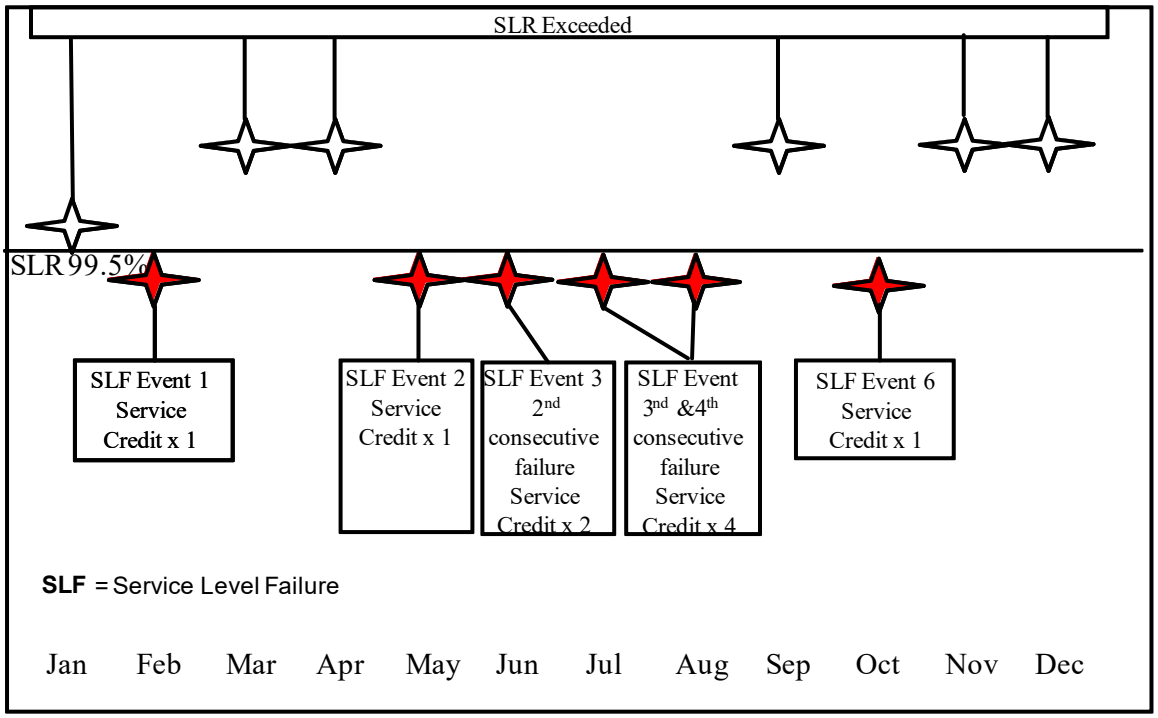
If a Service Level Failure with respect to a given Service Level recurs in consecutive Measurement Intervals, the amount of the applicable Service Credit payable to ACSA shall be multiplied by the following factors for subsequent Measurement Intervals:

(i) Service Level Failure in two consecutive Measurement Intervals, then **twice (x2)** the amount of the Performance Credit as originally calculated; and

(ii) Service Level Failure in three or more consecutive Measurement Intervals, then **four times (x4)** 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



15.3.6 **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.

15.3.7 **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 each 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.

15.3.8 **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 instead of any other rights and remedies ACSA has under the Agreement, at law or in equity.

15.3.9 **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 periods.

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.

15.4 Changes to performance measurements

15.4.1 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.

15.4.2 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.

15.4.3 Deletions

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

16.0 Meetings and Report Requirements

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

16.1.1 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

16.1.2 **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

16.1.3 **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 Name and frequency	Participants and roles	Documents to be produced after meeting by Service provider
Weekly Service Review	· ACSA-IT Engineer (chair) · Provider Senior Site Manager · Provider administrator	· Minutes of meeting · Running Action register for any open actions to be addressed
Weekly Project status update	· ACSA-IT PM (chair) · ACSA Technical Operations Manager · Provider Senior Site Manager · Provider Project Manager · Provider administrator	· Minutes of meeting · Updated project schedule · Action register for any open actions to be addressed · Risks and Issues register
Monthly Care Review	· ACSA Technical Operations Manager (chair) · Provider Senior Site Manager · Provider relationship Manager · Provider administrator	· Minutes of meeting · Action register for any open actions to be addressed · Risks and Issues register · Service Credit Report
Quarterly review meeting	· ACSA Technical Operations Manager (chair) · Provider Senior Site Manager · Provider Relationship Manager · Provider administrator · Senior Manager IT Infrastructure	· Minutes of meeting · Action register for any open actions to be addressed · Risks and Issues register
Annual review meeting	· ACSA Technical Operations Manager (chair) · Senior Manager IT Infrastructure · Provider Senior Site Manager · Provider Relationship Manager · Provider administrator · Senior Manager IT Infrastructure	· Minutes of meeting · Action register for any open actions to be addressed · Risks and Issues register

Table 59 Meetings 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	Summarised report weekly	COB every Friday	ACSA Technical Lead	Email written report summary with supporting tables.	Weekly Service Review
	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	ACSA Technical 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	ACSA Technical 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

Frequency	Report Name	Report Content	Due date	Submit to	Format	Meeting Name and frequency
	Baseline (CMDB) information	Review updates to Baseline CMDB	3 days before Quarterly review meeting	ACSA Technical Lead	Email Excel document	Quarterly review meeting
	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	ACSA Technical Ops manager	Email PDF document	Annual review meeting
	Contract adherence review	Summary of contract requirements and adherence thereof	3 days before annual review meeting	ACSA Technical Ops manager	Email PDF document	Annual review meeting

Table 60 Reporting definitions