Annexure A - Scope of Work

For

IT Telecommunication Services

Bid Number **COR7979/2025/RFP**

Description:

Request for Proposal for the Supply, Installation, Commissioning, Support and Maintenance of IT Telecommunication Services for 84 months to Airports Company South Africa

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

www.airports.co.za

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

Confidential

CONTENTS

TABLES

1.0 Scope Of Work Overview and Objectives

1.1 Background

The Airports Company South Africa (ACSA) invites licensed service providers to submit proposals for the provision of a unified voice, video, and data network that will connect all its local and international airports throughout South Africa, while ensuring seamless integration with public cloud services. The network should accommodate ACSA's requirements for both on-premises client-server communications and public cloud utilization, supporting the organisation's digital transformation objectives. As ACSA accelerates the migration of applications and workloads from on-premises environments to public cloud Software-as-a-Service (SaaS) and Infrastructure-as-a-Service (IaaS) platforms, our long-term vision is to establish a cloud-first Wide Area Network (WAN).

ACSA operates airports in Kempton Park, Cape Town, Durban, Gqeberha, East London, George, Bloemfontein, Kimberley, and Upington, with primary data centres located at O.R. Tambo and Cape Town International Airports.

National Coverage: Since ACSA requires services across airports in cities in multiple provinces (Kempton Park, Cape Town, Durban, Gqeberha, East London, George, Bloemfontein, Kimberley, and Upington), providers must hold Individual Electronic Communication Network Service (ECNS) and/or Individual electronic communications services (IECS) licences to operate nationally.

Cloud-First WAN: Providers offering cloud access services must ensure their Electronic Communication Services (ECS) licence covers data services and that their infrastructure supports high-speed, low-latency connections to public cloud platforms (SaaS and IaaS).

Voice over Internet Protocol (VoIP) and Numbering: For VoIP services, the IECS licence must include the ability to use numbers from the National Numbering Plan, supporting geographic and non-geographic numbers for ACSA's operations.

Network Reliability: Providers must demonstrate compliance with The Independent Communications Authority of South Africa's (ICASA) quality-of-service standards, especially for voice and data traffic, to meet ACSA's need for seamless connectivity between airports and data centres at O.R. Tambo and Cape Town International Airports.

NB: Bidders must assume that they have no existing network infrastructure on site when preparing their pricing. All costs should be based on delivering a full solution from scratch.

If the winning bidder has existing infrastructure that could be used, this will be discussed during contract negotiations and may be used to adjust the final price, as long as:

- **The infrastructure is proven to be owned and in good condition**
- **It meets all technical and service requirements**

1.2 High-Level Scope of Work Required

This annexure will form part of the contract with the service provider and the service provider is obliged to meet all the specifications and requirements as outlined in this Scope of Work document.

Note: Not all parts of the below scope are guaranteed to be implemented. ACSA may implement individual parts of the scope as and when required. There should be no minimum term for any parts of the scope.

1.2.1 WAN

ACSA uses a WAN network to provide reliable, high-performance, and scalable network connectivity between all nine ACSA airports.

1.2.2 Corporate Internet Breakouts

Due to the largescale utilisation of cloud services, ACSA uses enterprise grade internet links with dedicated bandwidth to provide local internet connectivity at all nine airports.

1.2.3 Public Internet Breakouts

ACSA offers all its passengers Free Public WIFI. A lower cost Internet solution with high bandwidth such as Fibre-to-the-Business (FTTB) is required at all airports to support this requirement.

1.2.4 Point to Point Long distance fibre links.

The Disaster Recovery (DR) site is at Cape Town International airport. Point to Point high speed fibre links are required between OR Tambo International Airport and the DR site at Cape Town International airport for data replication.

1.2.5 Voice Carrier Services

ACSA's telephony services are a key part of the communications platform upon which core business operations and processes are based. ACSA's requirement is to make outbound voice telephone calls at the most cost-effective way while retaining acceptable voice quality. Telephone calls between airports are expected to be free-on-net and will be routed over the corporate WAN.

1.2.6 Fibre-to-the-Home (FTTH) services

ACSA currently has multiple users that connect remotely to ACSA IT Systems using Virtual Private Network (VPN). Internet connectivity for these users at the remote sites is provided using FTTH.

1.2.7 MultiCloud Services

ACSA may require private, dedicated, and high-throughput connectivity between on-premises networks and cloud providers. It will serve as a direct, private connection between ACSA and the cloud providers that bypasses the public internet.

1.2.8 NAPAfrica Services

ACSA may consider hosting some of its Compute resources at Terraco Data centres located close to ACSA airports. In this case direct fibre links will be required from the three airports at O.R. Tambo International, Cape Town International and King Shaka International.

1.3 Service Objectives

The primary high-level service objectives that ACSA aims to accomplish through this Request for Proposal (RFP) are outlined below.

1.3.1 Provide a reliable, scalable, and resilient telecommunication services infrastructure to ACSA.

1.3.2 Acquire services with service quality guarantees backed by Service Level Agreements (SLAs).

1.3.3 Minimise administrative effort by engaging the Provider to provide the management function to achieve the SLAs specified in this scope of work.

1.3.4 Providing ACSA-IT with the ability to expand its service delivery and support services to ACSA business, subsidiaries, and stakeholders.

1.3.5 Reduce service delivery costs through re-using or transitioning existing infrastructure, and the effective utilisation of existing licensing agreements.

1.3.6 Receive services based on current industry standards and best practices.

1.3.7 ACSA continually drives to implement best practices and standards. ACSA has either implemented, is currently implementing, or is planning the implementation of these best practices. All work by the Providers must always align and assist ACSA in working towards implementing the desired strategy and standards.

2.0 Service Environment

2.1 Service locations.

2.1.1 A description and location of all ACSA facility and office locations requiring in-scope telecommunication services.

2.1.2 This Site Schedule can be revised by agreement between the ACSA and the Provider account manager/Service Manager from time to time to meet the ACSA's requirements at additional locations.

ACSA SITE ID		Physical Address
Cluster 1		
1	JNB	O.R. Tambo International Airport, Airport Rd, Johannesburg, 1627
2	BFN	Bram Fischer International Airport, Bloemfontein, 9300
Cluster 2		
3	CPT	Cape Town International Airport, Matroosfontein, Cape Town, 7490
4	GRJ	George Airport, Old Mosselbay Road, George, 6529
5	KIM	Kimberly Airport, Compound Patterson Road, Kimberly, 8300
6	UTN	Upington International Airport, Diedericks Street, Upington, 8801
Cluster 3		
7	DUR	King Shaka International Airport, La Mercy, 4407
8	PLZ	Chief Dawid Stuurman International Airport, Allister Miller Drive, Walmer, 6070
9	ELS	King Phalo Airport, Settlers Way, East London, 5200

Table 1 - Regional Distribution of ACSA locations

SITE CODE	ADDRESS
JNB	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	Chief Dawid Stuurman International Airport, Allister Miller Drive, Walmer, 6070
GRJ	George Airport, Old Mosselbay Road, George, 6529
ELS	King Phalo 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 2 - Detailed site schedule

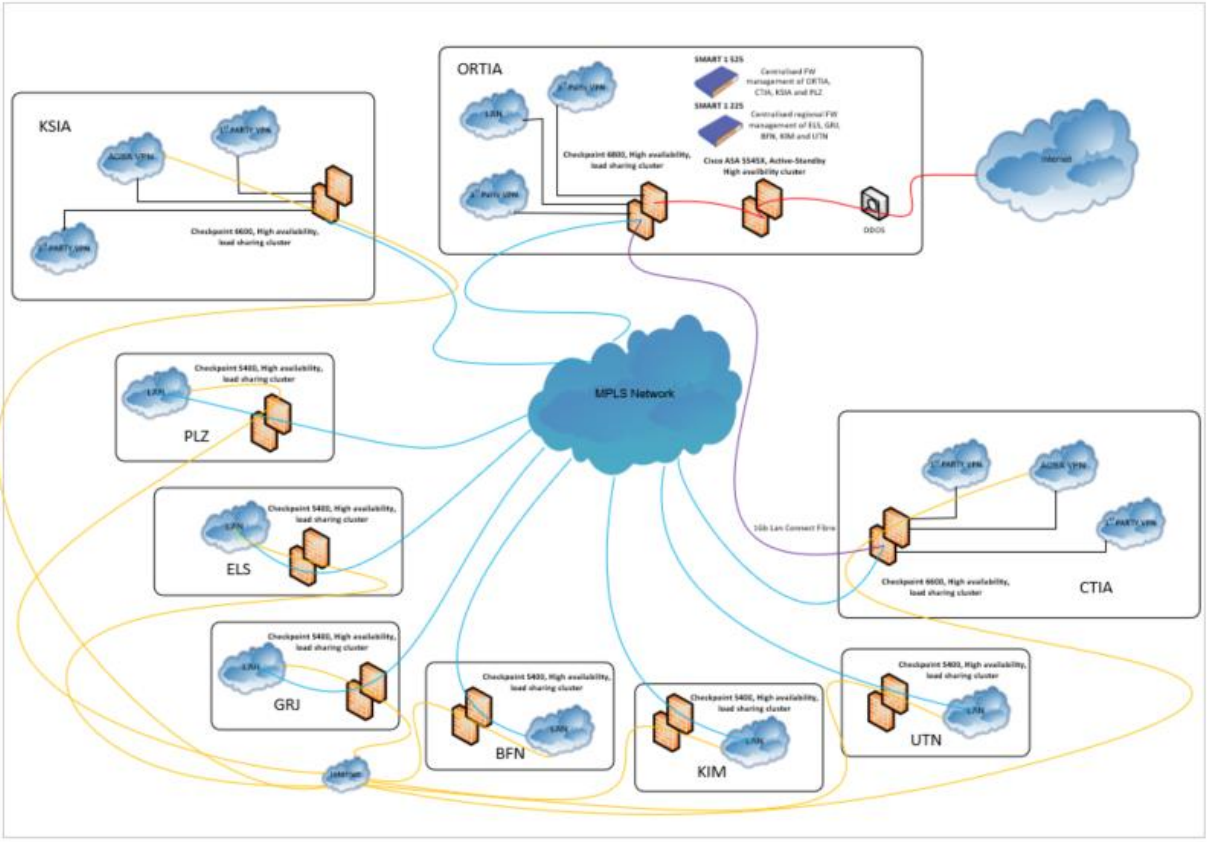


Figure 1: Current ACSA WAN Architecture diagram.

SITE	Facility
JNB – Primary	JOC Core Room 1 on 4th floor International Terminal A
JNB – Secondary	Core Room 3 on 3rd floor Domestic Terminal B
CPT – Primary	Core Room 3 in Central Terminal Building 2nd Floor
CPT – Secondary	Core Room 4 in Central Terminal Building 3rd Floor
DUR – Primary	Core Room 1 in Main Terminal Basement
DUR – Secondary	Core Room 2 in Main Terminal Basement
PLZ – Primary	Core Room 1 in Terminal A Basement
PLZ – Secondary	Core Room 2 in Terminal A Basement
GRJ – Primary	Server Room 1 on 1st floor Admin offices
GRJ – Secondary	Server Room 1 on 1st floor Admin offices
BFN – Primary	Server Room 1 on 1st floor Admin offices
BFN – Secondary	Server Room 1 on 1st floor Admin offices
KIM – Primary	Server Room 1 on 1st floor Admin offices
KIM – Secondary	Server Room 1 on 1st floor Admin offices
ELS – Primary	Server Room 1 on 1st floor Admin offices
ELS – Secondary	CCTV Control Server Room AKA Wire Centre 1
UTN – Primary	Sever Room 1 on Ground floor Admin offices

SITE	Facility
UTN – Secondary	Sever Room 1 on Ground floor Admin offices

Table 3 - ACSA Primary and Secondary Core Room Location

3.0 Scope Of Work

The Provider must design a solution using any technology if it meets the functional requirements, and is cost-effective, efficient, and adaptable to future growth. Alternative approaches and/or methodologies to accomplish the desired or intended results of this procurement are solicited. However, proposals which depart from, or materially alter the terms, requirements, or scope of work defined by this RFP will be rejected as being non-responsive. Any additional equipment required from ACSA to support any of the technologies implemented will be at the Provider's cost.

3.1 Wide Area Network (WAN)

The appointed Provider must provide the network that must include, but is not limited to, the following:

Implement an IP-based Wide Area Network (WAN) connecting all nine ACSA airports.

3.1.1 ACSA requires that last-mile connectivity for all services be delivered over fibre. ACSA might consider connectivity via microwave or 5G, but only as standby or failover link at the smaller local airports (ELS, GRJ, KIM, UTN, BFN). Copper connectivity is not an acceptable option.

3.1.2 Provide and manage edge devices that will connect directly via Cat6A LSZH SFTP patch leads to ACSA owned and managed WAN in-path optimization equipment at minimum 1Gbps Ethernet link speed.

3.1.3 The Provider must clearly indicate the maximum bandwidth that can be provisioned on the proposed infrastructure per site, without any further equipment costs such as license upgrades, etc.

3.1.4 Provision efficient Quality of Service (QoS) between ACSA sites throughout the Provider network.

3.1.5 The QoS must be flexible such that if there is no voice/video traffic, data should use all the physically available bandwidth on the link.

3.1.6 The Provider's network must offer on a per class basis specific worst-case end-to-end delay guarantees, which would be sufficient such that the applications and real-time traffic in each class would function adequately.

3.1.7 The primary route shall always carry all traffic unless the service is degraded for whatever reason.

3.1.8 Primary and secondary links are to be of equal latency, capacity and cost.

3.1.9 If the primary route fails, the traffic must automatically failover to secondary access route until the primary route is restored.

3.1.10 The Provider's network infrastructure should be compatible to migrate to IPv6 as and when required by ACSA without additional cost to ACSA. The infrastructure provided by the Provider

should support IPv6 and all other devices supplied by the Provider to commission the link should be IPv6 compliant.

3.1.11 Any of ACSA's network segments should be reachable directly from any other ACSA's location through the Provider's network, via the shortest path within the Provider's network.

3.1.12 The network should be logically isolated from Internet traffic even if running on the same physical core/backbone. It is required that same VPN does not run both customer business and Internet traffic. The inter-airport WAN network offered to ACSA should not carry any internet routes. Provider must provide a separate network topology showing how internet services is provided.

3.1.13 The Provider must submit proof undertaking for providing dedicated 1:1 media for the usage by ACSA, and that the WAN traffic is securely isolated from Internet traffic.

3.1.14 The Provider must provide a monitoring tool that should report on real-time and historic bandwidth utilisation. The reports should cater for overall bandwidth reporting or per specific source IP address. The reporting period must be configurable by days and or times, e.g., previous month, and times 9:00am to 5:00pm. The data must be accessible via Application Programmable Interface (API) calls or be automatically exportable in excel format on a schedule (RAW Data).

3.1.15 The Provider must cater for at least 100% increase in bandwidth should it be needed during the contract term.

3.1.16 The Provider must ensure that the latency between any two ACSA premises should be less than the following with and without load:

- 50 ms. - Optical fibre circuit
- 75ms. - Microwave

The above latency must be demonstrated by the Bidder, as and when required by ACSA, between the Bidder's demarcation points at each of ACSA's premises, including local lead and last mile cabling.

3.1.17 must cater for at least 100% increase in bandwidth should it be needed during the contract term.

3.1.18 WAN Quality of Service (Service Classes)

ACSA will classify all IP traffic with an appropriate DSCP value before it is transmitted to the WAN and these classifications shall be honoured by the Provider. Interclass bursting must be allowed so that bandwidth may be shared from one class to another. For example, if there is no voice or video traffic, then data should be able to use the full available capacity.

Class of Service (Coos) bandwidth allocation must be minimum as per Table 9 - Class of Service and Bandwidth Allocation. Note: Providers should scope the actual link speed as close as possible to these requirements depending on their service offerings.

SITE	Last Mile Connectivity	Physically Diverse Routes	Physically Diverse Customer Premises	Bandwidth
JNB – Active Link	Fibre	Yes	Yes	145Mbps
JNB – Standby Link	Fibre	Yes	Yes	145Mbps
CPT – Active Link	Fibre	Yes	Yes	55Mbps
CPT – Standby Link	Fibre	Yes	Yes	55Mbps

SITE	Last Mile Connectivity	Physically Diverse Routes	Physically Diverse Customer Premises	Bandwidth
DUR – Active Link	Fibre	Yes	Yes	50Mbps
DUR – Standby Link	Fibre	Yes	Yes	50Mbps
PLZ – Active Link	Fibre	Yes	Yes	25Mbps
PLZ – Standby Link	Fibre	Yes	Yes	25Mbps
ELS – Active Link	Fibre	Yes	No	25Mbps
ELS – Standby Link	Fibre	Yes	No	25Mbps
GRJ – Active Link	Fibre	Yes	No	25Mbps
GRJ– Standby Link	Fibre	Yes	No	25Mbps
BFN – Active Link	Fibre	Yes	No	25Mbps
BFN – Standby Link	Fibre	Yes	No	25Mbps
KIM – Active Link	Fibre	Yes	Yes	20Mbps
KIM – Standby Link	Fibre	Yes	Yes	20Mbps
UTN – Active Link	Fibre	Yes	No	20Mbps
UTN – Standby Link	Fibre	Yes	No	20Mbps

Table 4 - ACSA Inter-site minimum bandwidth requirement

3.2 Corporate Internet Breakout

3.2.1 The appointed Provider must provide Corporate Internet connectivity at all nine ACSA airports that must meet the following requirements: Each location must be allocated dedicated Internet bandwidth with capacity as per Table 5- ACSA Corporate Internet Bandwidth Requirement. Please note that these figures are preliminary and may be subject to reduction or increase at the time of contract finalization, depending on our evolving business needs and internal assessments

3.2.2 Bandwidth capacity is for local and international traffic.

3.2.3 The internet links must be fully redundant and support dynamic failover between the redundant links in less than one (1) minute.

3.2.4 The service should cater for disaster recovery for the internet connection and should not be dependent on any single site.

3.2.5 The internet link must be flexible to allow incremental bandwidth changes without hardware or access technology changes.

3.2.6 The internet link shall provide (1:1) full duplex Internet connectivity.

3.2.7 There should be a maximum latency of 10ms from any ACSA network to the Providers Data Centre known as Point of Presence (POP).

3.2.8 The Provider shall provide edge devices, if necessary, that will connect directly via Cat6A LSZH SFTP patch leads to ACSA-owned and managed routers at a minimum 1Gbps Ethernet link speed.

3.2.9 All ACSA-owned public IP ranges, provided in (Table 5 - ACSA Public IP ranges to be routed to ACSA sites) must be routed to the ACSA network.

3.2.10 All ACSA-owned domains are to be hosted by the Provider. (co.za and .com).

3.2.11 All DNS, PTR and MX records are to be hosted by the Provider.

3.2.12 The Provider must provide a portal where ACSA can add, remove, or update Domain Name Service (DNS) records as and when required.

3.2.13 The Provider shall configure QOS on the internet link to protect business-critical applications from congestion as directed by ACSA.

3.2.14 The selected Provider is bound to demonstrate the performance of all the links, as required by ACSA during the commissioning of the links and during the service period.

3.2.15 The Provider must provide a monitoring tool that should report on real-time and historic bandwidth utilisation. The reports should cater for overall bandwidth reporting or per specific source IP address. The reporting period must be configurable by days and or times, e.g. previous month, and times 9:00 am to 5:00 pm. The data must be accessible via API calls or be automatically exportable in excel format on a schedule (RAW Data).

3.2.16 The Provider shall have a minimum of two Internet breakouts out of South Africa on major cables. Documented proof showing the two breakout connections must be submitted.

3.2.17 The Provider must cater for at least 100% increase in bandwidth should it be required during the contract term.

Site Name	Airport Name	Bandwidth
JNB	OR Tambo International Airport	1024Mbps
CPT	Cape Town International Airport	600Mbps
DUR	King Shaka International Airport	500Mbps
PLZ	Chief Dawid Stuurman International Airport	100Mbps
ELS	King Phalo Airport	100Mbps
GRG	George Airport	100Mbps
BFN	Braam Fisher Airport	100Mbps
KIM	Kimberly Airport	100Mbps
UTN	Upington Airport	100Mbps

Table 5 - ACSA Corporate Internet Minimum Bandwidth Requirement

IP Range	Mask	Site
196.11.1.0	/24	JNB
196.11.2.0	/24	JNB
196.11.3.0	/24	JNB
196.11.4.0	/24	JNB
196.11.5.0	/24	JNB
196.11.6.0	/24	JNB
196.11.6.0	/24	JNB
196.11.7.0	/24	JNB
196.11.8.0	/24	CPT
196.11.9.0	/24	JNB
196.11.10.0	/24	JNB
196.11.11.0	/24	JNB
196.11.12.0	/24	DUR
196.11.13.0	/24	JNB
196.11.14.0	/24	JNB
196.11.15.0	/24	PLZ
196.11.16.0	/24	JNB
196.11.17.0	/24	JNB
196.11.18.0	/24	JNB
196.11.19.0	/24	JNB
196.11.20.0	/24	ELS
196.11.21.0	/24	JNB
196.11.22.0	/24	BFN
196.11.23.0	/24	JNB
196.11.24.0	/24	KIM
196.11.25.0	/24	JNB
196.11.26.0	/24	GRJ
196.11.27.0	/24	JNB
196.11.28.0	/24	UTN
196.11.29.0	/24	JNB
196.11.30.0	/24	JNB

Table 6 - ACSA Public IP ranges to be routed to ACSA sites.

3.3 Public Internet Breakouts

The appointed Provider must provide Internet connectivity that will be used for Public WIFI services at all nine ACSA airports. ACSA may have an existing service provider for this service at certain locations, and the new service will only commence once the existing contracts terminate. The service must meet the following requirements for optimal performance and reliability:

3.3.1 Usage Policies: All links provided by the supplier must be uncapped, offering symmetrical speeds without any shaping, throttling, or fair usage policy restrictions.

3.3.2 ISP Medium: All links should be fibre.

3.3.3 Termination Point: The links should terminate within the ACSA Core rooms as per Table 3 - ACSA Primary and Secondary Core Room Location

3.3.4 Infrastructure Support: Rack space, power, and cooling will be provided by ACSA in a secured, access-controlled environment to ensure the proper functioning and security of the equipment.

3.3.5 Below are the minimum bandwidth requirements per site.

3.3.6 The Provider must provide monitoring capabilities to allow ACSA to view real-time utilisation of bandwidth. This is crucial for detecting and addressing any instances of high utilisation. Monthly utilisation and availability reports need to be provided for all links.

3.3.7 The Provider must cater for at least 100% increase in bandwidth should it be required during the contract term.

ACSA SITE ID	Bandwidth required
JNB	5Gbps
CPT	2Gbps
DUR	2Gbps
PLZ	1Gbps
ELS	1Gbps
GRJ	1Gbps
KIM	1Gbps
BFN	1Gbps
UTN	1Gbps

Table 7 - Public Internet Minimum Bandwidth required per site

3.4 Point to Point long distance Fibre Links

The Provider shall provide redundant direct fibre links between

- OR Tambo International Airport and Cape Town International Airport.
- OR Tambo International Airport and King Shaka International Airport.
- King Shaka International Airport and Cape Town International Airport.

3.4.1 The redundant links shall follow different geographical routes. There shall be no single point of failure affecting both links.

3.4.2 The proposal shall include a detailed technical diagram and shall indicate the physical type of interface being provided at either end.

3.4.3 End customer devices will be network switches supporting a minimum 1Gbps SFP and 10Gbps SFP transceivers.

3.4.4 Link capacity shall be a minimum of 1Gbps.

3.4.5 The pricing schedule shall indicate monthly rental costs for an unmanaged reactive SLA solution as well as a managed and monitored service with a proactive SLA.

3.4.6 Point-to-Point fibre termination points are required in the following physical locations:

LINK NO	Side A – Location	Side B – Location	Medium
CPT - JNB	Cape Town International Airport, CTB 1st Floor Service Passage, Core Room 3	OR Tambo International Airport, 4th Floor International Terminal A, JOC Core room 1	Point-to-Point fibre
CPT - JNB	Cape Town International Airport, CTB 3rd Floor AMC, Core Room 4	OR Tambo International Airport, 3rd Floor Domestic Terminal B, Core Room 3	Point-to-Point fibre
CPT - DUR	Cape Town International Airport, CTB 1st Floor Service Passage, Core Room 3	King Shaka International Airport Terminal Basement Core Room 1	Point-to-Point fibre
CPT - DUR	Cape Town International Airport, CTB 3rd Floor AMC, Core Room 4	King Shaka International Airport Terminal Basement Core Room 2	Point-to-Point fibre
JNB - DUR	OR Tambo International Airport,4th Floor International Terminal A, JOC Core room 1	King Shaka International Airport Terminal Basement Core Room 1	Point-to-Point fibre
JNB - DUR	OR Tambo International Airport, 3rd Floor Domestic Terminal B, Core Room 3	King Shaka International Airport Terminal Basement Core Room 2	Point-to-Point fibre

Table 8 - Point to Point Fibre End Points

3.5 Voice Carrier Services

ACSA's objective is to achieve the lowest cost for calls at an acceptable quality. The Provider must provide pricing for all ACSA's outbound call destinations classes (e.g. International, national, local, mobile operator). ACSA will update its call routing strategy to the Providers based on the best pricing per destination. ACSA's strategy is to carry all internal fixed-line calls between airports using the Wide Area Network. The breakouts at all airports must be over SIP Trunking or equivalent technology.

SIP trunking bandwidth required:

Site	PABX	Bandwidth Required
JNB	Cisco CUCM	30Mb
CPT	Cisco CUCM	20Mb
DUR	Cisco CUCM	20Mb
PLZ	Cisco CUCM	9Mb
GRJ	Cisco CUCM	5Mb
ELS	Cisco CUCM	5Mb
KIM	Cisco CUCM	5Mb
BFN	Cisco CUCM	5Mb
UTN	Cisco CUCM	5Mb

Table 9 – Sip Trunking Bandwidth Requirements

The appointed Provider must provide the Voice Carrier Services that includes, but not limited to the following:

3.5.1 The Provider must cater for at least 100% increase in bandwidth should it be required during the contract term.

3.5.2 Managed Session Initiation Protocol (SIP) Connectivity on Provider's network infrastructure with guaranteed classes of service for voice network traffic.

3.5.3 Underlying communication technologies that enable ACSA's inbound and outbound voice communications at an acceptable quality and the lowest possible cost.

3.5.4 Ad-hoc - Future requirements for voice services as and when new airports/sites are built or acquired and for capacity increase or decrease.

3.5.5 The bidder must support < 35ms jitter for voice/real-time COS bandwidth for 1024 kbps and above links.

3.5.6 Call Detail Record (CDR) Telephone Management Reporting Portal

3.5.7 Connect the Provider's onsite termination equipment to the onsite gateway/PABX using Ethernet Network.

3.5.8 Maintenance and Support of equipment, software and service provided in line with the service level requirements.

3.5.9 The Provider's network must offer on a per class basis specific worst-case end-to-end delay guarantees, which would be sufficient for real-time traffic.

3.5.10 Primary and Secondary breakout SIP Trunking links at each ACSA site with Automatic failover to secondary access route in case of a failure on the primary route until the primary route is restored.

3.5.11 ACSA's voice traffic should be isolated from other customers' traffic even if running on the same core/backbone.

3.5.12 The Provider must be able to provide the Voice Carrier Services without requiring ACSA to change its numbers for inbound calls. The Voice Carrier Provider will therefore be required to port the

existing ACSA numbers to meet this condition as part of the transition. The numbers are provided in Annexure D – ACSA Telephone Number Ranges.

3.5.13 No least cost routing appliances/equipment must be used.

3.5.14 The pricing may be based on discounts that are contingent on the actual volume of outbound calls or on the actual spend ACSA makes to qualify for such discounts. However, ACSA is not able to predict the actual volume of calls in the future. If the pricing offered by a Provider in its Proposal includes volume discounts, such pricing must be clearly shown in addition to the based per second pricing.

3.5.15 Microsoft Teams – direct routing installation and associated licenses, DSP Media Processing Modules for Silk Transcoding and all other related software and configuration should be included in the costing.

3.5.16 The Provider must provide a monitoring tool that should report on real-time and historic bandwidth utilisation. The reports should cater for overall bandwidth reporting or per specific source IP address. The reporting period must be configurable by days and or times, e.g. previous month, and times 9:00 am to 5:00 pm. The data must be accessible via API calls or be automatically exportable in Excel format on a schedule (RAW Data).

3.5.17 Telephone Call Management and Reporting

ACSA requires the Provider to provide a Reporting Portal which is accessible by ACSA or an ACSA designated agent via a secure Internet connection. The proposed system must integrate with, and collect CDR's from Microsoft Teams, as well as the local Cisco Unified Communication Managers at each airport. The Reporting Portal in a Provider's Proposal must provide the following:

3.5.17.1 A downloadable electronic record of all details of inbound and outbound calls. The entire detailed history of all call records must be available for the duration of the term.

3.5.17.2 All aspects of call including duration, source, destination, and costs.

3.5.17.3 On demand and scheduled reports.

3.5.17.4 The facility to bar an extension once a designated budget value is reached.

3.5.17.5 The Reporting Portal must include functionality to:

- Effect role-based access with AD authentication.
- Filter all reports using date ranges, and other filters to limit the data selected. Summarisation functionality must allow summarisation to selectable time periods (e.g. per day, week, month, year etc.)
- Export raw data for further Analysis.
- Send email reports to individuals and schedule report to be sent automatically at desired frequencies.
- The data must be accessible via API calls

3.6 FTTH Services

The Provider shall provide remote connectivity services by any technology available to ACSA remote users. The below are the functional requirements:

3.6.1 As a minimum, the following must be supported:

- Fibre to the Home (FTTH) – min 50Mbps.
- Fibre to the Business (FTTB) – min 50Mbps.
- LTE uncapped**.**

3.6.2 The Provider shall provide remote support services for fault handling.

3.6.3 The Provider call centre for remote connectivity services shall be available 24 x 7 to log all incidents and provide support.

3.6.4 The Provider must include the call logging procedure and escalation process.

3.6.5 A facility should be provided to email users a daily/weekly/monthly report on their usage of the services, these reports must be available irrespective if the allocated data is unlimited.

3.6.6 The Provider shall bill only for active accounts during the billing month. Billing for accounts that are not activated during the billing month will not be accepted.

3.6.7 The Provider will be required to migrate all existing FTTH, FTTB and LTE services that are currently in use to the Provider's network. A list of all these street locations is provided in Annexure E – ACSA FTTH Locations. The full street address will only be provided at a later stage.

3.6.8 For new installations, the service provider is required to install within two weeks from date of request from ACSA.

3.7 Multicloud Services

Direct private connection from on-premises to cloud providers is not currently in use however, ACSA may require these services in the future based on the below requirements.

3.7.1 The service must be reachable from any ACSA airport.

3.7.2 The service should be provided with a minimum 100Mbps link.

3.7.3 The Provider must cater for at least 200% increase in bandwidth should it be required during the contract term.

3.8 NAP Africa Services

NAP Africa Services are currently not in use; however, ACSA may require these services in the future based on the below requirements.

3.8.1 The service must be provided for each of the three airports, namely, JNB, CPT and DUR, to the nearest NAP Africa peering point.

3.8.2 Connectivity must be provided via fibre links at a minimum speed of 100 Mbps per site.

3.8.3 Cost should include any port /enablement charges as part of the monthly rental to use the service, including any NAPafrica charges.

3.9 General Technical Requirements

3.9.1 All routers must have the ability to export traffic flow data to the ACSA management tools if requested.

3.9.2 Operating systems and firmware must be patched consistently to the latest stable and Original Equipment Manufacturer (OEM) recommended versions and maintain at minimum an N-1 relation to the latest recommended release.

3.9.3 Router information and configurations must be made available for audit purposes to the Auditor-General and ACSA or any third party appointed to audit ACSA's network security.

3.9.4 The Provider shall provide all required equipment and services, whether explicitly mentioned in this RFP to ensure the intent of specification, completeness, operability, maintainability, and upgradeability of the solution.

3.9.5 The solution must be scalable and flexible for downgrade, upgrade, and cancellation of sites as and when business requirements dictate.

3.9.6 The proposed technology must be reviewed every 12 (twelve) months to align the proposed technology with the latest technology trends in the market.

3.9.7 The Provider shall schedule and perform testing of backup links quarterly; these tests will be done afterhours, and result of the test shall be reported on a monthly service review management report.

3.9.8 The solution will include, designing, provisioning, installation, commissioning, integration, testing, acceptance, and maintenance of all equipment used in the solution.

3.9.9 The Provider must have full-fledged "Network Management Centre /Network Operating Centre (NMC/NOC)", operating around the clock (24x7x365 basis) staffed by skilled technical workforce, for the efficient centralized remote monitoring, configuration, diagnosis/troubleshooting and performance management of backbone network and last mile network over which the Internet Services connectivity for ACSA shall be provisioned.

3.9.10 The Provider's network infrastructure should be compatible to migrate to IPv6 as and when required by ACSA without additional cost to ACSA.

4.0 Baseline Information

This section provides a summary of information, which may be pertinent for determining the service requirements. These business requirements represent ACSA's projection of the service requirements from the first day of the contract. This baseline is to be maintained and updated by the Provider and reviewed with ACSA IT Infrastructure every quarter.

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

4.1 Current Voice Carrier Services

ACSA's requirement is to ensure that we maintain high availability of voice communications systems at optimal cost efficiency. ACSA' priority is to carry its inbound, outbound, and transferred voice calls using SIP technology to and from the airports.

A critical component of the Voice Carrier Services is the provision of up to date, and in certain cases real-time, (CDR) Call Detail Record Management system, which allows reporting and barring services to ACSA. The CDR telephone management system is web-based and allows integration to ACSA's on premise Cisco PABX's.

Site	PABX	Number of Handsets
JNB	Cisco CUCM	2053
CPT	Cisco CUCM	923
DUR	Cisco CUCM	868
PLZ	Cisco CUCM	87
GRJ	Cisco CUCM	55
ELS	Cisco CUCM	73
KIM	Cisco CUCM	33
BFN	Cisco CUCM	68
UTN	Cisco CUCM	41

Table 10 - ACSA Baseline of current IP Phone infrastructure

5.0 Invoices

5.1 All invoices' submissions to meet the following requirements:

5.1.1 Statement of account

5.1.2 Payment date

5.1.3 Invoice to have the ACSA purchase order number coded on it.

5.1.4 Copy of Purchase Order

5.1.5 All invoices to have the individual services itemised. In the event of a penalty being applied, the penalty will be calculated using the itemised values for the respective services where the SLR was breached.

5.1.6 A report must be included in the invoice pack as a PDF and an Excel file that contains:

5.1.6.1 Full usage report for the month in question

The report must show:

a. Utilisation
b. Availability
c. Number of calls made for voice invoice.

5.2 All invoices not in dispute will be paid according to payment terms.

6.0 Personnel

6.1 The Provider will be responsible for professional and appropriately certified staffing to meet the Services Roles and Responsibilities, and Service Levels outlined in this service specification.

6.2 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 four months of the request.

6.3 Suitably certified resources are required at all locations for preventative and corrective maintenance.

6.4 Providers should adapt their resourcing model to meet the Service Level Agreement (SLA) for preventative and corrective maintenance, respectively. SLR's are listed in Section 12.5 Service Level Requirements (SLRs).

6.5 All resources must sign the ACSA Non-Disclosure Agreement as supplied in this tender.

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

Role	Location	High-Level Function	Minimum Resources Required and Coverage Window
Technician	All Sites - Variable as and when required.	• Will be based offsite only required to meet the SLA requirements. • Monitor the environment for all sites– receive and respond to incidents and alerts. • Maintain the environment – maintenance including OS, Software, and firmware updates. Ensure compliance with ACSA IT standards. • IMACD plans • Reporting - as defined in the reporting table, and any other ad-hoc reports as requested by ACSA. • Co-ordinate new requests, change requests, documentation, quality control. • Assist with managing all site installations/projects/maintenance. • Preventative maintenance tasks, schedules, processes, and procedures will be part of the Provider's preventative maintenance plan.	As and when required to meet the SLA requirements
Account Manager	JNB - Variable as and when required.	• Manage service environment to meet the SLA requirements. • Schedule regular meetings with stakeholders and report on performance	As and when required to meet the SLA requirements

Table 11 - Minimum resource requirements

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

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

<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>JNB</td><td>24-hour operation</td><td>24-hour operation</td></tr>
<tr><td>CPT</td><td>24-hour operation</td><td>24-hour operation</td></tr>
<tr><td>DUR</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 - -7:00 - 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 that impact the live environment will take place after the last flight has departed and before the first flight departs/arrives in the morning. These hours vary from airport to airport, but 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 12 - Service Coverage Window definitions

6.9 The Provider should ensure a resourcing model is in place that allows the achievement of the SLAs and ensures the ability to deliver services during the defined Service Coverage Windows. The Provider is to always ensure a full complement of resources.

7.0 Equipment And Spares Holding Requirements

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

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

8.0 Preventative And Corrective Maintenance

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

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

8.3 Break/fix includes maintenance that is unforeseen and is necessary to restore the serviceability of the infrastructure, and functionality of the System. Some of this break/fix maintenance could be requested after hours on weekends and public holidays. Service Providers will be expected to respond and attend to all the faults.

8.4 The Provider must make provision for after-hours, weekends, and public holidays support on for incidents that impact the systems.

8.5 The Provider must cater for short notice callouts in an emergency where the supported system may be affected by other interruptions or change processes within the airport.

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

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

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

9.0 Special notes on pricing

9.1 The pricing specified in the contract will remain fixed for its entire duration, with no additional Consumer Price Index (CPI) adjustments beyond what is detailed in the provided pricing file.

9.2 Billing for a service will commence only after the service has been signed off by ACSA.

9.3 The term for each service will coincide with the contract's term (Co-Termination). For example, if the contract is for 84 months and a service is implemented in month 24, all services will terminate at the end of month 84 (main contract end date), regardless of their individual start dates.

10.0 Out of Scope

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

10.1 IT Facilities, Space, Power, HVAC.

11.0 Roles And Responsibilities

In this SOW, we use the RASCI ("Responsible, Accountable, Supporting, Consulted and Informed") chart approach for all roles and responsibilities matrices.
The RACI terminology is as follows:

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

Table 13 - Definition of the RASCI Model

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

11.1 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 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 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 visits when using non-regular or 3rd party resources	R, A	C, I
	13.	Ensure that support staff has access to reliable transport and valid driver's licences.	R, A	C, I
	14.	Support staff must have the relevant safety certifications, protective wear, and equipment to carry out corrective maintenance duties.	R, A	C, I
	15.	Ensure that the Provider always has a valid health and safety file where required	R, A	C, I
	16.	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
	17.	Parking fees at ACSA premises	R, A	I

Sub-area	Number	Task/Activity	Provider	ACSA
	18.	Any security-related training and payments for access to ACSA premises	R, A	I

Table 14 - Roles and Responsibilities – General

11.2 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 documenting the requirements for architectural, functional, performance, IT Service Continuity, and security requirements.

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

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

Sub area	Number	Task/Activity	Provider	ACSA
Architecture Planning and Analysis	1.	Adhere to, implement, and ensure alignment to the defined standards, timeframes and reporting requirements for planning, project management and analysis activities.	R, A	C,S,I
	2.	Attend and actively participate in the ACSA scheduled focus groups, stakeholder meetings, project, and technical workshops to provide the required expertise (addressing all tasks pre and post the meeting as required such as requirements gathering activities; solution design options)	R,A	C,S,I
	3.	Provide input into the review of the existing Services, architectural standards and project management practices for Planning and Analysis activities to ensure continuous alignment to best practice.	R, A	C,S,I
	4.	Ensure all documentation remains updated in the required ACSA format. (including but not limited to upgrade requirements, conversion requirements, design schematics and 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

Sub area	Number	Task/Activity	Provider	ACSA
	11.	Perform evaluation of new equipment considered for implementation in compliance with the ACSA's security and IT architecture policies, regulations, and procedures.	C,S,I	R,A
	12.	Define and approve any new architecture standards.	C,S,I	R,A
	13.	Conduct technical and business planning sessions to review standards, architecture, and project initiatives to align with best practises.	R,A	C,S,I
Continuous Improvement and Innovation Planning	14.	Conduct technical reviews and provide recommendations for improvements that increase efficiency, effectiveness and reduce costs.	R,A	C,I
	15.	Perform ad hoc investigations as requested by ACSA and submit recommendations for ACSA's consideration.	R,A	C,I
	16.	Conduct on-going, regular planning and recommendations for technology refresh and upgrades.	R,A	C,I
	17.	Highlight modern 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 modern 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.	R,A	C,I
	25.	Together with ACSA-IT perform feasibility studies for the implementation of new and existing technologies that best meet ACSA business needs and meet cost, performance, and quality objectives.	R,A	C,I
	26.	Review the latest technologies presented by the Service Provider.	C,I	R,A
Design and panning	27.	Develop, document, and maintain detailed technical design/engineering plans and environment configuration based on ACSA's business requirements.	R,A	C,I
	28.	Provide design documentation for yearly audits as requested by ACSA	R,A	C,I
	29.	Provide input into design plans through coordination with the appropriate ACSA technology standards groups and design architects.	C,I,S	R,A
	30.	Yearly audit of design documentation.	C,I,S	R,A
	31.	Adhere to production acceptance test criteria.	R,A	C,I
	32.	Conduct and document test plans and results.	R,A	C,I
	33.	Define and document production acceptance test criteria.	C,I	R,A
	34.	Review and approve test plans and results.	C,I	R,A

Table 15 - Roles and Responsibilities - Management, Planning, and design.

11.3 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 Align to all ACSA Project Office methodology requirements, governance, and documentation – use ACSA provided templated and naming convention.	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 16 - Roles and Responsibilities - Project Management Services

11.4 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
Demand Management	1.	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

Sub area	Number	Task/Activity	Provider	ACSA
	2.	Attend monthly review sessions to understand estimated consumption forecast where available to ensure achievement of timelines	R,A	C,I
	3.	Address any acquisition and management escalations from Service Provider	C,I	R,A
	4.	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	5.	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 business impacts	R,A	C,I
	6.	Request updates on equipment delivery timelines in the relevant meetings (project meetings etc.)	C,I	R,A
Standards Compliance	7.	Ensure that new equipment/ hardware complies with established ACSA standards and architectures	R,A	C,I
	8.	Ensure all procured hardware and software is listed as part of the ACSA architecture technology standards	C,I	R,A

Table 17 - Roles and Responsibilities - Acquisition and Management

11.5 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 documents and share folder for digital copies of the documents	I	R,A

Sub area	Number	Task/Activity	Provider	ACSA
	10.	Provide timely creation, updating, maintenance and provision of all documentation, (design documents; architectural diagrams; as built documents; test plans; all ACSA required project documentation; technical specifications, preventative and corrective maintenance plans and checklist; escalation reports; daily service request report; floor layout diagrams; OEM and third party documentation and management reporting in a form/format that is acceptable to ACSA for Service Projects and major Service activities	R,A	C,I
	11.	Manage all documentation in accordance with Configuration Management standards and guidelines	R,A	C,I
	12.	Document standard operating procedures (e.g., boot, failover/disaster recovery, backup)	R, A	I
	13.	Review and approve standard operation procedures Documentation	I	R,A

Table 18 - Roles and Responsibilities - Documentation

11.6 Roles and Responsibilities - Technology Refresh and Replenishment

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

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

Table 19 - Roles and Responsibilities - Technology Refresh and Replenishment

11.7 Roles and Responsibilities - Infrastructure Build and Change

Managing all infrastructure changes [standard, low, med, elevated 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
	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

Sub area	Number	Task/Activity	Provider	ACSA
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 (Configuration Management Database) 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 20 - Roles and Responsibilities - Infrastructure Build and Change

11.8 Roles and Responsibilities – Maintenance

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

Sub area	Number	Task/Activity	Provider	ACSA
Maintenance	1.	Define Maintenance requirements	I	R, A
	2.	Develop, document, and maintain in the Standards and Procedures Manual Maintenance procedures that meet requirements and adhere to defined policies	R, A	I
	3.	Develop Maintenance schedules (OEM recommended preventative maintenance to be considered)	R, A	
	4.	Review and approve Maintenance procedures and schedules	I	R, A
	5.	Ensure appropriate Maintenance coverage for all Service components	R, A	C, I
	6.	Provide Maintenance and break/fix support in ACSA's defined locations, including dispatching repair technicians to the point-of-service location if necessary	R, A	C, I
	7.	Perform (and/or coordinate with Third-Party Maintenance Vendor if applicable) diagnostics and maintenance on Service components, including hardware, software, peripherals, and special-purpose devices as appropriate	R, A	C, I
	8.	Perform an analysis of the impact and/or applicability of Vendor-provided (e.g., Omni) patches and/or service packs, in accordance with ACSA policies and requirements	R, A	C, I
	9.	Approve Vendor-provided patches and/or service packs	C, I	R, A
	10.	Review all patches relevant to the IT environment and classify the need and speed at which the Security patches should be installed, as defined by policies and Change Management	R, A	C, I
	11.	Install patches per ACSA's Change Management process and procedures including acquiring required ACSA approval	R, A	C, I
	12.	Install (and/or coordinate with Third-Party Maintenance Vendor if applicable) manufacturer field change orders,	R, A	C, I

Sub area	Number	Task/Activity	Provider	ACSA
		service packs, firmware, and software maintenance releases, etc.		
	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 log analysis – Continuous monitoring and responding with corrective actions to warnings and alerts. o Health Checks o Configuration Backups 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 Firmware Upgrades.	R,A	C,I
	18.	Initiate projects to execute on approved preventative maintenance recommendations	I,C	R,A
	19.	Provide detailed monthly reports on capacity, assets, changes, faults, potential risks, etc. as defined in the report schedule	R,A	C,I

Table 21 - Roles and Responsibilities – Maintenance

11.9 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 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 appointed subcontractors and Third Parties to meet Service and SLA requirements	R,A	C,I
	5.	Install, customise, and maintain the infrastructure management system for event monitoring and availability reporting.	I	R,A
	6.	Implement measures for proactive monitoring to limit infrastructure outages	I	R,A

Table 22 - Roles and Responsibilities - Infrastructure Monitoring, Operations and Administration

11.10 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

Sub area	Number	Task/Activity	Provider	ACSA
	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 optimization, and periodically provide updates to ACSA IT management	R, A	I
	18.	Ensure that all Availability Management improvement initiatives conform to defined Change Management procedures set forth in the Process and Procedures Manual	R, A	I
	19.	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 23 - Roles and Responsibilities - Project Management Services

11.11 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 operational 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, considering daily, weekly, and seasonal variations in capacity demands	R, A	I
	20.	Validate asset utilization and capital efficiency	I	R, A

Table 24 - Roles and Responsibilities - Capacity Management

11.12 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 25 - Roles and Responsibilities - Performance Management

11.13 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
Configu	1.	Define Configuration Management requirements	I	R, A

Sub area	Number	Task/Activity	Provider	ACSA
	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 26 - Roles and Responsibilities - Configuration Management

11.14 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

Sub area	Number	Task/Activity	Provider	ACSA
	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

Table 27 - Roles and Responsibilities - Asset Management

11.15 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

Table 28 - Roles and Responsibilities - Software License Management

11.16 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, 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 because of the change	R, A	I
	7.	Provide Change Management plan to ACSA for review	R, A	I
	8.	Approve Change Management plan	I	R, A
	9.	Develop and maintain a schedule of planned approved changes (Forward Schedule of Changes [FSC]) for ACSA to review	R, A	I
	10.	Coordinate, schedule, and conduct CAB meetings to include review of planned changes and results of changes made, ensuring that all appropriate parties are invited and represented in accordance with approved CAB policies	R, A	I
	11.	Participate in CAB meetings as ACSA deems appropriate or necessary	I	R, A
	12.	Provide change documentation as required, including proposed metrics as to how effectiveness of the change will be measured	R, A	I
	13.	Review and approve change documentation and change effectiveness metrics	I	R, A
	14.	Review and approve any RFC determined to have a cost, security, or significant risk impact to ACSA's IT systems or business	I	R, A
	15.	Authorize and approve scheduled changes or alter the schedule change requests as defined in the Change Management procedures	I	R, A
	16.	Publish and communicate the approved FSC to all appropriate IT and business unit stakeholders within ACSA of change timing and impact	I	R, A
	17.	Oversee the approved change build, test, and implementation processes to ensure these activities are appropriately resourced and completed according to change schedule	R, A	I
	18.	Ensure that thorough testing is performed prior to release and assess ACSA business risk related to any change that is not fully tested prior to implementation	I	R, A
	19.	Participate in business risk assessment for change to be introduced without being fully tested	R, A	I
	20.	Monitor changes, perform change reviews, and report results of changes, impacts, and change effectiveness metrics	R, A	I

Sub area	Number	Task/Activity	Provider	ACSA
	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 29 - Roles and Responsibilities - Change Management

11.17 Roles and Responsibilities - Training and Knowledge Transfer

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

- Training for the improvement of skills through education and instruction for Provider's staff. Provider will participate in any initial and ongoing training delivered by ACSA as required that would provide a learning opportunity about ACSA's business and technical environment.
- Training for ACSA-retained technical staff for the express purpose of exploiting the functions and features of the ACSA computing environment. Delivery methods may include classroom-style, computer-based, individual, or other appropriate means of instruction.
- Selected classroom-style and computer-based training (case-by-case basis) for standard COTS and Software as a Service (SaaS) applications, including new employee training, upgrade classes and specific skills.

Sub area	Number	Task/Activity	Provider	ACSA
Training and Knowledge Transfer	1.	Define Training and Knowledge Transfer requirements	I	R, A
	2.	Develop, document, and maintain in the Standards and Procedures Manual Training and Knowledge Transfer procedures that meet requirements and adhere to defined policies	R, A	C, I
	3.	Review and approve Training and Knowledge Transfer procedures	I	R, A
	4.	Develop and deliver training program to instruct ACSA personnel on the provision of Provider Services (e.g., "rules of engagement," requesting Services)	R, A	C, I
	5.	Review and approve Provider-developed training program	I	R, A
	6.	Develop, implement, and maintain an ACSA-accessible knowledge database/portal	R, A	C, I
	7.	Develop and implement Knowledge Transfer procedures to ensure that more than one individual understands key components of the business and technical environment	R, A	C, I
	8.	Provide training when substantive (as defined between ACSA and Provider) technological changes (e.g., new systems or functionality) are introduced into ACSA environment, to facilitate full exploitation of all relevant functional features	R, A	C, I
	9.	Provide training materials for ACSA technical staff for Level 1-supported applications	R, A	C, I
	10.	Provide ongoing training materials for help desk personnel on ACSA business and technical environments, as defined by ACSA	R, A	C, I
	11.	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 30 - Roles and Responsibilities - Training and Knowledge Transfer

11.18 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
Ma na ge	1.	Define Account Management requirements	I	R, A

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

Table 31 - Roles and Responsibilities - Account Management

11.19 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. 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 : o Perform event management monitoring of the Services to detect abnormal conditions or alarms, log abnormal conditions, analyse the condition and take corrective action o Manage entire Incident/Problem life cycle including detection, diagnosis, status reporting, repair and recovery o Coordinate and take ownership of problem resolution by managing an efficient workflow of incidents including the involvement of Third Party Providers (e.g., vendors). o Assign problems to L2 & L3 technical maintenance and repair staff as required o Review the state of open Problems and the progress being made in addressing these problems. o Interact on a regular basis with the IT service desk to ensure optimised efficient level of service delivery [scheduled meetings, reports, etc.]. o 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] o Manage and coordinate subcontractors and third parties in order to meet resolve Incidents/Problems o Upon rectification of the Incident/Problem, the Provider will immediately notify ACSA helpdesk that the Incident/Problem has been Resolved o Update all change configuration data bases prior to closing any call.	R, A	I,C

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

Table 32 - Roles and Responsibilities - Incident Resolution and Problem Management

11.20 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) and for ACSA Voice Network Services. ACSA applications, associated infrastructure and Voice Network 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 33 - Roles and Responsibilities - IT Service Continuity and Disaster Recovery

11.21 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 and Monitoring 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

Sub area	Number	Task/Activity	Provider	ACSA
	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 34 - Roles and Responsibilities - Service-Level Monitoring and Reporting

11.22 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 fiscal 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 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 35 - Roles and Responsibilities - Financial Management

11.23 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
Capacity Management	2.	Proactively keep the Provider informed of any requirements that would potentially impact on the Service Provider's HR resource requirements	I	R, A
	3.	Define any constraints for the use of Subcontractors	I	R, A
	4.	Approve or reject recommended Subcontractors	I	R, A
	5.	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
	6.	Analyse the impact of enhanced SLAs (if required by ACSA) on the allocated human resources and propose solution	R, A	I
	7.	Recruit and provide the human resources necessary for the performance of required Services in compliance with SLAs	R, A	I
	8.	Manage Employees time off and replacement	R, A	I
	9.	Recommend Subcontractors for delivery of Services, if applicable	R, A	I
Performance Monitoring	10.	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
	11.	Perform Annual Employee performance reviews	R, A	I
	12.	Consider ACSA satisfaction a key component of the assigned Employee performance reviews	R, A	I
Change Management	13.	On request by ACSA designate certain members of staff as Key Employees	R, A	I
	14.	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
	15.	Assign a new Provider Relationship Manager as necessary to discharge the Service Provider's responsibilities	R, A	I
	16.	Provide staff turnover data relevant to the Agreement when requested by ACSA	R, A	I
	17.	ACSA to nominate key employees where required	I	R, A
	18.	Request Provider staff turnover data when required	I	R, A
	19.	Communicate changes to internal ACSA Stakeholders	I	R, A

Table 36 - Roles and Responsibilities - Human Resources

11.24 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
	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

Sub area	Number	Task/Activity	Provider	ACSA
	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
	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 ACSA's security requirements and provide evidence of compliance	R, A	I
	44.	Periodically review equipment configurations and address any deficiencies or inconsistencies, and provide ACSA with results	R, A	I

Sub area	Number	Task/Activity	Provider	ACSA
		with detailed recommendations to remediating issues that are found		
	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
	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 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 37 - Roles and Responsibilities – Security

12.0 Service Management

12.1 Objectives

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

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

12.1.3 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 13.0 SERVICE CREDITS.

12.1.4 Provider shall provide written reports to the responsible ACSA representative regarding Provider's compliance with the SLRs specified.

12.2 Reports

12.2.1 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.

12.2.2 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.

12.3 Root Cause Analysis

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

12.4 Support Services

12.4.1 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.

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

12.4.3 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.

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

12.4.5 A superior performance on an SLA cannot compensate a substandard performance on another one.

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

12.5 SERVICE-LEVEL REQUIREMENTS (SLRs)

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

12.5.1 Review of Service Levels and KPIS

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

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

12.5.2 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: • VPNS failure affecting 1 or more sites. • Internet outage resulting in all users not being able to use internet services.
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: • Up to half of the users at a site are unable to use voice services. • Internet service is degraded at a specific site.
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: • Only single user is affected due to DNS.
Priority Level 4 — Low *Minimal Business Impact*	An incident that has minor 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: • Users cannot access and external website
Priority Level 5 — Low Impact that will take a week or two to resolve	Any services or equipment that has a minimal impact that will require a week or two to fix. • There is an issue with a secondary service

Table 38 - Priority Levels

12.5.3 **Incident management**

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

12.5.3.2 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 (temporary or permanent restoration)	<2 hours	99.0%
Priority Level 2	Time to Restore (temporary or permanent restoration)	<4 hours	99.0%
Priority Level 3	Time to Restore (temporary or permanent restoration)	<12 hours	98.0%
Priority Level 4	Time to Restore (temporary or permanent restoration)	Next business day	98.0%
Priority Level 5	Time to Restore (temporary or permanent restoration)	Next business day or as agreed	98.0%
Priority Level 1	Resolution (permanent fix)	Next business day or as agreed if next business day is not possible due to fix required	99.0%
Priority Level 2	Resolution (permanent fix)	Next business day or as agreed if next business day is not possible due to fix required	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	Next business day or as agreed	99.0%
Root-Cause Analysis	Time to Report	Within 48 hours of incident resolution	98.0%
	Formula	Number of tasks completed within Performance Target	
	Measurement Interval	Monthly	
	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 39 - Incident management response and resolution times for International Airports (Operational Hours)

Incident management response and resolution times for International Airports (After hours Hours) and local airports All 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)	<3 hours	99.0%
Priority Level 2	Time to Restore (Not linked to hardware failure)	<5 hours	99.0%
Priority Level 3	Time to Restore (Not linked to hardware failure)	<12 hours	98.0%
Priority Level 4	Time to Restore (Not linked to hardware failure)	Next business day	98.0%
Priority Level 5	Time to Restore (Not linked to hardware failure)	Next business day or as agreed	98.0%
Priority Level 1	Resolution (permanent fix)	Next business day or as agreed if next business day is not possible due to fix required	99.0%
Priority Level 2	Resolution (permanent fix)	Next business day or as agreed if next business day is not possible due to fix required	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	Next business day or as agreed	99.0%
Root-Cause Analysis	Time to Report	Within 48 hours of incident resolution	98.0%
	Formula	Number of tasks completed within Performance Target	
	Measurement Interval	Monthly	
	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 40 - Incident management response and resolution times for International Airports (After hours Hours) and local airports All hours

Availability Management for JNB, CPT, DUR, PLZ							
Availability	**Service Measure**	**Performance Target**	**Wan SLR Performance %**	**Corporate Internet SLR Performance %**	**Public Internet SLR Performance %**	**Voice Services SLR Performance %**	**Point to Point SLR Performance %**
System Availability	Availability %	>	99.9%	99.9%	98%	99.9%	99,9%
	Formula	Downtime in minutes /total minutes per month					
	Measurement Interval	Monthly					
	Reporting Period	Monthly					
	Measurement Tool	Availability reports provided by the service provider and verified by ACSA.					
	SLR Element Weighting Factor Allocation	50%					

Table 41– Availability management - JNB, CPT, DUR, PLZ – (All Hours)

Availability Management for GRJ, KIM, BFN and UTN							
Availability	**Service Measure**	**Performance Target**	**Wan SLR Performance %**	**Corporate Internet SLR Performance %**	**Public Internet SLR Performance %**	**Voice Services SLR Performance %**	**Point to Point SLR Performance %**
System Availability	Availability %	>	99.5%	99.5%	98%	99.5%	99,5%
	Formula	Downtime in minutes /total minutes per month					
	Measurement Interval	Monthly					
	Reporting Period	Monthly					
	Measurement Tool	Availability reports provided by the service provider and verified by ACSA.					
	SLR Element Weighting Factor Allocation	50%					

Table 42– Availability management - GRJ, KIM, BFN, ELS and UTN– (All Hours)

Performance Management			
Performance	**Service Measure**	**Performance Target**	**SLR Performance %**
SIP trunks	Jitter	<= 35ms	99.5%
WAN optical fibre	Response time	<= 50ms	99.5%
WAN Microwave	Response time	<=75ms	99.5%
	Formula	Downtime in minutes /total minutes per month	
	Measurement Interval	Monthly	
	Reporting Period	Monthly	
	Measurement Tool	Performance report provided by the service provider and verified by ACSA.	
	SLR Element Weighting Factor Allocation	50%	

Table 43– Performance management

12.5.4 Service requests.

System Administration Service-Level Requirements			
System Administration Task	**Service Measure**	**Performance Target**	**SLR Performance %**
Add new IP range to network routing table	Elapsed Time	Within 16 hours (in business hours)	98.0%
Install FTTH service	Elapsed Time	Within 5 Working Days from quote approval	98.0%
Increase bandwidth	Elapsed Time	Within 16 hours (in business hours) from quote approval	98.0%
	Formula	Number of tasks requests within Performance Target	
	Measurement Interval	Measure Monthly	
	Reporting Period	Report Monthly	
	Measurement Tool	Data from ACSA Service management Tool (Service NOW) complimented with other Provider tools if applicable	
	SLR Element Weighting Factor Allocation	30%	

Table 44 - Service requests SLR

12.5.5 Configuration management

12.5.5.1 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.

12.5.5.2 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 CMDB 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:	**Manual Checks**
SLR Element Weighting Factor Allocation	20%

Table 45 - Configuration Management SLR

12.5.6 Software/Firmware Refresh

Software refresh for all upgrades and new releases.

Software /firmware Refresh Service-Level Requirements			
Software Refresh	**Service Measure**	**Performance Target**	**SLR Performance %**
Notification of vendor Software upgrades and new releases	Response Time	Within 30 days after Software vendor announcement	95.0%
Implementation of service packs and updates to "dot" releases	Response Time	Within 60 days after approved by Client	95.0%
Implementation of version or major release updates	Response Time	Within 120 days after approved by Client	95.0%
	Formula	Number of requests completed on time ÷ Total of all requests occurring during Measurement period	
	Measure Interval	Measure Quarterly	
	Reporting Period	Report Quarterly	
	Measurement Tool	Electronic audit, conducted quarterly from date of contract commencement	
	SLR Element Weighting Factor Allocation	5%	

Table 46 - Software/Firmware Refresh SLR

12.5.7 Project Management

Project tasks during installations and changes

Project Tasks Service-Level Requirements			
Project Tasks	**Service Measure**	**Performance Target**	**SLR Performance %**
Any task as defined in the project schedule	Completion time	Within agreed deadline on project plan	99.0%
	Formula	Number of tasks completed on time ÷ Total of all tasks on project plan	
	Measure Interval	Monthly	
	Reporting Period	Monthly	
	Measurement Tool	Agreed upon project plan	
	SLR Element Weighting Factor Allocation	50%	

Table 47 – Project Tasks SLR

12.5.8 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 48 - SLA Measurement Exclusions

13.0 SERVICE CREDITS

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

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

13.1 Principles

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

13.1.1 Service Credits only occur because of Service Level Failures.

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

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

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

13.1.5 A superior performance on a SLR cannot compensate a substandard performance on another one.

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

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

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

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

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

13.2 **Definitions**

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

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

13.2.3 **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.

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

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

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

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

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

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

13.3 **Methodology**

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

13.3.1.1 **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 costs should the ACSA tools not be enough.

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

13.3.1.2 **Reports**

The Service Provider shall report to ACSA its performance of the Services against each SLR monthly 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) (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.

13.3.1.3 **Root cause analysis**

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

13.3.2 **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.

13.3.3 **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.

13.3.4 **Several service level failures**

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

13.3.5 **Successive service level failures**

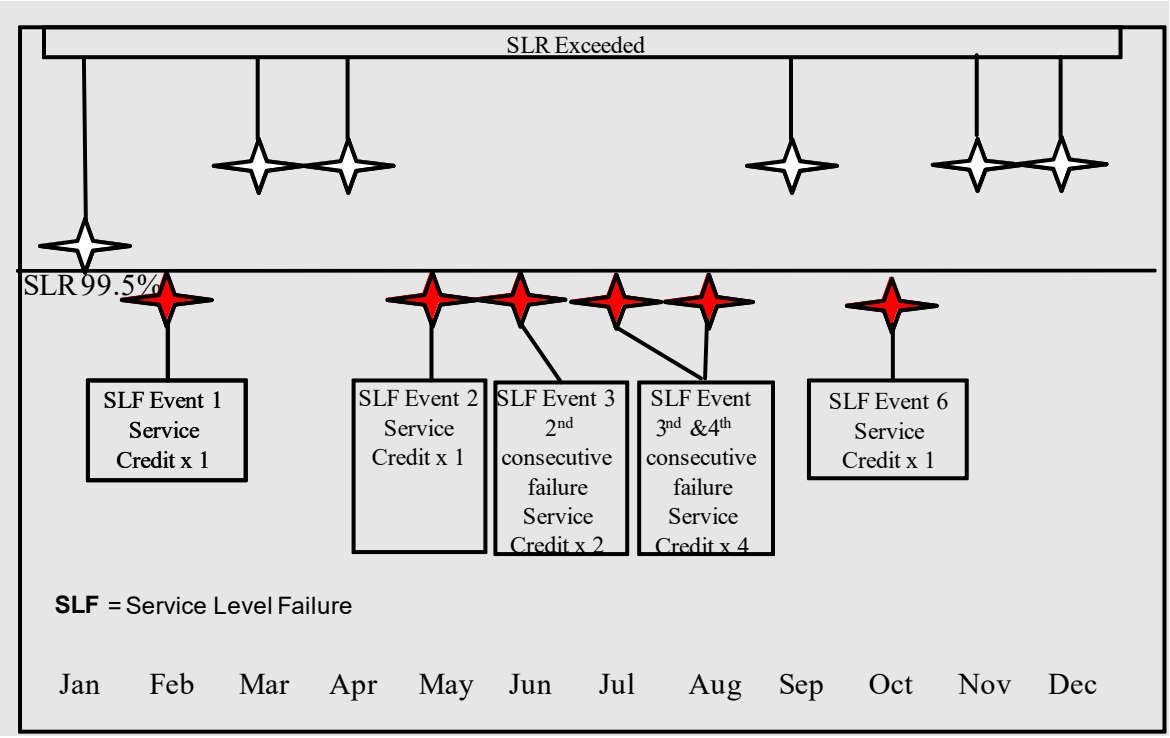
If a Service Level Failure with respect to a given Service Level recurs in consecutive Measurement Intervals, the amount of the applicable Service Credit payable to ACSA shall be multiplied by the following factors for subsequent Measurement Intervals:

(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



13.3.6 **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.

13.3.7 **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.

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

13.3.9 **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 period.

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

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

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

13.4 Changes to performance measurements

13.4.1 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.

13.4.2 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.

13.4.3 Deletions

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

14.0 Meetings and Report Requirements

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

14.1.1 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.

14.1.2 **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.

14.1.3 **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 Project status update	ACSA-IT PM (chair)	· Minutes of meeting
	ACSA-IT Engineer	· Updated project schedule
	Provider Senior Site Manager	· Action register for any open actions to be addressed
	Provider Project Manager	· Risks and Issues register
	Provider administrator	
Monthly Care Review	Operations Manager (chair) ACSA-IT Engineer	· Minutes of meeting
	Provider Senior Site Manager	· Action register for any open actions to be addressed
	Provider relationship Manager	· Risks and Issues register
	Provider administrator	· Service Credit Report
Quarterly review meeting	Operations Manager (chair) ACSA-IT Engineer	· Minutes of meeting
	Provider Senior Site Manager	· Action register for any open actions to be addressed
	Provider Relationship Manager	· Risks and Issues register
	Provider administrator	
	Senior Manager IT Infrastructure	
Annual review meeting	Operations Manager (chair) ACSA-IT Engineer	· Minutes of meeting
	Senior Manager IT Infrastructure	· Action register for any open actions to be addressed
	Provider Senior Site Manager	· Risks and Issues register
	Provider Relationship Manager	
	Provider administrator	
	Senior Manager IT Infrastructure	

Table 49 Meetings definitions

Frequency	Report Name	Report Content	Due date	Submit to	Format	Meeting Name and frequency
Daily	Fault Summary if there outstanding faults	Reported faults summary (resolved and outstanding)	Start of business every date	ACSA Technical Lead	Email written report summary with supporting tables.	Weekly Service Review
	Fault Summary escalation if there outstanding faults	Outstanding faults and notification	Start of business every date	ACSA Technical Lead	Email written report summary with supporting tables.	Weekly Service Review
	Re-opened fault summary if there outstanding faults	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
	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
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	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

Frequency	Report Name	Report Content	Due date	Submit to	Format	Meeting Name and frequency
	Asset Data	Asset Register	3 days before monthly account meeting	ACSA Technical Lead	Email Excel document	Monthly Care Review
	Areas of concern	Testing done on Print Services highlighting areas of concern. Weekly to review previous weeks' reports	3 days before monthly account meeting	ACSA Technical Lead	Word/Excel	Monthly Care Review
Quarterly	Stock levels	BOM register documenting stock levels on hand	3 days before quarterly review	ACSA Technical Lead	Email Excel document	Quarterly review meeting
	Contract appendix review	Review updates to contract appendixes are completed	3 days before Quarterly review meeting	ACSA Technical Lead	Email PDF document	Quarterly review meeting
	Baseline (CMDB) information	Review updates to Baseline CMDB	3 days before Quarterly review meeting	ACSA Technical Lead	Email Excel document	Quarterly review meeting
	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	3 days before annual	ACSA Technical Ops manager	Email PDF document	Annual review meeting

Frequency	Report Name	Report Content	Due date	Submit to	Format	Meeting Name and frequency
		adherence thereof	review meeting			

Table 50 Reporting table

15.0 General Requirements

15.1 No parts of the scope are guaranteed to be executed and there is no minimum term for any part that is executed. ACSA may choose to implement any part during the term of the contract and all services will end together after the contract term of 84 months.

15.2 The service provider is obligated to deliver any service that they have quoted for, should it be requested by ACSA. Penalties will apply if the service provider is unable to deliver services.

16.0 Transition Requirements

16.1 Provide a detailed Transition plan that covers the below sections:

- Transition Organization structure
- Key Roles and responsibilities
- Work Breakdown Structure
- Communication plan
- Estimated Timetable
- Documentation schedule

17.0 Important Information

Please note that this Statement of Work document will form part of the contract and the service provider is obliged to meet all the requirements stated above. Please take note of the below critical requirements to deliver the service.

Key Items	
1	All WAN, Voice and Corporate services must be fully redundant at all sites and have diverse geographical Point of Presence
2	All infrastructure required for the solution whether MPLS or SDWAN, will be provided by the bidder at its own cost, and fully compatible with ACSAs existing infrastructure.
	There must not be any dependency on running open standard routing protocols like BGP or OSPF between ACSA's branches/offices and PE Routers of the Bidder. The Bidders MPLS VPN or SDWAN network should also support multicast traffic in all variants. ACSA should be free to use any LAN IP schema throughout the bidder's MPLS VPN or SDWAN if it is unique in ACSA's network. WAN IP Schema will be mutually agreed with the selected bidder. The Bidder should be able to route ACSA's LAN subnets, loopback in their MPLS VPN or SDWAN and support any routing protocols (static/dynamic) preferred by ACSA.

3	The solution must provide monthly uptime for WAN, Corporate Internet, and Voices services of 99.9% for the following sites on 24x7x365 basis. JNB, CPT, DUR, PLZ and ELS and 99.5% for the following sites on 24x7x365 basis. GRJ, KIM, BFN and UTN
4	If the service provider misses any committed timelines for project implementations required for the initial delivery of services, all associated costs incurred by ACSA to continue with the existing services, will be passed onto the new service provider
5	Any of ACSA's network segments should be securely reachable directly from any other ACSA's location through the service providers MPLS VPN or SD-WAN network, via the shortest path within the service providers network and not have to traverse a central ACSA site.
6	The service providers must ensure that the latency between any two ACSA premises should be less than the following with and without load: The Bidder must ensure that the latency between any two ACSA premises should be less than the following with and without load: • 50 ms. - Optical fibre circuit • 75ms. - Microwave
7	The bidder must be able to provide a minimum of 1Gbps direct fibre links between OR Tambo International Airport and Cape Town International Airport. The links should be fully redundant and follow different geographical routes. There should be no single point of failure between the 2 routes. The fibre must be terminated at the ACSA location points provided
8	Service provider will host DNS, PTR and MX records for ACSA owned domains.
9	The service provider must be able to route ACSA owned public IP address ranges over the internet to the ACSA local network.
10	The service provider must own or be able to port all ACSA existing number ranges, as per Annexure D.
11	Service provider to integrate with MS Teams through direct routing or similar, to allow ACSA users to make and receive PSTN calls via MS Teams. There should be no additional charges for this as it needs to be integrated into the pricing.
12	The service providers must be able to replace the existing FTTH, FTTB and LTE services that are in use, as per the locations in Annexure E, within the 12-week period.
13	All pricing in the pricing file is to be inclusive of installation, rental charges and CPI.
14.	Please note that all bandwidth figures are preliminary and may be subject to reduction or increase at the time of contract finalization, depending on our evolving business needs and internal assessments
15	**Bidders must assume that they have no existing network infrastructure on site when preparing their pricing. All costs should be based on delivering a full solution from scratch.** **If the winning bidder has existing infrastructure that could be used, this will be discussed during contract negotiations and may be used to adjust the final price, as long as:** **• The infrastructure is proven to be owned and in good condition** **• It meets all technical and service requirements**