Annexure A

Scope of Work

For

Enterprise Applications Managed Services

Bid Number COR6727/2021/RFP

Description: Request for Proposal for the Enterprise Applications Managed Services a Period of 60 months to Airports Company South Africa.

CONTENTS

TABLES

1.0 ENTERPISE APPLICATIONS MANAGED SERVICES SCOPE OF WORK OVERVIEW AND OBJECTIVES

1.1 Background

The Enterprise Applications Division within ACSA IT is responsible for the development and maintenance of Enterprise Applications within the organisation to achieve ACSA's strategic objectives, and ensure that targeted benefits are achieved, this is done while managing the constraints imposed by ACSA's leadership and external factors.

The Bidder must work as a "Managed Services Provider (MSP)" for ICT Applications Development, Support and Maintenance and provide the services as described in this Scope of Work to ACSA, including any additional services that the Bidder has committed to provide during the contract term. The services include all support functions, tasks and responsibilities as accepted by the Bidder.

The MSP must manage and perform the services seamlessly by function regardless of technology platform and must do so using Information Technology Infrastructure Library (ITIL) practices and continuous improvement processes.

The MSP is expected to manage and resolve incidents, service request logged by end-users according to the agreed service levels. It is the responsibility of the Service Provider to ensure that incidents are categorised properly and resolved in accordance with the ACSA change management process. The MSP must provide the services described in this Scope of work (SOW) as they evolve and change during the contract term, through the change control process. This may include modifying, changing, replacing, supplementing, and enhancing the support services over time. Furthermore, problem management must form part of incident resolution strategy and recurring incidents are logged in the problem register and root cause analysis is performed and reported regularly as agreed with ACSA.

The MSP must ensure that the environments are stabilised and improvements on system availability is tightly managed. The number of incidents logged per month will be used as an indicator of environments stability and service improvement. Moreover, end-user surveys must be conducted on a regular basis and the survey outcome/feedback shared with the IT Enterprise Applications Management team.

Service level and management meetings must be scheduled by the MSP with the IT Enterprise Applications Management team. The objective of this meeting is to provide feedback on the performance and to discuss areas of improvement or concerns that require escalation.

The MSP is responsible for ensuring that end-user satisfaction is continuously improving, and that training is conducted on a regular basis and on a need basis. The purpose of the end-user training is to encourage system utilisation, accurate execution of system processes and system adoption.

The MSP bidder must also ensure that change management forms part of service level management. The purpose of change management is to improve adoption of new changes and meaningful engagement of end-users regarding proposed and implemented changes. The services described in this SOW are intended to be comprehensive, but are not all-inclusive in describing the activities, resources, or other details necessary for the proper performance of the support services.

Objectives of the Enterprise Applications Managed Services RFP

The purpose of this RFP is to inform prospective Bidders as to the requirements of the appointment of an entity to provide managed services to ACSA for:

- **Tower: 1 Applications Support and Maintenance**
- **Tower: 2 Ad hoc Systems Development and Configuration Services (Dev- Ops Framework)**

Furthermore, the Bidder must provide and fulfil the following requirements to be competent in the bidding process:

- Provision of trained and experienced professionals in supporting the specified applications environments (Application Support and Maintenance)
- A support methodology that provides efficiency and high-quality services.
- A structured support approach based on **off-site** support staff.
- Availability of support skills up to a 24 x 7 x 365 service offering as specified in the service requirement that includes resources on standby/on-call.
- Provisioning of emergency after-hours support as specified in the service requirement.
- A design methodology that provides efficiency and high-quality services.
- A development methodology that provides efficiency and high-quality services and
- Provisioning of additional resources on Time & Material basis for identified and agreed adhoc demands and projects with a flexible model.

ACSA places strong emphasis on Quality to minimise systems downtime and repeated incidents. ACSA expects that the MSP's Service Management Processes and Tools are aligned to ITIL standards to manage Incidents, Problems, Change, Demand and Release management.

Key Drivers

- Cost optimization (lower support costs while maintaining quality)
- Increased availability (less downtime)
- Lower latency (improved Quality of Service [QoS])

- Ability to add and change capacity to support internal business processes (scalability)
- Adoption and consistency of global processes (improved response times and faster resolution times)
- Offload routine enterprise applications maintenance and support tasks to the MSP (focus on core competencies, focus on strategic initiatives).
- Where customization is necessary to meet business needs, ACSA IT should play a leading role in ensuring that such customizations undergo appropriate governance and project management processes.

1.1.1 Tower:1 – Applications Support and Maintenance

This Service is intended to provide Support, Maintenance and Development of all applications in operational use listed in the Applications Service Catalogue, and which come under the responsibility of the ACSA IT Operations. Work performed by this service will be expected to adhere to the ITIL Service Management processes in place and be fully integrated into the existing service desk processes and tools.

The scope of the potential Applications Support, Maintenance and Development Services is to provide a contract to a potential bidder that meets the requirements stipulated in the Requirements listed below. Potential bidders in their responses are expected to demonstrate their ability to meet the requirements stipulated and should provide relevant references and methodologies to be adopted that suit the ACSA IT.

Following is the list of requirements as part of the scope to be included but not limited to:

- Incident, Service Request, Problem, Change and Release management along with reporting.
- Monitoring, maintenance and support of systems and services, which include patch management.
- Configuration, Installation, Testing and Upgrades of existing systems and services.
- Installation of fully tested patches, firmware and minor upgrades to all environments in scope.
- Maintenance Services which include corrective and preventive maintenance.
- Work with business analysts, system architects, designers, developers and contractors/3rd party vendors to support the implementation of configuration changes and upgrades.
- All new enhancements and requests based on the applications in this scope of work
- Release planning and deployment support.
- Adherence to change management principles and procedures.
- Adherence to and implementation of Integration standards and methodologies.
- Maintenance, Testing and validation of Backup & Restore procedures/schedules.
- Testing and support of Disaster Recovery and Business Continuity process as per ACSA schedules.
- Testing support during projects, business related changes and for operational purposes; and
- Ad-hoc report generation and database queries.

For all second level support, including break-fixes and database corrections, ACSA would expect to establish Service Level Agreements (SLAs) with the appointed MSPs in order to have a predictable level of service to the user community.

All the minor Change Requests (CRs) shall be completed within the Applications Support and Maintenance services agreement. This will include data correction fixes where minor code change is required to resolve the specific incident while correction of the root cause is more likely to require a more significant change, which would be handled by a formal CR process and associated SOW under Applications Development services. For the purpose of the scope of work, a minor change request is defined as a change that requires maximum 5 days (40 hours) development effort.

Value Added Services

In addition to providing the expected level of quality for Applications Support & Maintenance and Development activities, the following items should be part of the proposal as a value-added service:

- Best practices and processes in line with the global ITIL standards across the applications landscape in scope
- Introduction of new Ways of Working in the areas of Support, Maintenance, Development and Implementation methodologies e.g., Agile, Scrum etc.
- Implementation of tools and techniques in the areas of Digitisation, Automation and Artificial Intelligence at various stages of application life cycle.

Pricing quotation must include both the Applications Support and Maintenance and Value-Added services.

Additionally, the bidder needs to bring in the industry best practices/standards in providing the necessary support and maintenance for Airport Applications Support & Maintenance in particular.

1.1.2 Tower:2 – Ad Hoc Systems Development and Configuration

This service is intended to provide development services for all new applications that have been approved through the ACSA IT Governance processes. Additionally, it will provide development support for all existing applications based on approved Change Requests and signed SOWs. When complete, new service applications/services/packages will be transitioned into production use and passed to the Applications Support and Maintenance Services team. A clear and concise transition and handover plan of completed development work should form part of the bidder's response in Tower 2.

Following is the summary scope of work included but not limited to for this tower.

- Technical design, development and testing of critical fixes, changes and new projects
- Development of new interfaces and services

- Adherence to change management principles and procedures.
- Adherence and implementation of development standards and methodologies
- Process and code reverse engineering
- Code deployment and source code management
- Testing (Unit, System, Integration, Penetration and Stress testing) including test strategy and plans
- Defect management
- Estimations on time and cost for all new developments and approved changes
- Systems configuration for all applications in this scope of work

For all future applications development and configuration work including any non-fix enhancements to existing applications, ACSA will issue a Statement of Work (SOW). Once ACSA and the MSP have agreed on the scope of the work, the MSP will be expected to provide a "Fixed Price and Schedule" offer based on a pre-agreed standard rate card and then deliver, based on the agreed deliverable and time-lines. For smaller pieces of work, the MSP will be expected to use ACSA approved Change and Release Management process, while for more significant work the established ACSA project methodology will be applied.

ACSA IT as part of its continuous innovation is looking to implement the DevOps (CI-CD) set of practices that combines software development and information-technology operations, which aims to shorten the systems development life cycle and provide continuous delivery with high software quality. Bidders must provide a strategy to implement the DevOps chain for all the development opportunities within the scope of applications. Also, there is a need to provide a roadmap to extend this to the entire IT landscape across ACSA with provision of further maintenance & support. The pricing proposal must include quote for this along with the mandatory applications and tools that are intended to be included to achieve optimum DevOps goals. This tower will be executed at ACSA's discretion based on availability of funds. Applications Development work will be demand driven and is difficult to predict in advance. Hence, the MSP must provide the most cost-effective offer based on the resource availability for this area of work.

NB: Please take note that all other services and expectations listed in this document are part of the scope of work. The services that are not part of this scope of work are explicitly mentioned under section 9.0 "Out of Scope".

2.0 SERVICE ENVIRONMENT

2.1 Scope of Applications to be Supported

2.1.1 Oracle

ACSA has implemented several modules within the Oracle e-Business suite. The current e-Business suite Application version is R12.1.3 and the database version is 12c. The Linux server (Redhat) is on version 7. Furthermore, ACSA has implemented Oracle Business Intelligence application and the current version is 11X.

The current version (12.1.3) is reaching end of life in December 2021. ACSA has, in order to maintain its premium support, started a project to upgrade the current version to version R12.2.9. This project should be completed before the current version expires. Therefore, the support services will be on R12.2.9, which includes SOA and WebLogic capability.

Number of Instances in Production and at Disaster Recovery site for all application:

Production Instance - 8 Servers

Oracle Enterprise Resource Planning (ERP) - 1 DB 1 App
Business Intelligence (BI) - 1 DB 1 App
Enterprise Performance Management (EPM) - 1DB 2 App
Connect Direct - 1 App

Disaster Recovery - 1 Server

1 DB and App

The following are the Oracle ERP product suite that have been implemented and migrated to Production. Application Support and Maintenance will include these but not limited to.

HUMAN RESOURCES (HR)

- HR Core
- HR Self-service
- HR Payroll
- HR Compensation Workbench

Cloud Services:

- Taleo Recruit
- Fusion Performance Management

FINANCE

- Account Receivable
- Accounts Payable
- General Ledger
- Cash Management
- Treasury Management
- Fixed Assets
- Hyperion Financial Management
- Project Costing

Cloud Services

- Planning and Budgeting Cloud Services
- Enterprise Performance Reporting Cloud Services

SUPPLY CHAIN MANAGEMENT (SCM)

- Procurement
- i-Procurement
- i-Supplier
- Contracts Management

ASSET MANAGEMENT

- Enterprise Asset Management
- Property Management

BUSINESS INTELLIGENCE

- All Modules

Historical Support Incidents and Service Requests Trend

Oracle environment is stable and in good management patch level (n-1 approach). However, there are incidents and service requests that are logged from time to time by the end-users. Incidents and service requests are summarised in the table below.

Table 1 – Annual Historical Support incidents and Service Request Trends : Oracle

Oracle Module	Number of users per module	Number of Requests per year	Number of Incidents per Year
Oracle Fixed Assets	63	76	196
Oracle Projects	136	38	162
Oracle Procurement	843	34	187
Oracle Accounts Payable	124	64	187
Oracle Cash Management	50	21	56
Oracle Payments	6	32	32
Oracle Property Manager	30	61	117
Oracle EAM	237	26	79
Oracle Business Intelligence	56	41	48
Oracle EBS Payroll	3255	69	410
Oracle EBS Human Resource	3255	43	223
Oracle Fusion Talent	3255	27	104
Oracle Taleo Recruit	3255	35	349
Oracle Taleo Learn		25	71
Planning and Budgetting Cloud Services	360	63	52
Oracle Accounts Receivable	110	79	163
Oracle General Ledger	106	12	51
Oracle Iexpense	3255	53	116
Total Number of calls per year		**1027**	**3352**

It is the responsibility of the MSP to ensure that incidents are minimised or reduced over time by providing training and performing necessary system maintenance and enhancements. The MSP is expected to manage minimum of 20 enhancements per year as part of the Applications Support and Maintenance service contract.

Skills required to support ORACLE Environment.

Each technical resource must display certain skill sets and demonstrate the ability to perform certain functions and/or take responsibility for certain actions. This level of expertise should be based on the resources' experience

on providing such support functions in similar projects/assignments with other clients (ACSA can be added as additional reference). Through possessing the relevant qualifications and experience, the resource must demonstrate a good level of understanding of the following skills and accountabilities: (please note that these skills are set out as a guide only and should not be viewed as exhaustive, Bidders are encouraged to provide their own descriptions of the skills set according to the resources level of skill, if applicable).

Oracle Specialisation	**Minimum Skill Set**
Oracle Functional Specialist	• Extensive knowledge of Oracle/Business best practice business processes • Extensive knowledge of business requirements gathering • Extensive knowledge and experience of Oracle implementation • Extensive knowledge of Oracle support and module enhancement • Extensive experience and knowledge of functional design documents • Working knowledge of Oracle Service Request Management process • Working knowledge and experience of Change Management process • Working knowledge of testing Oracle modules including but not limited to test script drafting • Extensive experience and knowledge of end-user training • Working knowledge of Oracle implementation methodology (OUM/AIM)
Oracle Database Administrator	• Extensive experience and knowledge of Installation, upgrades, and manage services in Application (R12) and Database (12c) • Working experience of AD utilities • Knowledge of and ability to clone Production to other non-production systems • Extensive experience and knowledge of Concurrent managers • Ability to Backup and clean up various log files on the application • Working knowledge of Networks, Security, Storage and Oracle Infrastructure. • Extensive knowledge of database and application tuning • Working experience of release and change management • Ability to manage and optimise Storage • Ability to ensure system audit compliance

	• Working experience of script writing for custom scripts • Working knowledge and experience of Dataguard • Working experience of OBIEE, WebLogic, SOA, OEM, ODI, UPK • Extensive knowledge of Installation, patching, monitoring Oracle databases • Ability to monitor, and verify backups and perform ad-hoc backups • Working experience of script writing for data extraction, transformation, and loading • Ability to perform routine security and authentication measures. • Extensive knowledge and working experience of database upgrade execution • Ability to write and interpret SQL queries. • Extensive knowledge and working experience of database lock, space management, export and import of the database • Ability to install, configure, and maintain the Linux servers on a Virtual Machine Infrastructure • Extensive knowledge of Linux systems upgrade execution
Oracle Developer	• Extensive experience and knowledge of writing PL/SQL in Oracle 11g/12c. • Development of reports for Human Resource, Projects and Financial modules in Oracle E-Business Suite R12. • Extensive knowledge and ability to create .rtf and e-text templates in oracle BI Publisher • Ability to define concurrent requests • Extensive experience in design and document modules implemented changes, design review and assistance to be provided by systems analyst and architects • Participation in workshops to determine overall functional design. • Extensive knowledge of version control • Extensive experience in supporting existing systems by investigating, identifying and rectifying problems • Ability to investigate & correct data problems as per data fix policy • Ability to test, debug and quality assure programmed code to ensure that unit testing is conducted successfully accordingly to the functional specification document, user requirements and test pack • Extensive knowledge of Application Extensions/Customisations via Oracle Applications Framework (OAF) • Working knowledge of coding standards

Oracle Business Intelligence	• Extensive experience of Oracle OBIEE reporting tools with solid reporting experience (Dimensional Modelling and OBIEE RPD development OBIEE Answers, Dashboards, Publisher, Delivers Understanding) • Extensive knowledge of OBIEE Repository Development • Extensive experience of using ETL tools - preferably Oracle's ODI product • Working knowledge and extensive experience of Oracle PL/SQL and SQL • Working experience of version control • Extensive experience in supporting existing systems by investigating, identifying and rectifying problems • Ability to investigate & correct data problems as per data fix policy • Investigation & correction of data problems as per data fix policy. • Working experience and ability to perform testing, debugging and to quality assure programmed code to ensure that unit testing is conducted successfully accordingly to the functional specification document, user requirements and test pack • Working knowledge of coding standards
Oracle System Administrator	• Experience in task and resource coordination • Extensive knowledge and ability to troubleshoot problems and resolve application issues within pre-defined SLA requirements • Working experience and capability to analyse logged support incidents, identify gaps in training and support functions and identify solutions • Extensive knowledge of root cause analysis and problem management • Ability to manage relationships with third level support team to ensure the efficient resolution of issues including the logging, follow-up and feedback to clients • Ability and knowledge of service level agreement management • Ability to manage and report on overall compliance to core governance processes, policies and procedures • Working experience of managing and coordinating both internal / external audit related matters • Working experience and ability to assess and manage system operations risks • Working experience and knowledge of managing and coordinating risk register

	• Ability to execute, analyse reports and reconcile data to highlight risks, issues, misuse of the system and general non-compliance to defined processes • Working knowledge and experience of relevant and applicable legislative requirements pertaining to Oracle applications • Working experience and knowledge of security compliance • Ability to manage and monitor IT security standards and best practice execution • Working experience to execute IT security activities within the environment • Extensive knowledge of user access management to ensure complies with data protection and company data security policies

2.1.2 **IBM SUITE SERVICES**

- **IBM INTEGRATION BUS**
- **IBM Power 8 AIX**
- **IBM DataPower**
- **IBM Message Queuing (MQ)**

Historical Support Incidents and Service Requests Trend

The IBM ESB environment is highly stable. However, due to the nature and agility of airport business integration requirements/requests are frequently requested in order to keep the Airport Management Operations running smoothly and accurately at all times. This environment is a real-time environment, which requires above average system availability, and the resources are expected to be available 24/7 including after hours and during holidays period.

Table 2 – Historical Support incidents and Service request Trends: IBM Suite

ESB Module	Category of Users	Number of Requests per Year	Number of Incidents per Year	Number of Changes All Airports
2DBC	Airport Operations including Airlines	3	4	3
Zeus	Airport Operations including Airlines	0	10	0
Apex	Airport Operations including Airlines	5	15	5
AMS	Airport Operations including Airlines	20	7	15
SAC	Airport Operations including Airlines	0	3	
Other (Active Directory, Firewall, Security, Network, Desktop Applications)	Airport Operations including Airlines	7	1229	7
Total Number of calls per year		**35**	**1268**	**30**

Skills required to support IBM Environment.

Each technical resource must display certain skill sets and demonstrate the ability to perform certain functions and/or take responsibility for certain actions. This level of expertise should be based on the resources' experience on providing such support functions in similar projects/assignments with other clients (ACSA can be added as additional reference). Through possessing the relevant qualifications and experience, the resource must demonstrate a good level of understanding of the following skills and accountabilities: (please note that these skills are set out as a guide only and should not be viewed as exhaustive, Bidders are encouraged to provide their own descriptions of the skills set according to the resources level of skill, if applicable).

IBM Focus Area	Minimum Skill Set
IBM Power 8 AIX	• Extensive technical knowledge and working experience in Windows Server, Linux and Unix Operating systems • Extensive technical knowledge and working experience in Working experience of AIX server technology • Knowledgeable about the networks • Extensive technical knowledge and working experience in setting up IBM stack such as Integration Bus, IBM MQ and IBM DataPower servers • Extensive knowledge and ability to configure and manage storage, switches and controllers on servers • Extensive knowledge of scripting background for server administration • Working knowledge and ability to upgrade IBM software stack and monitor and manage IBM licences • Ability to perform backup and restore of the IBM and other software stacks • Working knowledge and understanding of database administration such Oracle, PSQL, MSSQL and Mongo DB
IBM DataPower	• Extensive knowledge of the IBM appliance technology • Working experience of and understanding the SOA architecture and where IBM DataPower fits in in the SOA and ESB architecture • Extensive knowledge and working experience of IBM DataPower administration • Extensive knowledge and working experience IBM DataPower development patterns • Extensive knowledge and working experience IBM DataPower security and administration especially running the commands on the CLI • Knowledgeable about Firewall and Networking

	• Extensive knowledge and ability to expose ports and to test connections with the stakeholders connecting via IBM DataPower • Extensive knowledge f and working experience in IBM DataPower capabilities and IBM integration Bus • Knowledgeable about the use of IBM DataPower as an integration solution • Extensive knowledge and working experience of backup and restore DataPower appliances. • Knowledgeable about Load balancing on the appliance
IBM MQ	• Extensive knowledge of Message queueing • Working knowledge and understanding of Queue Manager Cluster • Working experience of SSL to secure the MQ channels and Extensive knowledge and working experience of Queue Manager. • Extensive knowledge and working experience of MQ firmware upgrade and restoration. • Ability to run MQ commands on the MQ cli
IBM Integration Bus (IIB)	• Extensive knowledge and background on the development/implementation of the MQ bases messages flows with sequencing on the messages. • Working knowledge of developing and securing API solutions in Integration Bus • Extensive knowledge and working experience in Message routing and filtering. • Understanding and ability to implementation of Common logging and exception handling in IBM Integration Bus and IBM DataPower • Extensive knowledge and working experience of HTTPS, FTPS and MQ protocol • Extensive knowledge and working experience ESQL mapping patterns and standards for message transformation. • Ability to implement SOAP webservices in IBM Integration Bus • Ability to diagnosis Error messages in IBM integration Bus • Extensive knowledge and working experience on how to setup configurable service in IBM integration Bus • Understanding of what a contract is in IBM Integration Bus

	• Extensive knowledge and working experience of how IBM Integration bus, IBM MQ and IBM DataPower interconnect and exchange message in the enterprise service Bus

2.1.3 MICROSOFT SHAREPOINT AND OTHER

ACSA has developed and implemented custom SharePoint applications across the organisation. The organisation's Intranet is based on the SharePoint capabilities and BindTuning capability. The SharePoint environment is a hybrid environment i.e. some applications run on the On-Premises environment and others on the Microsoft Cloud services. The current MS SharePoint version is SP server 2013, SLQ server version 11.0.6020 and SharePoint Online with PowerApps, Power BI and MS Flows. Nintex Forms and Workflows are used to complement the MS SharePoint applications. There is a planned upgrade of MS SharePoint from the current 2013 to 2016 or later version. Therefore, the support and maintenance will initially be on 2013 version and later transitioned to 2016 or later version.

SharePoint in ACSA is integrated with NINTEX software to achieve automation of projects that require workflows, forms and mobile applications. ACSA currently is licensed with NINTEX forms, workflow and mobile.

- **On-Premises SharePoint 2013**
- **SharePoint Online**

Historical Support Incidents and Service Requests Trend

The SharePoint environment is highly stable. However, business departments frequently ask for enhancements or service requests intended to improve developed applications per department.

Table 3 – Historical Support Incidents and Service Requests Trend: Microsoft Share Point

Application Type	Number of users per application	Number of Requests per year	Number of Incidents per Year
SharePoint Applications	3500	85	100
Web Applications (Internet & Intranet)	3500	30	145
Total Number of calls per year		**115**	**245**

It is the responsibility of the Service Provider to ensure that incidents are minimised or reduced over time by providing training and performing necessary system enhancements.

Skills required to support MICROSOFT SharePoint Environment

Each technical resource must display certain skill sets and demonstrate the ability to perform certain functions and/or take responsibility for certain actions. This level of expertise should be based on the resources' experience on providing such support functions in similar projects/assignments with other clients (ACSA can be added as additional reference). Through possessing the relevant qualifications and experience, the resource must demonstrate a good level of understanding of the following skills and accountabilities: (please note that these skills are set out as a guide only and should not be viewed as exhaustive, Bidders are encouraged to provide their own descriptions of the skills set according to the resources level of skill, if applicable).

SharePoint Focus Area	Minimum Skill Set
SharePoint Administrator	• SharePoint server administrations and support • Strong knowledge and working experience of .NET, C# and JavaScript programming and web-development • Understanding of Production and Business support • Good understanding of the agile methodology for continuous support of the business while implementing code for multiple projects running concurrently • Extensive knowledge and working experience of SharePoint Online and SharePoint On-Prem • Working experience and ability to do upgrade the software stack. • Understanding of the share point workflow
SharePoint Development	• Good understanding of the agile methodology for continuous support of the business while implementing code for multiple projects running concurrently • Extensive knowledge and working experience of SharePoint Online and SharePoint On-Prem • Working experience and ability to do upgrade the software stack. • Extensive knowledge and working experience of the SharePoint workflow

	• Extensive knowledge and development experience of the Office365 PowerApps and Microsoft Flow. • Working experience of AD utilities • Ability to Backup and clean up various log files on the application • Working knowledge of Cloud Security • Working experience of script writing for data extraction, transformation, and loading • Ability to perform routine security and authentication measures. • Ability to write and interpret SQL queries.
SQL Database Administrator	• Extensive experience and knowledge of Installation, upgrades, and manage services in SQL application and Database • Working experience of AD utilities • Knowledge of and ability to clone Production to other non-production systems • Extensive experience and knowledge of Concurrent managers • Ability to Backup and clean up various log files on the application • Working knowledge of Networks, Security, Storage and Oracle Infrastructure. • Extensive knowledge of database and application tuning • Working experience of release and change management • Ability to manage and optimise Storage • Ability to ensure system audit compliance • Working experience of script writing for custom scripts • Extensive knowledge of Installation, patching, monitoring Oracle databases • Ability to monitor, and verify backups and perform ad-hoc backups • Working experience of script writing for data extraction, transformation, and loading • Ability to perform routine security and authentication measures. • Extensive knowledge and working experience of database upgrade execution • Ability to write and interpret SQL queries. • Extensive knowledge and working experience of database lock, space management, export and import of the database
Web Development	• Extensive NET Web API/Node.js development experience • Extensive and working experience of Token based authentication • Extensive knowledge and experience of security including the

	use of certificates to secure web sites/web services • Working experience of Cloud services including but not limited to Azure/AWS • Working knowledge and experience of Microservices architecture • Working knowledge of HTML 5 and CSS • Working knowledge of API integration
Power BI	• Designing, developing, and maintaining business intelligence solutions • Crafting and executing queries upon request for data • Presenting information through reports and visualization • Evaluate and enhance current Power BI reports

2.2 Service locations

2.2.1 All Enterprise applications are supported from the Corporate office. Should there be any changes to the address of the corporate office, the service provider will be notified and will be expected to consider the new address as the Corporate office. The services are offered for Corporate office and all the 9 airports as listed below.

SITE CODE	ADDRESS
COR	Riverwoods Office Park, 24 Johnson Road, Gardenview, 2047
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	Port Elizabeth Airport, Allister Miller Drive, Walmer, 6070
GRJ	George Airport, Old Mosselbay Road, George, 6529
ELS	East London Airport, Settlers Way, East London, 5200
KIM	Kimberly Airport, Compound Patterson Road, Kimberly, 8300
BFN	Bram Fischer International Airport, Bloemfontein, 9300
UTN	Upington International Airport, Diedericks Street, Upington, 8801

Table:5 Regional Distribution of ACSA airports

3.0 RATE OF EXCHANGE, QUOTATIONS AND INVOICES

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

3.1 Quotations

3.1.1 All initial Quotations for engagements will use a Fixed Rate.

3.1.2 Once scoping for an engagement is completed and funds secured. The provider will provide a final quote for the scope.

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

3.2 Invoices

3.2.1 All invoices should include

I. the ACSA purchase order number
II. All deliverables and/or timesheets (signed off by ACSA official)
III. Monthly Fixed costs to include signed off SLA reports

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

4.0 SOFTWARE LICENSE MANAGEMENT

Due to the complexity of licensing agreements, it is important for the service provider to assist with managing licenses and optimization thereof to avoid overutilization and reduce licensing costs.

4.1 Asset management

4.1.1 Tracking and monitoring of license utilisation against entitlements remain the responsibility of the MSP for the duration of the contract.

4.1.2 All applications remain in the control of the MSP for the duration of the contracts.

4.1.3 All deliverables must be signed off by an ACSA resource or representative and an MSP representative.

5.0 PERSONNEL

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

5.2 The MSP 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 agreed period of time.

5.3 Suitably certified resources are required to service this contract. Normal working hours will prevail with **off-site** support but may extend to after-hours or overtime on a need basis. Minimum resources must be made available onsite on an ad hoc basis for meetings and clarification of scope if there is a need to do so.

5.4 If a need arises for resources to be security vetted by the state security agency, the MSP will be expected to comply with such requirements. The MSP would also be expected to pay for any associated costs of security vetting.

5.5 All resources must sign the ACSA Non-Disclosure Agreement (NDA) as supplied in this tender.

5.6 The table below indicates the service coverage hours

Table 6 – Service Coverage Window definitions

Service Class	Service Coverage Window
Standard Office Hours	Normal Office Hours - 08:30 - 17:00 on Mon - Fri, excluding public holidays
Extended Office Hours	Normal Office Hours - 06:00 - 18:00 on Mon - Fri, excluding public holidays

Service Class	Service Coverage Window
Weekday After Hours	After Hours – 18:00 – 06:00 on Mon – Fri, excluding public holidays
Weekends	Weekend and Public Holidays – 24 Hours Saturday and Sunday, including public holidays
Project & IMACD	All project and IMACD tasks that impact the live environment will take place after hours or over the weekends. These will be determined by ACSA representatives and the service provider

Resources should always be available for standard working hours and on a need basis for extended, weekday after hours and weekend on a need basis or to attend to critical incidents. Projects will be delivered as per the agreed schedule.

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

6.0 PREVENTATIVE AND CORRECTIVE MAINTENANCE

6.1 Preventative Maintenance includes tests, software upgrades, firmware upgrades, patch management and any activity aimed at preventing failures through maintaining the condition of the system or assessing its condition for the purposes of corrective maintenance.

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

6.3 Break/fix includes maintenance that is unforeseen and is necessary to restore the application, and functionality of the System. Some of these. break/fix maintenance could be requested after hours on weekend and public holiday. Service providers will be expected to respond and attend to all the faults

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

6.5 The provider must cater for short notice call-out in an emergency where the supported system may be affected by other interruptions or change processes. The provider must provide a call-out basis and hour rate at the specific site.

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

6.7 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.

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

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

Table 7 – Preventative Maintenance Schedule

Component	Focus Area	High level maintenance task/checks description	Frequency
Oracle Operating System	System Checks	• check log files and take action accordingly • Action any alerts or errors or recommendations	Daily
	Storage	• • Ensure system has adequate space	Weekly
	System Mails	• • check system mails and respond accordingly	Daily
	Redundancy Tests	• Check applicable patches and action accordingly • Check applicable patches and action accordingly	3 Monthly
IBM	Health Checks	• Monitor the hardware health and ensure all back-end services, including replication are operational • Action any alerts or errors • PowerHA cluster status monitoring and health • Monitor the hardware, operating system health and ensure all back-end services, including replication are operational • Check management console status and error reporting • PowerVM virtualization status monitoring and health • Action any alerts or errors	Daily
	Capacity Management	• Monitor capacity to ensure utilization stays within range of best practice	Monthly
Database	DB Health Checks	• Check DB and listener • Action any alerts or errors or recommendations	Daily
	Capacity Management	• • Ensure system has adequate space to function	Weekly
	DB log analysis	• Monitoring of system log and responding to any deviations. Monitoring of alarms and faults	Daily
	Patching	• • Check applicable patches and action accordingly	3 Monthly
Applications	Application Check	• check frontend login and performance • Check front-end login and performance	Daily
Disaster Recovery Environment	Redundancy Test	• Ensure system fails over according to OLA with Business Continuity Management Team	Bi-annually

7.0 Baseline Information

7.1 This section provides summary of users per application which should be taken into consideration by the bidders.

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

Oracle Module	User Count
Oracle Fixed Assets	65
Oracle Projects	114
Oracle Procurement	964
Oracle Account Payable	124
Oracle Cash Management	63
Oracle Property Manager	40
Oracle EAM	270
Oracle Business Intelligence	52
Oracle EBS Human Resource	2644
Oracle Fusion Talent	2644
Oracle Taleo Recruit	2644
Planning and Budgeting Cloud Services	557
Oracle Accounts Receivable	113
Oracle General Ledger	105

Table:8 Oracle number of users

Application Type	Number of users per application
SharePoint Applications	2644
Web Applications (Intranet & Internet)	2644

Table:9 SharePoint number of users

Table 10 – IBM ESB incidents and Service Request Trends

ESB Module	Category of Users	Number of Requests per Year	Number of Incidents per Year	Number of Changes All Airports
2DBC	Airport Operations including Airlines	3	4	3
Zeus	Airport Operations including Airlines	0	10	0
Apex	Airport Operations including Airlines	5	15	5
AMS	Airport Operations including Airlines	20	7	15
SAC	Airport Operations including Airlines	0	3	
Other (Active Directory, Firewall, Security, Network, Desktop Applications)	Airport Operations including Airlines	7	1229	7
Total Number of calls per year		**35**	**1268**	**30**

7.3 Agreements and Licenses

Table 11 – Agreements and Licences

Equipment Supplier(s)	Number of licenses	Contract Renewal Date	Comments
Oracle On Prem	3000	01-May-21	Yearly renewed, maintenance and subscriptions
Oracle Planning Budgeting Cloud Services	360	01-Jan	Yearly renewed, maintenance and subscriptions
Oracle Human Capital Taleo and Fusion (Cloud)	3000	01-Jan	Yearly renewed, maintenance and subscriptions
Oracle Technical Licenses	Unlimited	01-May-21	Yearly renewed, maintenance and subscriptions

IBM Message Queuing (MQ)	700	01-May-21	Yearly renewed, maintenance and subscriptions
IBM Blueworks	200	08-Jun-21	Yearly renewed, maintenance and subscriptions
Nintex Licenses	5	31-Dec-21	Yearly renewed, maintenance and subscriptions

8.0 Current Hardware Standards

Table 12 – Server and Virtualisation Hardware Device Standards

Device Type	Manufacturers
BladeSystem Enclosures	HPE
MQ Appliances	IBM
DataPower Appliances	IBM
ESB databases	Oracle
MQ IPT Gateway	IBM
Storage controllers	IBM
Fabric Switches	IBM (Brocade OEM)
p-Series Servers	IBM
Virtualization	VMware, Microsoft Hyper-V and PowerVM

9.0 Out of Scope

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

9.1 Procurement of hardware and software

9.2 Infrastructure support and maintenance

9.3 Support and Maintenance of Convene solution

9.4 Host to Host Banking Solution

10.0 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:

Table 13 – Definition of RASCI model

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

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

10.1 Roles and Responsibilities- General

Table 14 -Roles and Responsibilities – General

Sub area	Number	Task/Activity	Service Provider	ACSA
General	1.	Provide Services and the supporting processes that support ACSA business needs, technical requirements and End-User requirements	R, A	C
	2.	Approve Services and the supporting processes that support ACSA's business needs, technical requirements and End-User requirements	I	R
	3.	Comply with ACSA policies, guiding principles, standards and regulatory requirements applicable to the ACSA for information, information systems, personnel, physical and technical security	R, A	C
	4.	Develop and maintain an approved comprehensive Standards and Procedures Manual that contains the standards, processes and procedures that will be used in the delivery of all Services. The manual will include clearly delineated roles and responsibilities, touch points and measurements between ACSA and the vendor.	R, A	C
	5.	Approve the comprehensive Standards and Procedures Manual that contains the standards, processes and procedures that will be used in the delivery of all Services. The manual will include clearly delineated roles and responsibilities, touch points and measurements between ACSA and the vendor.	I	R
	6.	Conform to changes in laws, regulations and policies. Major Service Changes shall be proposed on a project-by-project effort basis to alter the environment to conform to the new requirements.	R	C, A
	7.	Report performance against Service-Level Requirements (SLRs)	R, A	I
	8.	Coordinate all Changes to the IT systems that may affect the SLRs of any other Service	R, A	C, I
	9.	Provide timely creation, updating, maintenance and provision of all appropriate project plans, project time and cost estimates, technical specifications, management documentation and management reporting in a form/format that is acceptable to the ACSA for all Service projects and major Service activities	R, A	C
	10.	Adhere to IT service management (ITSM) best practices and Key Performance Indicators (KPIs)	R, A	I
	11.	Approve the use of the ITSM best practices and KPIs	C, I	R
Site Acce	12.	Coordinate with site IT staff to schedule On-Site Technical Support visit when using non-regular or 3rd party resources	R, A	C, I

Sub area	Number	Task/Activity	Service Provider	ACSA
	13.	Ensure that all support staff has valid airside permits for the airports that they support.	R, A	C, I
	14.	Ensure that support staff strictly adheres to the terms and conditions of their permit allowances	R, A	C, I
	15.	Ensure that support staff has access to reliable transport and valid driver's licences.	R, A	C, I
	16.	Ensure that the provider has a valid health and safety file at all times in line with CIVID-19 requirements	R, A	C, I
	17.	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 support	I	R,A
	18.	Parking fees at ACSA premises	R, A	I
	19.			
	20.	Any security related training and payments for access to ACSA premises	R, A	I

10.2 Roles and Responsibilities - Management, Planning and design

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

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

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

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

Table 15 – Roles and Responsibilities – Management, Planning and design

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	R, A	C,S,I

Sub area	Number	Task/Activity	provider	ACSA
		Planning and Analysis activities to ensure continuous alignment to best practise.		
	4.	Ensure all documentation remains updated in required ACSA format. (including but not limited to upgrade requirements, conversion requirements, design schematics, WC/CR/DC design diagrams etc). 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 application landscape at an enterprise level (e.g., technology strategy, technology architecture, functional, availability, capacity, performance, backup and IT Service Continuity)	S,I	R,A
	7.	Provide ACSA documentation format standards. Review and approve updated documentation presented by Service provider	I	R,A
	8.	Review and update the existing Services, standards and project management practices for Planning and Analysis activities	I	R,A
Technical Architecture	9.	Attend, actively participate in and provide technical assistance and subject matter expertise in technical and business planning sessions to review standards, architecture and project initiatives to align with best practise	R,A	C,S,I
	10.	Document current and future Technical Architecture in the agreed formats and update these throughout the service lifecycle	R,A	C,S,I
	11.	Perform evaluation of new equipment considered for implementation in compliance with the ACSA's security and IT architecture policies, regulations and procedures.	C,S,I	R,A
	12.	Define and approve any new architecture standards	C,S,I	R,A
	13.	Conduct technical and business planning sessions to review standards, architecture and project initiatives to align with best practises	R,A	C,S,I
Continuous Improvement and Innovation Planning	14.	Conduct technical reviews and provide recommendations for improvements that increase efficiency, effectiveness and reduce costs	R,A	C,I
	15.	Perform ad hoc investigations as requested by ACSA and submit recommendations for ACSA's consideration.	R,A	C,I
	16.	Conduct on-going, regular planning and recommendations for technology refresh and upgrades	R,A	C,I
	17.	Showcase new technology enhancements to ACSA hence allowing ACSA the option to upgrade to any new 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

Sub area	Number	Task/Activity	provider	ACSA
	20.	Review and approve recommendations for technology refresh and upgrades	C,I	R,A
	21.	Review any new technology enhancements presented	C,I	R,A
Management and Testing Tools	22.	Use existing System management tools to monitor measure, manage and document the environment.	R,A	C,I
	23.	Provide access to existing System management tools to monitor measure, manage and document environment	C,I	R,A
Research	24.	Provide expert advice and research latest technologies on a constant basis and formally submit these presentations to ACSA IT Infrastructure on a 3-monthly basis.	R,A	C,I
	25.	Participate in in-scope IT-Commercial initiatives as requested ACSA-IT – this includes understanding the required solution and outcome, provide solution design and architecture documentation relating to this service towner	C,I	R,A
	26.	Together with ACSA-IT perform feasibility studies for the implementation of new and existing technologies that best meet ACSA business needs and meet cost, performance and quality objectives.	R,A	C,I
	27.	Review the latest technologies presented by the Service provider.	C,I	R,A
	28.	Request provider to participate in in-scope IT-Commercial initiatives.	C,I	R,A
Design and panning	29.	Develop, document and maintain detailed technical design/engineering plans and environment configuration based on ACSA's business requirements	R,A	C,I
	30.	Provide design documentation for quarterly audits as requested by ACSA	R,A	C,I
	31.	Provide input into design plans through coordination with the appropriate ACSA technology standards groups and design architects	C,I,S	R,A
	32.	Quarterly audit of design documentation	C,I,S	R,A
	33.	Adhere to production acceptance test criteria	R,A	C,I
	34.	Conduct and document test plans and results	R,A	C,I
	35.	Define and document production acceptance test criteria	C,I	R,A
	36.	Review and approve test plans and results	C,I	R,A

10.3 **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").

Table 16 – Roles and Responsibilities – Project Management Services

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)	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

10.4 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.

Table 17 – Roles and Responsibilities – Acquisition and Management

Sub area	Number	Task/Activity	provider	ACSA
Policies, Processes	1.	When procurement is requested by ACSA-IT, provider to adhere to acquisition/procurement policies	R,A	C,I
	2.	Provide guidance on ACSA acquisition/procurement policies	C,I	R,A

Sub area	Number	Task/Activity	provider	ACSA
	3.	Develop, document and maintain in the Standards and Procedures Manual Acquisition and Management procedures that meet requirements and adhere to defined policies	R,A	C,I
	4.	Review and approve Acquisition and Management procedures	C,I	R,A
	5.	Perform periodic audits of procurement procedures	I,C	R,A
Demand Management	6.	Escalate any issues to ACSA-IT, notify ACSA immediately upon learning of such issues that may result in non-performance	R,A	C,I
	7.	Attend monthly review sessions to understand estimated consumption forecast where available to ensure achievement of timelines	R,A	C,I
	8.	Address any management escalations from Service provider	C,I	R,A
	9.	Quarterly, ACSA shall provide the Service provider with its estimated consumption forecast of all in scope applications. The forecast process will be a joint effort between ACSA and the provider using historical data.	C,I	R,A
Standards Compliance	10.	Ensure that all application developments comply with established ACSA standards and architectures	R,A	C,I
	11.	Ensure all software is listed as part of the ACSA architecture technology standards	C,I	R,A

10.5 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.

Table 18 – Roles and Responsibilities – Documentation

Sub area	Number	Task/Activity	provider	ACSA
Documentation	1.	Ensure that the entire in scope applications are 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 applications (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

Sub area	Number	Task/Activity	provider	ACSA
	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 applications directory is well documented and constantly updated	I	R,A
	7.	Review checklist and implement action plans based on any exception reports and recommendations	I	R,A
	8.	Work with provider to specify the content, purpose, format and production schedule of all documents within scope	C,I	R,A
	9.	Provide space to store physical copies of all documents and share folder for digital copies of the documents	I	R,A
	10.	Provide timely creation, updating, maintenance and provision of all documentation, (design documents; architectural diagrams; as built documents; test plans; all ACSA required project documentation; technical specifications, preventative and corrective maintenance plans and checklist; escalation reports; daily service request report; floor layout diagrams; OEM and third party documentation and management reporting in a form/format that is acceptable to ACSA for Service Projects and major Service activities	R,A	C,I
	11.	Manage all documentation in accordance with Configuration Management standards and guidelines	R,A	C,I
	12.	Document standard operating procedures	R, A	I
	13.	Review and approve standard operation procedures Documentation	I	R,A

10.6 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.

Table 19 – Roles and Responsibilities – Technology Refresh and Replenishment

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

Sub area	Number	Task/Activity	provider	ACSA
	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

10.7 Roles and Responsibilities - Applications Build and Change

Managing all applications changes [simple, average, complex, very complex] 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
- Upgrades to any existing or live facility
- Retirement and Disposal of software assets

Table 20 – Roles and Responsibilities – Applications Build and Change

Sub area	Number	Task/Activity	provider	ACSA
Installations and Additions		Complete IMACD plan per installation and addition	R,A	C,I
		Present IMACD plan to ACSA for approval	R,A	C,I
		Complete IMACD	R,A	C,I
		Receive and review IMACD plan per installation and addition presented by Service provider	I	R,A
		Approve IMACD plans received from Service provider	I	R,A
		Approve and sign off IMACD installations and additions in alignment with approved plans	I	R,A
Changes		Recommend changes to meet service requirements	R,A	C,I
		Perform changes to meet business requirements	R,A	C,I
		Review and approve recommended changes presented by the provider where required	I	R,A
		Sign off implemented changes	I	R,A
Decommission		Complete IMACD plan per decommission requirement	R,A	C,I
		Present IMACD plan to ACSA for approval	R,A	C,I
		Complete IMACD decommission per approved IMACD plan (timelines / tasks / pre-decommission checks / UAT etc.)	R,A	C,I
		Disposal of equipment and materials in accordance with ACSA policies upon request.	R,A	C,I
		Receive and review IMACD plan per decommission by Service provider	I	R,A
		Approve IMACD plans received from Service provider	I	R,A
		Approve and sign off IMACD decommission in alignment with approved plans	I	R,A
		Sign off the decommissioned applications in accordance with ACSA policies with Service provider, and ensure financial asset disposal tasks are completed	I	R,A
IMACD Completion Sign-Off		Conduct and document production acceptance tests and provide results to obtain signed completion form (production acceptance) from ACSA	R,A	C,I
		Maintain and update records to ensure baseline CMDB is always up-to-date	R,A	C,I
		Review acceptance test and results for sign off	I	R,A

Sub area	Number	Task/Activity	provider	ACSA
		Review before during and after photos taken during changes	I	R,A
		Review CMDB baseline reports quarterly as defined in report schedule	I	R,A

10.8 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.

Table 21 -Roles and Responsibilities - Maintenance

Sub area	Number	Task/Activity	provider	ACSA
Maintenance		Define Maintenance requirements	I	R, A
		Develop, document and maintain in the Standards and Procedures Manual Maintenance procedures that meet requirements and adhere to defined policies	R, A	I
		Develop Maintenance schedules (OEM recommended preventative maintenance to be taken into account)	R, A	I
		Review and approve Maintenance procedures and schedules	I	R, A
		Ensure appropriate Maintenance coverage for all Service components	R, A	C, I
		Provide Maintenance and break/fix support to ACSA	R, A	C, I
		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
		Perform an analysis of the impact and/or applicability of Vendor-provided patches and/or service packs, in accordance with ACSA policies and requirements	R, A	C, I
		Approve Vendor-provided patches and/or service packs	C, I	R, A
		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
		Install patches per ACSA's Change Management process and procedures including acquiring required ACSA approval	R, A	C, I
		Install (and/or coordinate with Third-Party Maintenance Vendor if applicable) manufacturer field change orders, service packs, firmware and software maintenance releases, etc.	R, A	C, I

Sub area	Number	Task/Activity	provider	ACSA
		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
		Perform Maintenance-related software distribution and version control, both electronic and manual	R, A	C, I
		Replace (and/or coordinate with Third-Party Maintenance Vendor if applicable) preventive Maintenance, according to the manufacturer's published mean-time-between-failure rates	R, A	I
		Initiate projects to execute on approved preventative maintenance recommendations	I,C	R,A
		Provide detailed monthly reports on capacity, assets, changes, faults, potential risks, etc. as defined in the report schedule	R,A	C,I

10.9 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

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

Sub area	Number	Task/Activity	provider	ACSA
Management and Administration	1.	Utilise ACSA Monitoring tools to monitor the applications that will meet the monitoring and service level reporting requirement	R,A	C,I
	2.	Implement measures for proactive monitoring to limit outages	R,A	C,I
	3.	Manage and coordinate provider appointed subcontractors and Third Parties to meet Service and SLA requirements	R,A	C,I
	4.	Suggest any additions or changes to ACSA monitoring tools landscape to improve the service	R,A	C,I
	5.	Implement measures for proactive monitoring to limit outages	R,A	C,I

10.10 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 Applications 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.

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 Applications to ensure IT Services are designed to deliver the appropriate levels
- Identifying opportunities to optimize the availability of the IT Applications to deliver cost-effective improvements that deliver tangible business benefits.
- Supporting the targets for availability, reliability and maintainability for the IT Application 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 Application 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

Table 23 – Roles and Responsibilities – Availability Management

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

Sub area	Number	Task/Activity	provider	ACSA
	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 Applications and services design	I	R, A
	11.	Coordinate with the IT service support and IT service delivery process owners and managers from ACSA to research, review and assess Availability issues and optimization opportunities	R, A	C, I
	12.	Define the availability measures and reporting required for the IT Infrastructure and its components that underpin an upgraded and/or new IT Service, as the basis for an SLA that reflects business, End-User and IT support organization requirements	I	R, A
	13.	Participate with ACSA in defining the availability measures and reporting requirements	R, A	I
	14.	Recommend appropriate tools and practices to measure and report on agreed-upon availability measures for upgraded and/or enhanced IT Infrastructure	R, A	I
	15.	Review and approve availability measurement tools and practices	I	R, A
	16.	Ensure that approved availability measurement tools and practices are implemented	R, A	I
	17.	Monitor and maintain an awareness of technology advancements and IT best practices related to availability 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 for in scope appliations	R, A	I

Sub area	Number	Task/Activity	provider	ACSA
	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

10.11 Roles and Responsibilities - Capacity Management

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

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

Table 24 – Roles and Responsibilities – Capacity Management

Sub area	Number	Task/Activity	provider	ACSA
Capacity Management	1.	Define Capacity Management requirements	I	R, A
	2.	Develop, document and maintain in the Standards, Process and Procedures Manual Capacity Management procedures that meet requirements and adhere to defined policies	R, A	I
	3.	Review and approve Capacity Management process and procedures	I	R, A
	4.	Establish a comprehensive Capacity Management planning process	R, A	I
	5.	Review and approve Capacity Management planning process	I	R, A
	6.	Define, develop and implement tools that allow for the effective capacity monitoring/trending of IT Infrastructure, applications and IT components	R, A	I
	7.	Identify future business requirements that will alter capacity requirements	I	R, A
	8.	Develop a periodic (usually yearly) capacity plan, including quarterly updates	R, A	I
	9.	Develop and implement capacity models and run simulations to validate the capacity plan	R, A	I
	10.	Participate in all capacity planning activities	I	R, A
	11.	Assess capacity impacts when adding, removing or modifying applications and infrastructure components	R, A	I
	12.	Continually monitor IT resource usage to enable proactive identification of capacity and performance issues	R, A	I
	13.	Capture trending information and forecast future ACSA capacity requirements based on ACSA-defined thresholds	R, A	I
	14.	Assess incidents/problems related to capacity and provide recommendations for resolution	R, A	I
	15.	Recommend changes to capacity to improve service performance	R, A	I
	16.	Assess impact/risk and cost of capacity changes	R, A	I
	17.	Approve capacity-related recommendations	I	R, A
	18.	Maintain capacity levels to optimize use of existing IT resources and minimize ACSA costs to deliver Services at agreed-to SLRs	R, A	I
	19.	Ensure adequate capacity exists within the IT environment to meet SLRs and requirements, taking into account daily, weekly and seasonal variations in capacity demands	R, A	I
	20.	Validate asset utilization and capital efficiency	I	R, A

10.12 **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)

Table 25 – Roles and Responsibilities – Performance Management

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 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

10.13 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

Table 26 – Roles and Responsibilities - Configuration Management

Sub area	Number	Task/Activity	provider	ACSA
Configuration Management	1.	Define Configuration Management requirements	I	R, A
	2.	Develop, document and maintain in the Standards Process and Procedures Manual Configuration Management procedures that meet requirements and adhere to defined policies	R, A	I
	3.	Review and approve Configuration Management procedures and processes	I	R, A
	4.	Identify and document the configuration item structure	R, A	I
	5.	Approve the configuration item structure	I	R, A
	6.	Establish Configuration Management database, in accordance with ACSA requirements	R, A	I
	7.	Review and approve Configuration Management database	I	R, A
	8.	Select and provide Configuration Management tools	I	R, A
	9.	Install and maintain Configuration Management tools	R, A	I
	10.	Enter/upload configuration data into configuration database	R, A	I
	11.	Establish process interfaces to Incident and Problem Management, Change Management, technical support, maintenance and Asset Management processes	R, A	I
	12.	Establish appropriate authorization controls for modifying configuration items and verify compliance with software licensing	R, A	I
	13.	Establish guidelines for physical and logical separation between development, test and production and the process for deploying and back-out of configuration items	I	R, A
	14.	Develop procedures for establishing configuration baselines as reference points for rebuilds, and provide ability to revert to stable configuration states	R, A	I
	15.	Develop procedures for establishing security baselines as reference points for rebuilds, and provide ability to revert to stable configuration states	I	R, A
	16.	Establish procedures for verifying the accuracy of configuration items, adherence to Configuration Management process and identifying process deficiencies	R, A	I
	17.	Provide a deficiency report and steps taken to address the issues identified	R, A	I
	18.	Provide ACSA Configuration Management reports as required and defined by ACSA	R, A	I
	19.	Audit Configuration Management process and accuracy of configuration data	I	R, A
	20.	Perform physical asset verifications	R,A	C,I
	21.	Manage the IT Storerooms at ORTIA and Corporate office	R,A	C,I

Sub area	Number	Task/Activity	provider	ACSA
	22.	Coordinate the IT asset disposals	R,A	C,I
	23.	Maintain and manage the CMDB	R,A	C,I

10.14 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.

Table 27 – Roles and Responsibilities – Software License Management

Sub area	Number	Task/Activity	provider	ACSA
Software License Management	1.	Define Software License Management requirements	C, I	R, A
	2.	Recommend improvements to Software License Management requirements and policies	R, A	I
	3.	Develop, document and maintain in the Standards and Procedures Manual Software License Management procedures that meet requirements and adhere to defined policies as mapped to Asset Management	R, A	I
	4.	Review and approve Software License Management processes and procedures	I	R, A
	5.	Manage and maintain (e.g., monitor, track status, verify, audit, perform contract compliance, reassign) software licenses and media through software license life cycle	R, A	C, I
	6.	For ACSA-retained contracts, be responsible for procurement, renewal and upgrade costs, and vendor agreements	I	R, A
	7.	For non-ACSA-retained contracts, be responsible for procurement, renewal and upgrade costs, and vendor agreements	R, A	C, I
	8.	Develop and maintain inventory of all Software licenses within the Asset Management system	R, A	I
	9.	Report to ACSA on any exceptions to Vendor terms and conditions including license non-compliance	R, A	I
	10.	Periodically (at least yearly), conduct software license and maintenance agreements review, allowing for sufficient time prior to expiration for negotiations	R, A	I
	11.	Participate in software license and maintenance agreements review	I	R, A
	12.	Provide ACSA with reports and recommendations to use in making software acquisition and discontinuance decisions	R, A	I
	13.	Provide recommendations to purchase additional license allocation, recommending alternatives or curtailing usage where necessary and appropriate, to restore or continue to maintain license compliance	R, A	I
	14.	Identify and report license compliance issues to ACSA and provide recommendations to resolve the compliance issue	R, A	I

Sub area	Number	Task/Activity	provider	ACSA
	15.	Review license compliance issues and document completed resolution	I	R, A
	16.	Manage and perform audits and reconcile the number of licenses to the number of installs, as requested by ACSA	R, A	I
	17.	Provide recommendations to ACSA to resolve any software reconciliation issues	R, A	I
	18.	Report on resolution to software reconciliation issues	I	R, A
	19.	Obtain approval from ACSA for any license change or replacement	R, A	I

10.15 Roles and Responsibilities - Change Management

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

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

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

The Change Management process includes the following process steps:

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

Table 28 - **Roles and Responsibilities - Change Management**

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

Sub area	Number	Task/Activity	provider	ACSA
	20.	Monitor changes, perform change reviews and report results of changes, impacts and change effectiveness metrics	R, A	I
	21.	Verify that change met objectives based upon predetermined effectiveness metrics, and determine follow-up actions to resolve situations where the change failed to meet objects	R, A	I
	22.	Review and approve Change Management results	I	R, A
	23.	Close out RFCs that met the change objectives or changes that were abandoned	R, A	I
	24.	Perform Change Management quality control reviews and audits of Change Management processes and records	c, I	R, A
	25.	Provide ACSA Change Management reports as required and defined by ACSA	R, A	c, I

10.16 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.

Table 29 – Roles and Responsibilities – Training and Knowledge transfer

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 ACSA-accessible knowledge database/portal	R, A	C, I

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

10.17 **Roles and Responsibilities - Account Management**

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

Table 30 – Roles and Responsibilities – Account Management

Sub area	Number	Task/Activity	provider	ACSA
Management	1.	Define Account Management requirements	I	R, A
	2.	Develop, document and maintain in the Standards Process and Procedures Manual Account Management procedures that meet requirements and adhere to defined policies	R, A	I
	3.	Review and approve Account Management process and procedures	I	R, A
	4.	Develop a detailed "IT" catalogue that details Services offered, including all Service options, pricing, installation time frames, order process (new, change and remove service) and prerequisites	R, A	I
	5.	Approve Service catalogue	I	R, A

Sub area	Number	Task/Activity	provider	ACSA
	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

10.18 Roles and Responsibilities - Incident Resolution and Problem Management

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

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

Table 31 – Roles and Responsibilities – Incident Resolution and Problem Management

Sub area	Number	Task/Activity	provider	ACSA
Incident Resolution and Problem Management	1.	Adhere to ACSA Incident resolution and Problem Management process and procedures	R, A	I
	2.	Provide ACSA Incident resolution and 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	R, A	I,C

Sub area	Number	Task/Activity	provider	ACSA
		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.		
	7.	ACSA-IT Representative to review Incident and Problem management tasks by the provider in Monthly Care Review Meetings to ensure the provider is completing tasks in accordance to 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,

10.19 **Roles and Responsibilities - IT Service Continuity and Disaster Recovery**

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

Table 32 – Roles and Responsibilities – IT Service Continuity and Disaster Recovery

Sub area	Number	Task/Activity	provider	ACSA
IT Service Continuity and Disaster Recovery	1.	As needed, assist ACSA in 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

10.20 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.

Table 33 – Roles and Responsibilities – Service-Level Monitoring and Reporting

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

10.21 Roles and Responsibilities - Financial Management

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

Table 34 – Roles and Responsibilities – Financial Management

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

10.22 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.

Table 35 – Roles and Responsibilities – Human Resources

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

10.23 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

Table 36 – Roles and Responsibilities - Security

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

Sub area	Number	Task/Activity	provider	ACSA
Data Security	15.	Assume custodial responsibility for all storage media Related to services provided	R, A	I
	16.	Protect portable media while in transit and maintain transmittal records	R, A	I
	17.	Eradicate all data from storage media (server memory, disk, tape, optical, other) before redeployment or disposal, in accordance with ACSA's procedures	R, A	I
	18.	Perform periodic (e.g., monthly) reconciliation reporting of all data media and perform annual audit to reconcile all storage media	R, A	I
	19.	Report reconciliation discrepancies to ACSA and take corrective action to address issue	R, A	I
Identity and Access Management	20.	Provide Identity and Access Management in conformance with ACSA practices, policies and procedures	R, A	I
	21.	Establish roles, authorized activities and minimum rights granted to Service provider personnel (including non-user accounts)	R, A	I
	22.	Establish roles, authorized activities and minimum rights granted to ACSA personnel (including non-user accounts)	I	R, A
	23.	Approve roles and authorization activities performed by provider	I	R, A
	24.	Establish and manage the process for defining, granting, modifying and revoking user accounts and enforcing role restrictions	R, A	I
	25.	Establish and manage process to support temporary access	R, A	I
	26.	Review and approve user and system user account management process	I	R, A
	27.	Approve Service provider personnel who are authorized to manage user accounts	I	R, A
	28.	Provide IT Identity and Access Management technology solution that integrates with ACSA systems	I	R, A
	29.	Support and maintain IT Identity and Access Management technology solution for Applications in scope	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

Sub area	Number	Task/Activity	provider	ACSA
	37.	Monthly audit production system access logs and activities to identify malicious or abnormal behavior 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
	41.	Review and approve remediation approach	I	R, A
	42.	Recommend changes to baseline to meet ACSA requirements	I	R, A
	43.	Configure equipment to approved security requirements	R, A	I
	44.	provider collaborates with ACSA on plan to implement security patches.	R, A	I
	45.	Install security patches per the Change, Configuration and Release Management processes and procedures	R, A	I
	46.	Establish logging and archiving specifications	R, A	I
	47.	Identify logging and archiving specifications in order to support business requirements	I	R, A
	48.	Approve logging and archiving specifications.	I	R, A
	49.	Log and archive user and system activity.	R, A	I
	50.	Provide ACSA with reports on any logs/intrusion detection activities, anomalies or deficiencies that could result in a compromise of the system's data confidentially, integrity or system performance	R, A	I
	51.	Provide ongoing support (patches, upgrades, signatures), tuning and management	R, A	I

11.0 SERVICE MANAGEMENT

11.1 Objectives

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

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

11.1.3 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 12.0 SERVICE CREDITS.

11.1.4 provider shall provide written reports to Senior Manager: Enterprise Applications regarding provider's compliance with the SLRs specified.

11.2 Reports

11.2.1 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.

11.2.2 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.

11.3 Root cause analysis

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

11.4 Support services

11.4.1 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.

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

11.4.3 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.

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

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

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

11.5 SERVICE-LEVEL REQUIREMENTS (SLRs)

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

11.5.1 Review of Service Levels and KPIS

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

11.5.1.2 This change can take effect only after the provider has had sufficient time (maximum 3 weeks) to review the requested change and determine if any modifications are required to the delivery of the support and maintenance services. Should changes be required by the provider, then ACSA will follow the above-mentioned process.

Any change will only be effective upon both parties agreeing to the change in writing.

11.5.2 Priority levels

Table 37 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 application 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: • Oracle Payroll • Oracle Finance Billing • IBM Integration Bus Services (IIB) • IBM Message Queuing Services (MQ)
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: • Oracle Finance Planning and Budgeting • Oracle Payables • Oracle SCM PO creation • Oracle SCM i-Procurement Services
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: • Oracle HR Leave Management Services • Oracle HR Performance Management Services • Oracle Finance General Ledger • Oracle Fixed Asset Management
Priority Level 4 — Low *Minimal Business Impact*	An incident that has little impact on normal business processes and can be handled on a scheduled basis. A workaround is available or there is minimal negative impact on a user's ability to perform their normal daily work. Example: • Service available but slow response
Priority Level 5 — Low Impact that will take a week or two to resolve	Service requests and project

11.5.3 **Incident management Review**

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

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

Table 38 – Incident Response and Resolution Time (Operational Hours) – See table on next page

Incident management response and resolution times for International Airports (Operational Hours)			
Incident/Problem Resolution	**Service Measure**	**Performance Target**	**SLR Performance %**
Time to Notify ACSA of or to accept/acknowledge a Priority 1	Time to Respond	<10 minutes	99.0%
Time to Notify ACSA of or to accept/acknowledge a Priority 2 Incident	Time to Respond	<20 minutes	99.0%
Time to Notify ACSA of or to accept/acknowledge a Priority 3 or 4 Incident	Time to Respond	<120 minutes	98.0%
Time to Notify ACSA of or to accept/acknowledge a Priority 5 Incident	Time to Respond	<3 hours	98.0%
Priority Level 1	Time to Restore (Not linked to hardware failure)	<2 hours	99.0%
Priority Level 2	Time to Restore (Not linked to hardware failure)	<4 hours	98.0%
Priority Level 3	Time to Restore (Not linked to hardware failure)	<8 hours	98.0%
Priority Level 4	Time to Restore (Not linked to hardware failure)	Next business day or as prioritized by provider	98.0%
Priority Level 5	Time to Restore (Not linked to hardware failure)	To be agreed	98.0%
Priority Level 1	Resolution (permanent fix)	To be agreed	99.0%
Priority Level 2	Resolution (permanent fix)	To be agreed	99.0%
Priority Level 3	Resolution (permanent fix)	To be agreed	98.0%

Incident management response and resolution times for International Airports (Operational Hours)			
Priority Level 4	Resolution (permanent fix)	To be agreed	98.0%
Priority Level 5	Resolution (permanent fix)	To be agreed	98.0%
Priority Level1-5 Hardware Failure	Fix/replacement	In line with the hardware support procured by ASCA	99.0%
Root-Cause Analysis	Time to Report	Within 48 hours of incident resolution	98.0%
	Formula	Number of requests completed within Performance Target ÷ Total of all requests occurring during Measurement Interval	
	Measurement Interval	Weekly	
	Reporting Period	Monthly	
	Measurement Tool	Data from ACSA Service management Tool (Service NOW) complimented with other provider tools if applicable	
	SLR Element Weighting Factor Allocation	50%	

Table 39 – Incident Management response and resolution times for international airports (outside operational hours) and regional airports operational hours (please see next page)

Incident management response and resolution times for International Airports (Outside Operational Hours) and regional airports operational hours.			
Incident/Problem Resolution	**Service Measure**	**Performance Target**	**SLR Performance %**
Time to Notify ACSA of or to accept/acknowledge a Priority 1	Time to Respond	<15 minutes	99.0%
Time to Notify ACSA of or to accept/acknowledge a Priority 2 Incident	Time to Respond	<20 minutes	99.0%
Time to Notify ACSA of or to accept/acknowledge a Priority 3 or 4 Incident	Time to Respond	<160 minutes	98.0%
Time to Notify ACSA of or to accept/acknowledge a Priority 5 Incident	Time to Respond	<3 hours	98.0%
Priority Level 1	Time to Restore (Not linked to hardware failure)	<3 hours	99.0%
Priority Level 2	Time to Restore (Not linked to hardware failure)	<5 hours	98.0%
Priority Level 3	Time to Restore (Not linked to hardware failure)	<10 hours	98.0%
Priority Level 4	Time to Restore (Not linked to hardware failure)	Next business day or as prioritized by provider	98.0%
Priority Level 5	Time to Restore (Not linked to hardware failure)	To be agreed	98.0%
Priority Level 1	Resolution (permanent fix)	To be agreed	99.0%
Priority Level 2	Resolution (permanent fix)	To be agreed	99.0%
Priority Level 3	Resolution (permanent fix)	To be agreed	98.0%

Incident management response and resolution times for International Airports (Outside Operational Hours) and regional airports operational hours.			
Priority Level 4	Resolution (permanent fix)	To be agreed	98.0%
Priority Level 5	Resolution (permanent fix)	To be agreed	98.0%
Priority Level1-5 Hardware Failure	Fix/replacement	In line with the hardware support procured by ASCA	99.0%
Root-Cause Analysis	Time to Report	Within 48 hours of incident resolution	98.0%
	Formula	Number of requests completed within Performance Target ÷ Total of all requests occurring during Measurement Interval	
	Measurement Interval	Weekly	
	Reporting Period	Monthly	
	Measurement Tool	Data from ACSA Service management Tool (Service NOW) complimented with other provider tools if applicable	
	SLR Element Weighting Factor Allocation	50%	

11.5.4 **Resource Availability**

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

11.5.5 **System Administration**

System Administration Service-Level Requirements			
	Service Measure	**Performance Target**	**SLR Performance %**
Advise Client of need to allocate additional processing resources based on predefined parameters and observed growth patterns	Proactive monitoring and reporting to Client of need to increase capacity	Sustained average daily CPU utilization approaches 80% of installed processor capacity—Inform Client within 1 Business Day Number of service requests closed as per	99.0%

	Formula	Number of requests completed within Performance Target ÷ Total of all requests occurring during Measurement Interval
	Measurement Interval	Measure Weekly
	Reporting Period	Report Monthly
	Measurement Tool	ACSA Service Desk Stats/ Provider request schedule
	SLR Element Weighting Factor Allocation	20%

11.5.6 **IMACDs**

11.5.6.1 Any software installation, upgrade, or update in accordance with Change Management policies. IMACDs are usually planned and scheduled in advance.

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

Service Measure:	**Performance Target:**	**SLR Performance %**
Receipt of IMACD the installation / decommission / move / change plan According to ACSA standards.	IMACD plan to be received by ACSA within 5 days of request. No IMACD plan or written confirmation that the provider cannot achieve the required	98%

	timelines will be deemed as a missed SLA	
On receipt of approval to proceed with IMACD, the provider is to complete the IMACD on time as per the approved plan	Each IMACD milestones not delivered on time as per the approved IMACD plan will be deemed a missed SLA	98%
	SLR Element Weighting Factor Allocation	50%

11.5.7 **Configuration management**

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

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

Configuration Management SLR	
Service Measure:	**Performance Target:**
Configuration Record Accuracy: Data accuracy – chosen sample of all configurations (hardware and software) tracked by the ACSA NMS tools	98%
Timelines of updates: Time to update configuration records	1 day after change to configuration
Measurement Interval:	Electronic audit, conducted quarterly from date of contract commencement
Measurement Tool:	ACSA Configuration management Tools
SLR Element Weighting Factor Allocation	30%

11.5.8 **Overall service satisfaction**

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

Table 40 – Overall Satisfaction SLR

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

11.5.9 Software/Firmware Refresh

Software refresh for all upgrades and new releases.

Table 41 – Software/firmware Refresh SLR

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

11.5.10 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.

Table 42 – SLA Measurement Exclusions

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 1 SLA Measurement Exclusions

12.0 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 also 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.

12.1 Principles

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

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

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

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

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

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

12.1.6 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.

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

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

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

12.1.10 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

12.2 **Definitions**

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

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

12.2.3 **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.

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

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

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

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

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

12.2.7.2 **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%).

12.3 **Methodology**

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

12.3.1.1 **Monitoring**

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

12.3.1.2 **Reports**

The Service provider shall report to ACSA its performance of the Services against SLAs on a monthly basis.

12.3.1.3 **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.

13.0 Meetings and Report Requirements

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

13.1.1 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

13.1.2 **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

13.1.3 **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 a platform for the provider to report on their performance.

Table 43 – Meeting definitions

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

Meeting Name and frequency	Participants and roles	Documents to be produced after meeting by Service provider
	· Senior Manager IT Infrastructure	
Annual review meeting	· ACSA Management Representative (chair) · Senior Manager IT Enterprise Applications · provider Senior Site Manager · provider Relationship Manager · provider administrator · Senior Manager IT Enterprise Applications	· Minutes of meeting · Action register for any open actions to be addressed · Risks and Issues register

Table 44 – Reporting definitions

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

Frequency	Report Name	Report Content	Due date	Submit to	Format	Meeting Name and frequency
	Project and IMACD updates	Installations completed including relocations and projects. Present detailed job cards.	One day before project status update meeting	ACSA Technical Lead & ACSA Project Manager	Email written report summary with supporting tables.	Weekly Project status update
	Data/wire centre areas of concern	Testing done on data/core/wire centres highlighting areas of concern Weekly to review previous weeks' reports	3 days before meeting	ACSA Management Representative	Email written report summary with supporting tables.	Weekly Service Review
Monthly	Consolidated Care Report	Monthly consolidated report · Spares Usage · Calendar month Incidents · Payment · Monthly services deliverables · SLA Report (performance against SLR's) · SLA improvement plan ·Service Credits	3 days before meeting	ACSA Management Representative	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
Quarterly						
	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 Management Representative	Email PDF document	Annual review meeting
	Contract adherence review	Summary of contract requirements and adherence thereof	3 days before annual review meeting	ACSA Management Representative	Email PDF document	Annual review meeting

Requested By

Seoka Nkunyane: Senior Manager Enterprise Applications

Signature …… Date……

Approved by:

Kelebogile Mosiane: Chief Technology Officer

Signature …… Date…….