TERMS OF REFERENCE:

ICASA 08/2026: APPOINTMENT OF A SERVICE PROVIDER AT THE INDEPENDENT COMMUNICATIONS AUTHORITY OF SOUTH AFRICA (ICASA) TO PROVIDE AN AUTOMATED SPECTRUM MANAGEMENT SYSTEM (ASMS) WITH A THREE (3) YEAR SUPPORT AND MAINTENANCE

Table of Contents

1 INTRODUCTION

The Independent Communications Authority of South Africa ("the Authority" or "ICASA") draws its mandate from the Electronic Communications Act (Act No. 36 of 2005, as amended) ("the ECA") and the Independent Communications Authority of South Africa Act (Act No. 13 of 2000, as amended) ("the ICASA Act")) to regulate radio frequency spectrum in the public interest.

The Authority is issuing this open bid to fulfil its mandate of regulating the radio frequency spectrum by procuring the Automated Spectrum Management System (ASMS).

2 BACKGROUND AND OBJECTIVES

The Authority is currently using an ASMS that does not meet its operational objectives and has contributed to a backlog in spectrum management processes. The existing system lacks efficiency, effective integration of critical components, and the necessary data integrity to support the spectrum management framework. To address these challenges, the Authority intends to implement a new ASMS with a proven track record of delivering reliable and effective performance.

The ASMS will optimise the Authority's management of the radio frequency spectrum, ensuring efficient and transparent processes for spectrum planning, licensing, type approval, service licensing, monitoring, and compliance. At the core of this ASMS is a platform designed for applicants and licensees, providing a streamlined, user-friendly interface for applying for, and managing various licenses with the Authority.

The objectives of the Authority for this open bidding project are:

- To acquire a fully customised, implemented, and commissioned ASMS;
- To ensure that the ASMS database contains current data that has undergone a thorough cleanup, verification, and consolidation process by the appointed service provider, either prior to or during the migration to the ASMS database;
- To provide comprehensive support for the ASMS and its usage, including maintenance, for a period of three (3) years following acceptance;
- To facilitate full upgrades of the ASMS to new software versions, including software patches, operating system, and database updates, as they become available, for a duration of three (3) years;
- To provide training for both administrative and technical users, ensuring that they are fully equipped to operate and maintain the ASMS immediately upon its acceptance and full implementation; and
- To train technical staff in the fundamentals of spectrum management embedded within the ASMS, in accordance with ITU spectrum management principles.

The ASMS should be compliant with the ECA and applicable regulations, such as:

- Radio Frequency Spectrum Regulations, 2015 as amended[1];
- Radio Frequency Spectrum Fees Regulations, 2010 as amended[2];
- Licensing Processes and Procedures Regulations for Class Licences, 2010[3], as amended;
- Licensing Processes and Procedures Regulations for Individual Licences, 2010[4], as amended;
- Type Approval regulations[5];
- Type Approval labelling regulations[6]; and
- Type Approval regulations[7].

3 SCOPE OF WORK

The following outlines the scope of work for the terms of reference related to the different modules of the ASMS. Each module is designed to integrate seamlessly, ultimately resulting in a competent ASMS. This system will effectively support the ICASA in executing its spectrum management mandate. Each module will address specific aspects of spectrum management, ensuring comprehensive coverage of regulatory requirements, technical standards, and operational efficiency necessary for effective oversight, allocation, and assignment of spectrum resources.

3.1 Client Portal

3.1.1 The client portal is to provide a secure, user-friendly online environment where applicants and licensees/certificate holders can submit and track applications and manage licences/certificates for radio frequency spectrum licensing, type approvals and service licensing.

3.1.2 The client portal should be web-based and supported for various browsers in common use.

3.1.3 The client portal must provide external stakeholders with the following functionality with regard to their user accounts:

3.1.3.1 User Account Creation and Management: Stakeholders should be able to easily create and modify user accounts as needed. This includes the ability to assign multiple usernames, set up profile information, and manage user permissions to ensure appropriate access levels.

3.1.3.2 Multi-Factor Authentication (MFA): The system must support multi-factor authentication to enhance security. This should include options for various authentication methods, such as SMS verification codes, email confirmations, or

[1] Published in Government Gazette No. 38641 (Notice 279 of 2015) on 30 March 2015, as amended by Notices No. 386 of 2015, 781 of 2016, 585 of 2019 and 737 of 2021.
[2] [2] Published in Government Notice No. 33495 of 2010, as amended by Notices No. 385 of 30 March 2015 and No. 280 of 30 April 2015
[3] Published in Government Gazette No. 33297 (Notice 526 of 2010) on 14 June 2010
[4] Published in Government Gazette No. 33293 (Notice 522 of 2010) on 14 June 2010
[5] Published in Government Gazette Number 36785, Notice number 871 on 26 August 2013
[6] Published in Government Gazette Number 36786, Notice number 872 on 26 August 2013
7 Published in Government Gazette Number 36792, Notice number 883 on 27 August 2013

authenticator apps, and require users to provide additional proof of identity when accessing their accounts.

3.1.3.3 Role-Based Access Control: The module must implement role-based access to facilitate both individual and corporate accounts. This means user permissions should be tailored to users' roles, enabling fine-grained control over who can access specific features and data within the system.

3.1.3.4 Secure Password Management and Account Recovery: There should be robust mechanisms for secure password management, including guidelines for password complexity, history encryption & reuse, number of unsuccessful attempts (i.e., three attempts) for account lock, inactive account lock and expiration period. Additionally, the module must include reliable, multiple account recovery processes/methods that enable users to regain access to their accounts almost instantly and securely in the event they forget their passwords or face other access issues.

3.1.4 The client portal must support the various applications as well as different features to manage licences/certificates for radio frequency spectrum licensing, type approvals and service licensing.

3.1.5 The applications and management options will be distinct for different types of applications as well as different service categories, each with its own:

3.1.5.1 Application forms,

3.1.5.2 Technical parameters,

3.1.5.3 Workflow,

3.1.5.4 Required documents,

3.1.5.5 Fees, and

3.1.5.6 Approval paths.

3.1.6 Each input, where possible, should be subjected to real-time data validation and integrity checks before submission. Enforce mandatory fields/documents to be populated/uploaded, and applications with incomplete information must not be allowed to be submitted. Mandatory fields/documents must be populated/uploaded, and incomplete information must be rejected and not allowed to be submitted beyond the capturer. The system must perform business rule validations where possible, data completeness checks, data accuracy and cross verifications (including GPS Coordinate location display and verification). The system should further keep an audit trail and log of information, and cater for error handling & exception integrity and flexible reporting capabilities on it.

3.1.7 The module should prompt the user to select the type of licence/certificate that it is applying for and dynamically load the appropriate application form. This form will include all specific fields and rules for the type of licence/certificate being applied for. Data validation will extend to fields in this form, such as frequency ranges, power limits, which are aligned to the radio frequency spectrum assignment plans for each band. Data captured should include integrity checks such as input validations with specific range and limits, type validation (numeric, alphabetical, or alphanumeric), and mandatory fields.

3.1.8 Moreover, the module must include an option to submit bulk applications (e.g., multiple fixed links within a single application) and subsequent assignments for the radio frequency spectrum.

3.1.9 The system must feature a wizard-based application process with step-by-step guidance. It should automatically populate existing data for consistency when applicable, validate mandatory fields, and allow users to upload supporting technical documents, including large files (limited to 100MB) of different formats (including PDF, XLSX).

3.1.10 The portal must provide an up-to-date, real-time display of the status of each application. This display should include clear and easily understandable status indicators that represent the current phase of the application process, such as:

3.1.10.1 Submitted: Indicates the application has been successfully submitted.

3.1.10.2 Under Review: Denotes that the application is currently being evaluated.

3.1.10.3 Awaiting Information: Signifies that additional information or documentation is needed from the applicant before proceeding.

3.1.10.4 Technical Evaluation: Refers to the stage where the application undergoes a technical assessment.

3.1.10.5 Pending Payment: Indicates that the application is awaiting the necessary payment to continue the processing.

3.1.10.6 Approved: Marks that the application has met all criteria and has been officially accepted.

3.1.10.7 Rejected: Signals that the application has not met the required standards and has been denied.

3.1.10.8 Cancellation: Internal/external users should be able to cancel incorrect applications and automatically reverse billing or credit notes related to the application or licence.

3.1.11 The system must be able to list all of a user's applications submitted and licences/certificates issued, as well as indicate relevant information about it, such as the status (expired, pending, active and cancelled), relevant dates, etc.

3.1.12 The portal must also calculate and present the total processing time that has elapsed since the initial submission of the application, giving applicants a comprehensive view of the duration of their application journey.

3.1.13 Specific escalation procedures should be established to address instances where an application surpasses the defined regulatory turnaround times.

3.1.14 The client module must support license management, allowing licensees to view and manage licenses/certificates effectively. It can allow for the amendment of certain information by themselves (such as contact details), while other information will require an amendment application process.

3.1.15 The client module must support mail/SMS alerts for status changes, pending information, payments, approvals, or rejections, provide a secure messaging interface for queries between applicants and the Authority, and automated reminders for outstanding tasks.

3.1.16 The system should automatically identify licenses that are due for renewal based on their expiry dates and status, and it must provide an option to trigger the license renewal process before the license expires. The specific notice period will depend on the type of licence.

3.1.17 Licensees should have the ability to print security-enabled licenses and certificates.

3.1.18 The portal must allow applicants to download licenses, rejection letters, authorisation letters, and invoices.

3.1.19 The portal should enable users to view payment statuses and outstanding balances, and to initiate online payments via a secure payment gateway.

3.1.20 The portal must allow users to edit captured data and upload documents at any stage whilst the application is in process. Directly after submission of an application, the appropriate application fee will be invoiced, and the user should be notified accordingly.

3.1.21 Amendments to licences/certificates should make it clear what parameters are being amended. If all parameters remain the same, then the applications should not be allowed to proceed.

3.1.22 The portal must provide an option for applicants to submit confidentiality requests through a configurable online form, together with the required supporting documentation.

3.1.23 The Client Portal should allow users to create profiles for third parties, with the necessary proxy, and submit them for approval. The portal should further allow users to submit applications on behalf of authorised third parties.

3.1.24 The Client Portal should allow the licensee to log requests for interference investigations, should their assigned spectrum be affected by such during implementation.

3.2 Spectrum Planning Module

3.2.1 This module is aimed at supporting the planning, allocation and efficient use of the radio frequency spectrum in accordance with the ITU Radio Regulations and Recommendations, National Radio Frequency Plan and any other framework put in place, such as the spectrum outlook.

3.2.2 The module shall be capable of importing and maintaining the ITU-R Table of Frequency Allocation and allowing updating of the National Radio Frequency Plan with incorporation of all the footnotes and those applicable nationally.

3.2.3 The module should allow authorised users to incorporate radio frequency spectrum assignment plans, ITU-R Recommendations and rules applicable to each and every spectrum band. The rules per spectrum band include the assignment methods (e.g., standard application procedure/first-come-first-served, market-based approach (beauty contest or auction)), moratoria, sharing conditions, guard bands, technology neutrality or restrictions. All these rules should be made available to the internal licensing module for action and to the client portal for read-only guidance.

3.2.4 The module should allow authorised users to capture and manage frequency migration plans by defining legacy services, target bands and transition timelines. This information is critical for the internal licensing module so that the bands under migration can be flagged during licensing evaluations, prevent the issuance of new licences where migration restrictions

apply, and support coexistence periods where applicable. Affected licensees and new applicants should be notified if a particular service is to be migrated via a client portal module.

3.2.5 The module should support in-band and adjacent-band compatibility studies, coexistence analysis between various services by making information available, such as on existing licensing assignment data, and monitoring data for historical spectrum usage within the specific band.

3.2.6 The spectrum planning module must integrate with:

3.2.6.1 Internal licensing module to provide applicable band rules, ITU-R references and migration alerts and to further enforce planning constraints during licensing evaluations.

3.2.6.2 Spectrum Monitoring and Compliance Module to receive spectrum utilisation and performance data.

3.2.6.3 Technical Database to store all allocations, planning and study datasets.

3.2.6.4 Client Portal: Flag the migration alerts, assignment methods and moratoria on the spectrum bands affected.

3.3 Spectrum Licensing Module

3.3.1 The internal licensing module provides the Authority's staff with a complete, end-to-end internal system for processing, evaluating, approving, issuing, renewing, amending, transferring, withdrawing and surrendering radio frequency spectrum licences across all service categories.

RFS Licensing Administration:

3.3.2 The system should expire licences where the licensees failed to renew their licences for a new licence year. Such a process must be done as per the prescribed procedures in the RFS regulations.

3.3.3 However, the system must differentiate between licences issued in accordance with a service licensing, as prescribed in Chapter 3 of the ECA, whereas such a licence does not expire on an annual basis but on a prescribed period, irrespective of whether the annual fees were paid or not.

3.3.4 Furthermore, renewal of a multi-year radio frequency spectrum licences for the provision of a service licences (Broadcasting and Electronic Communication Network Services) must be done six ("6") months before expiration.

3.3.5 Therefore, the module should notify internal users when the service licence associated with the radio frequency spectrum licence expires three months prior. Moreover, the system must also notify multi-year radio frequency spectrum licence holders that the linked service licence would expire twelve (12) months before expiry.

3.3.6 The system must have a configurable workflow capable of catering for new, renewal, amendment, transfer/transfer of control, cancellation/surrender applications.

3.3.7 In addition to the management allocating and reallocating for RFS applications, the module should have an efficient way for automatically allocating applications to users in accordance with present rules in the system within a specific financial year.

3.3.8 The tool should support polygon-based geographic spectrum assignments and licensing areas, including the creation, editing, import, export, and visualisation of polygons for service areas, coordination zones, and exclusion zones.

3.3.9 The internal spectrum licensing module is responsible for receiving and logging all applications submitted by licensees and applicants for various application types from the Client portal, as specified below:

3.3.9.1 New applications, including those submitted in accordance with the standard application procedure,

3.3.9.2 The licensing module should include a digital platform to receive time-bound applications, which use an extended application procedure (i.e., Invitation to Apply or Invitation to Pre-Register (ITP-R) process).

3.3.9.3 Authorisation for temporary use of RFS (such as for special events and state visits)

3.3.9.4 Trial or test of RFS licence

3.3.9.5 Amendment of existing RFS licence

3.3.9.6 Surrender/cancellation of the existing RFS licence

3.3.9.7 Withdrawal of the existing RFS licence

3.3.9.8 Transfer of existing RFS licences

3.3.9.9 Transfer of control of existing RFS licences

3.3.9.10 Renewal of RFS licences

3.3.9.11 Satellite/space segment registration applications

3.3.9.12 Registration of point-to-point links in the self-coordination block for E-band.

3.3.10 The typical service sub-module should include services allocated in accordance with the National Radio Frequency Plan, such as, but not limited to, the following:

3.3.10.1 Broadcasting: This encompasses terrestrial television and radio services according to the allocated spectrum bands.

3.3.10.2 Satellite: This includes satellite broadcast carriers, the space segment, Earth stations, VSAT terminals.

3.3.10.3 Mobile Services: This covers International Mobile Telecommunications and related technologies, as well as private mobile radio networks, etc.

3.3.10.4 Fixed services: This pertains to microwave/point-to-point Links and Point-to-Multipoint Systems

3.3.10.5 Maritime and Aeronautical Services: This includes ship stations, aircraft radios, beacons, recording of call signs, Maritime Mobile Service Identity (MMSI) and navigation aids.

3.3.10.6 Amateur radio services: This includes the licences for radio amateurs, including recording of call signs, to candidates who wrote and passed an examination to show their competence to operate on the amateur radio frequency bands.

3.3.10.7 Radio dealer certificates: The Authority must at all times maintain a list of all approved entities that install, repair, or sell radio apparatus in the country.

3.3.11 The appropriate application- and licensing fee(s) should be calculated automatically, based on the type of application as well as the technical information of the application and it will be based on predefined formulas that can be customised by a designated user.

3.3.12 Once submitted, each application should be routed to the appropriate departmental unit based on the service sub-module. The system should allow for the application to undergo a completeness verification process to identify any missing or incorrect information, and an internal reference number will be automatically assigned. The module should allow applications within the appropriate departmental unit, based on the service sub-module pool to be allocated to officials by the line manager or supervisor.

3.3.13 The categorised application types will be guided through a customizable workflow defined within the administrative module of the system. This workflow will support multi-level reviews, allowing different levels of management to evaluate and approve applications, thereby streamlining the decision-making process. The current spectrum licensing application processes are contained in **Appendices A and B**, for radiocommunication services and broadcasting services, respectively. These processes can be optimised as appropriate when implemented in the ASMS systems. For instance, there are other applications that are delegated to be processed and finalised by the regional offices, therefore those types of applications must be sorted and allocated as such.

3.3.14 The module must include a database of call signs from which assignments must be made to the different services in accordance with the ITU-approved ranges for South Africa. This database must be linked with the licensee details.

3.3.15 The module must include a database of registered point-to-point links in block A of the E-Band and allow external users to register links on this database as well as make this database available to all external users for self-coordination.

3.3.16 The module must include a database of MMSI numbers for the assignment to applicable maritime ship stations to the different services in accordance with the ITU-approved ranges for South Africa. This database must be linked with the licensee details.

3.3.17 The designated internal user(s) should have access to the above three databases (call signs, E-band Block A, MMSI) to make amendments or additions when necessary.

3.3.18 Decision and Issuance: Based on the technical or administrative analysis of the application and following a workflow process, a decision on the application should be made.

3.3.19 In cases where the application is recommended for approval, the internal licensing module should be capable of capturing the results of the technical or administrative analysis in accordance with the relevant legislative and regulatory frameworks. The module must accept input parameters that will be included in the radio frequency spectrum license and authorisation issued to the applicant. This includes, but is not limited to, details about the entity name, trading name, shareholding, contact information, notification addresses, license validity period, geographic coverage area, terms and conditions, license obligations (if applicable), service licence number (where applicable), type approval number and general conditions. Every licence issued should have a unique licence number assigned to it.

3.3.20 The spectrum licensing module needs to inform the service licensing module about the approval of the radio frequency spectrum application. No radio frequency spectrum licence should be issued without the approval of the service licence (broadcasting or electronic communication network service), where applicable.

3.3.21 Conversely, in instances where the application is rejected, the module must be able to accept input parameters that will be incorporated into the rejection letter, as well as any other relevant evidence (e.g., technical analysis results) needed to inform the applicant and notify the service licensing module about the rejection.

3.3.22 Internal users should be able to track each application throughout its lifecycle, gaining insights into its current stage, the department responsible, the individual assigned to manage it, and the total number of days it has been in the process. There should be an audit trail of each user's activity in processing the application.

3.3.23 To enhance accountability and efficiency, the system must automatically generate alerts when Service Level Agreement (SLA) timelines are at risk of being exceeded. This will include timely escalations to relevant internal stakeholders, along with regular reminders and notifications for any pending tasks requiring attention, ensuring no application is overlooked, and all deadlines are met.

3.3.24 The module should generate reports that cover more than just individual and departmental performance metrics. These reports should also include technical evaluation logs, assignments across various bands by province, district municipalities, and local municipalities, as well as details on licenses issued, renewed, amended, rejected, surrendered, or withdrawn.

3.3.25 The module should provide a database which includes, amongst others, a list of licences, expired licences, and their associated technical parameters categorised nationally, provincially, per district municipality, and local municipality.

3.3.26 The system should allow for the functionality to make public records available, such as applications, licences/certificates (that are not subject to confidentiality), etc.

3.3.27 The internal licensing module must integrate with:

- Client Portal: For application intake and sharing the application status updates.
- RF Engineering analysis module: To read and write all technical parameters, frequency plan, equipment lists, coverage and GIS data.

- Spectrum Planning module: To get an update on the frequency band assignment rules and receive alerts for migration.
- Monitoring and Compliance Module: To submit active assignment data and receive interference reports and spectrum utilisation per band.
- Financial Integration: No applications should reach the internal licensing module if the payments are not made and confirmed. Provide financial officers with the necessary access to reports and invoicing parameters.
- Service Licensing: There should be integration between the Spectrum Licensing Module and Service Licensing Module to record the service licences associated with the spectrum licences and vice versa.

RFS Engineering Module

3.3.28 The Authority requires a ready-made technical analysis tool that has been widely used by regulators worldwide. This tool will be utilised by designated users to conduct technical analyses of applications, as described in paragraph 3.3.9. The technical analysis tool is entirely dependent on the technical database and should have the following capabilities, but not limited to:

3.3.28.1 **Allotment management**: The analysis tool should have the capability for designated users to create, edit, and manage frequency allotments for different services. The technical parameters for each allotment should include the frequency band, bandwidth, channel spacing, maximum transmitter power, and service types, in line with applicable ITU-R channel plans. The allotments should be consistent with the National Radio Frequency Plan and Radio Frequency Spectrum Assignment Plans, and thus require an appropriate approval process to be effective.

3.3.28.2 **Frequency Assignment Calculations**: The tool should enable designated users to scan frequency availability within a specific band. The tool should allow authorised users to validate transmit power, bandwidth, location coordinates, and emission designators. Additionally, the tool should flag assignments outside national borders and those within coordination zones.

3.3.28.3 **Interference Analysis**: The tool should be capable of conducting interference analysis on all service types. This includes adjacent-channel checks, co-channel evaluations, intermodulation checks, protection ratios, and impacts on cross-border coordination.

3.3.28.4 **Coverage Analysis**: The tool must enable authorised users to conduct coverage predictions using various ITU-R propagation models. It should display service contours based on received signal strength, signal-to-noise ratio (SNR), and link budget analyses (including topographical link profile and Fresnel zone analysis). The results will be presented in an integrated Digital Terrain Model (DTM) and must allow overlaying the results in a Geographic Information System (GIS), including Google Earth.

3.3.28.5 **Prohibition areas**: The tool should be able to incorporate and display exclusion zones. Moreover, the tool should have the ability to flag applications that fall in areas where prohibition to frequency use apply, such as radio astronomy protection areas**.**

3.3.29 The tool should include map management features that allow users to overlay map layers, technical analysis output (Interference and coverage map display), display satellite imagery and topographic maps, and view administrative boundaries. Additionally, it should enable users to save customised map views and export them as image files or report attachments, such as KMZ and KML files.

3.3.30 Authorised users should have access to maps of South Africa and its neighbouring countries for coordination purposes.

3.3.31 The granularity of the digital terrain maps should at least be at 20m DEM, with an option of 100m DEM as well. The use of clutter maps should also be available.

3.3.32 ITU-R tools integration: The tool should be capable of reading BR-IFIC data and facilitate the updating of ITU Master International Frequency Register (MIFR) with approved assignments.

3.3.33 The RFS Engineering module must integrate with:

- Client Portal: For application intake and sharing the application status updates.
- Technical Database: To read and write all technical parameters, frequency plan, equipment lists and coverage and GIS data.
- Spectrum Planning module: To get an update on the frequency band assignment rules and receive alerts for migration.
- Monitoring and Compliance Module: To submit active assignment data and receive interference reports and spectrum utilisation per band.

3.4 Type Approval (Equipment Standardisation)

3.4.1 The intent of this module is to ensure that all electronic communication equipment sold/used within the country complies with the Type Approval regulations and operates within authorised spectrum parameters, thereby preventing harmful interference, supporting efficient spectrum use and strengthening network integrity.

3.4.2 The Type Approval applications must be submitted through the Client Portal, supporting the different application types, which are Radio Frequency and Telecommunication Terminal Equipment (TTE). These two types of application must be classified as:

3.4.2.1 New – An application for any electronic communication equipment that has not been approved before by the Authority.

3.4.2.2 Variant- An application where a modification was made on the equipment that was approved by the Authority for the same supplier.

3.4.2.3 Provisional – An application for a temporary approval by the authority for trials, testing, demonstration, and research purposes.

3.4.2.4 Simplified – An application that is followed in the event where the equipment has already obtained Type Approval from the Authority.

3.4.2.5 Amendment – An application to amend user profile and approved certificates.

3.4.2.6 Certificate transfer – An application to transfer a certificate from one licensee to another.

3.4.3 The module should allow for an option to withdraw a certificate, which is initiated by the Authority**.**

3.4.4 This module must be able to review and evaluate equipment details captured in the client portal, such as equipment name, model, equipment category, equipment description and all technical parameters. Applicants must pay the applicable Type Approval fee before applications can be evaluated.

Evaluation of application:

3.4.5 The applications would go through a flexible multi-stage evaluation workflow which includes administrative completeness checks, technical conformity checks and management approval. This workflow will support multi-level reviews, allowing different levels of management to evaluate and approve applications, thereby streamlining the decision-making process. The current type approval application processes are contained in **Appendix C**. These processes can be optimised as appropriate when implemented in the ASMS systems.

3.4.6 Internal users should be able to track each application throughout its lifecycle, gaining insights into its current stage, the department responsible, the individual assigned to manage it, and the total number of days it has been in the process. There should be an audit trail of each user's activity in processing the application.

3.4.7 To enhance accountability and efficiency, the system must automatically generate alerts when Service Level Agreement (SLA) timelines are at risk of being exceeded. This will include timely escalations to relevant internal stakeholders, along with regular reminders and notifications for any pending tasks requiring attention, ensuring no application is overlooked, and all deadlines are met.

3.4.8 The module should generate reports that cover more than just individual and departmental performance metrics. These reports should also include technical evaluation logs, type-approved equipment across various bands for each application type, as well as details on certificates issued, amended, rejected, or withdrawn.

3.4.9 The module should have an efficient way for automatically allocating applications to type-approval specialists equitably within a specific financial year, taking into account the applications already processed. In addition to the system performing auto-allocation of applications, management must be able to allocate and reallocate type approval applications.

3.4.10 The application evaluation page must show fields such as Application Number, Application Type, Equipment Type, Certificate Holder Details, equipment name, model, brand, equipment category, equipment description, original equipment manufacturer details, local maintenance address, and all technical parameters.

3.4.11 For Variant and Simplified applications, the user must be able to search for the approved Master Type Approval Certificate.

3.4.12 The management approval page must show fields such as the Application Number, Application Type, Equipment Type, Certificate Holder Details, equipment name, model, brand, equipment category, equipment description, original equipment manufacturer details, local maintenance address, and all technical parameters.

3.4.13 The module must give applicants an option to make administrative and technical amendments.

3.4.14 The module must indicate all the certificates that are affected by the administrative amendment application and give the Type Approval management the option to do a bulk regeneration of the certificates affected by the changes to reflect the latest information.

3.4.15 The module must, to the extent possible, identify the Type Approval specialist who approved the original application and automatically assign the technical amendment application to their name.

3.4.16 The module must have a functionality to recreate legacy Type Approval Certificates.

3.4.17 The module must have the ability to automatically update the list of approved equipment and share the same with the Internal Licensing Module, Technical Database and Monitoring and Compliance Module.

3.4.18 The system should allow for the functionality to make a list of approved type-approved equipment public.

3.4.19 The module should allow for integration with the Spectrum Licensing Module to ensure that the equipment to be used with those licences are Type-Approved.

3.5 Service Licensing

3.5.1 The Service Licensing Module is aimed at providing an end-to-end, automated platform to manage the full-service licensing lifecycle, including the submission, processing, evaluation, and approval of applications for new registrations, renewals, amendments, transfers, surrender of licenses, and licence exemptions for class and individual licences.

3.5.2 The licensing module should include a digital platform to receive time-bound applications, which use an extended application procedure (i.e., Invitation to Apply (ITA) or Invitation to Pre-Register (ITP-R) process).

Service Licensing Administration:

3.5.3 The internal service licensing module is responsible for receiving and logging all Class and Individual applications submitted by licensees and applicants for various licence types from the Client portal, as specified below:

3.5.3.1 New service licences, which would also include ITA and ITP-R processes

3.5.3.2 Special events licence

3.5.3.3 Trial or test of service licence

3.5.3.4 Amendment of existing service licence

3.5.3.5 Surrender/cancellation of the existing service licence

3.5.3.6 Withdrawal of the existing service licence

3.5.3.7 Transfer of existing service licences

3.5.3.8 Transfer of control of existing service licences

3.5.3.9 Renewal of service licences

3.5.3.10 Licence exemption

3.5.4 Once submitted, each application should be routed to the appropriate departmental unit based on the service type. The system should allow for the application to undergo a

completeness verification process to identify any missing or incorrect information, and an internal reference number will be automatically assigned. The module should allow applications within the appropriate departmental unit, based on the service type pool to be allocated to officials by the line manager or supervisor.

3.5.5 The service-type applications would go through a flexible multi-stage evaluation workflow, which includes administrative completeness checks and management approval. This workflow will support multi-level reviews, allowing different levels of management to evaluate and approve applications, thereby streamlining the decision-making process. The current service licensing application processes are contained in **Appendices B, D and E** for class and individual applications, respectively. These processes can be optimised as appropriate when implemented in the ASMS systems.

3.5.6 Internal users should be able to track each application throughout its lifecycle, gaining insights into its current stage, the department responsible, the individual assigned to manage it, and the total number of days it has been in the process. There should be an audit trail of each user's activity in processing the application.

3.5.7 To enhance accountability and efficiency, the system must automatically generate alerts when Service Level Agreement (SLA) timelines are at risk of being exceeded. This will include timely escalations to relevant internal stakeholders, along with regular reminders and notifications for any pending tasks requiring attention, ensuring no application is overlooked, and all deadlines are met.

3.5.8 The module should generate reports that cover more than just individual and departmental performance metrics. These reports should also include metrics on applications assessed by application type, and approved applications by local, district municipality, and province. The module should be able to produce a report on which licences are due for renewal, shareholding, Broad-Based Black Economic Empowerment and Historically Disadvantaged Group requirements.

3.5.9 The module should provide a database which includes, amongst others, a list of licences, expired licences, and their associated licence conditions categorised nationally, provincially, per district municipality, and local municipality. The module should also provide functionality to make public records available, such as applications, licences/certificates (that are not subject to confidentiality), etc.

3.5.10 The module should further enable monitoring, reporting, and statistical analysis to support management oversight, regulatory accountability and continuous improvement of the service licensing processes, including keeping up to date with regulatory developments.

3.5.11 Decision and Issuance: Based on the analysis of the application and following a workflow process, a decision on the application should be made.

3.5.12 In cases where the application is recommended for approval, the internal service licensing module should be capable of capturing the analysis in accordance with the relevant legislative and regulatory frameworks. The module must accept input parameters that will be included in the service license issued to the applicant. This includes, but is not limited to, details about the entity name, trading name, shareholding, contact information, notification addresses, license validity period, coverage service area, terms and conditions, license obligations (if applicable), radio frequency spectrum licence number (where applicable) and general conditions. Further, the service licensing module needs to inform the spectrum licensing

module about the approval of the service licence application. No service licence should be issued without approval of the spectrum licence, where applicable.

3.5.13 Conversely, in instances where the application is rejected, the module must be able to accept reasons for rejection and issue the rejection letter. Further, the spectrum licensing module must be notified about the rejection.

3.5.14 The renewal of a service licence for the provision of Broadcasting, Electronic communications services and Electronic Communication Network Services must be done six ("6") months before expiration.

3.5.15 Therefore, the system must notify service licence holders at 12 months and at 9 months prior to licence expiry to renew their licences.

3.6 Spectrum Monitoring and Compliance

3.6.1 The ASMS must be able to integrate with fixed spectrum monitoring stations, mobile monitoring units by supporting ingestion of monitoring data from these systems through real-time and batch-uploading. The ASMS must provide interfaces to ingest data from existing and future spectrum monitoring systems.

3.6.2 The module must be able to correlate monitoring data with active spectrum licences and technical parameters to detect and flag transmissions without valid licences, operations outside licensed parameters and expired or suspended licences still transmitting.

3.6.3 The module should be able to generate a compliance report that may be used in further investigation.

3.6.4 The integration should be maintained with the spectrum licensing and planning modules.

3.7 Requirements common to various Modules

3.7.1 Finance

3.7.1.1 Financial Integration: No applications should reach the internal licensing module if the payments are not made and confirmed as described in the sections above.

Integration to Financial System & Billing Workflow

3.7.1.2 The ASMS must establish a secure, real-time, and bidirectional integration with ICASA's Financial System. This integration shall serve as the authoritative financial backbone for all radio frequency spectrum, broadcasting, service, and type approval fee processing. The Authority requires a modern, API-driven integration that minimises custom middleware, reduces batch-file dependencies, and enables end-to-end automation of financial processes. The integration must allow for daily bulk batch creation instead of a single batch for a single transaction.

3.7.1.3 The ASMS should automate the calculation, invoicing, payment, collection, and reconciliation of all radio frequency spectrum, service licensing, and type approval fees through proforma invoices generated in JDE.

Billing

3.7.1.4 The ASMS should automate the calculation of fees and integrate the information into the financial system for the creation of proforma invoices and credit notes. The system must

have a mandatory field for attaching proof of payment (PoP). Proof of payment should be automatically be recorded when payment is made online using the credit card.

Payment confirmation/approval by finance

3.7.1.5 The application will be assigned to the finance task pool for the processing of payment confirmation.

3.7.1.6 Finance will verify the PoP validity and confirm payment. All applications with confirmed payments must automatically be assigned to the relevant licensing pool (Spectrum Licensing, Type Approval or Services Licensing). The approval of payment must trigger the conversion of the proforma invoice into an invoice. (The proforma will be auto-deleted and replaced by the invoice).

3.7.1.7 The module must allow for bulk payment approvals and bulk assignment of the approval tasks to the team members, instead of a single transaction per application process.

3.7.1.8 The system should allow Finance to reject an invalid PoP by selecting predefined reasons such as invalid payment, previously used, short payments, etc. The rejection must trigger a notification to the applicant to allow the application to correct and re-upload the PoP.

3.7.1.9 Should the applicant not attend to the request to re-upload a valid PoP in a specified time, this should automatically lead to the rejection of the application, and a rejection letter should be sent to the applicant accordingly.

Reporting

3.7.1.10 The module should generate reports that cover more than just individual and departmental performance metrics. These reports should also report on approved and rejected applications within a specified period, and integration exceptions reports between the ASMS system and ICASA's financial system.

Step-by-Step Logic Flow

3.7.1.11 Below is a step-by-step description of the logic flow:

- *Application Submission:* User submits application.
    - *Debtor Status:* No. (Proforma Invoice generated in JDE , but this is usually a "Statistical" or "Quotation" document, not an Account Receivable (A/R) document).
- *Payment & Verification:* User pays; Finance clicks "Confirm Proof of Payment."
    - *Debtor Status:* Pending. (Money is received, but the official revenue recognition hasn't happened yet)
- *Final Approval (The Trigger):* Finance user approves the application.
    - *Action:* The ASMS sends the "Finalise Billing" command to the Integration Layer.
- *JDE Processing:*
    - JDE receives the command.

- JDE creates the Final Invoice (This transaction creates the accounting entry: *Debit Debtors Control / Credit Revenue*).
- JDE sends a success response back to ASMS with the Final Invoice Number.

- *ASMS Update:*
  - *Debtor Status:* Yes. (The system now links the Applicant/Licensee to the Final Invoice Number in JDE, effectively recognising them as a debtor for that specific transaction).

3.7.1.12 Proforma Invoice Generation: Upon application submission, the ASMS must forward the required information to the JDE system so that a proforma invoice can be created. The ASMS must upload this invoice from the JDE system and issue it to the applicant for payment via email and SMS. The invoice must also be made available to the applicant via the Client Portal to facilitate payment.

3.7.1.13 Two-Step Invoice Approval: Final (Official) invoices must only be generated and interfaced to JDE after a two-step verification:

3.7.1.13.1 Financial Approval: A finance user must approve the transaction within the ASMS, confirming the correct payment amount has been received for the correct Proforma/Application.

3.7.1.13.2 Bulk Operations: The system must allow authorised users to approve multiple applications at the same time (and subsequent final invoicing) simultaneously.

3.7.1.14 Data Synchronisation: The ASMS must integrate bi-directionally with JDE (and other financial systems) via RESTful APIs to track revenue and synchronise payment statuses.

Automated Billing & Fee Calculation

3.7.1.15 Dynamic Fee Engine: Administrators must be able to define and manage fee schedules based on service type, sub-category, frequency band, and location (province/district), in alignment with national regulations (Spectrum Fees, General Licence Fees, Type Approval).

3.7.1.16 Proration Logic: The system must automatically calculate pro-rata fees for mid-term applications, temporary licenses, or license variations to ensure accuracy on both Proforma and Final invoices.

3.7.1.17 Payment Lock: The system must prevent the submission or processing of applications if the required payment has not been satisfied (i.e., the system checks for payment against the Proforma before allowing final submission/approval).

3.7.1.18 Manual Adjustments: The system must allow officers to enter offline or manual fee entries for cash payments or complex adjustments, which may generate corresponding Proforma or Credit notes in JDE.

Online Payments & Reconciliation

3.7.1.19 Multi-Channel Payment Gateway: The ASMS must integrate with various online payment gateways (Credit/Debit Card, EFT, Mobile Money, Government Portals, Post office) via RESTful APIs. The payment page should clearly reference the Proforma Invoice number.

3.7.1.20 Automated Status Updates: Upon successful payment, the system must automatically:

- *Match the payment to the outstanding Proforma Invoice.*
- *Update the payment status in the Client Portal and Licensing Module.*
- *Trigger the creation of the Final Tax Invoice/Receipt in JDE.*
- *Generate and dispatch an electronic final receipt to the applicant.*
- *Send confirmation notifications.*
- *Release the licence document for issuing to the applicant.*

3.7.1.21 Reconciliation Tools: The system must support manual reconciliation processes for cash or other offline payments received outside the gateway and match them against the issued Proforma Invoices.

Financial Administration & Reporting

3.7.1.22 Customizable Reporting: The system must provide web-based, downloadable reports (Excel/PDF) including:

- Revenue reports filtered by service type, sub-module, frequency band.
- Payment histories for individual licensees and corporate clients.
- Invoicing Reports: Reports distinguishing between Proforma Invoices issued and Final Paid Invoices.
- Credit Note reports.
- Aging Analysis: Applications approval aging report by user, displaying associated License Numbers and both Proforma/Invoice Numbers.
- Database Status Report: Filterable reports based on database fields such as Custom fields, Active status, Cancelled, and Expired.

3.7.1.23 Audit & History: The system must capture a historical trail of all financial queries, adjustments, and user actions, including the lifecycle of a Proforma converting to a Paid Invoice.

Security & Compliance

3.7.1.24 Data Protection: All financial data must be encrypted in transit (TLS/SSL) and at rest (Database Encryption).

3.7.1.25 Access Control: Strict role-based access control (RBAC) must be implemented to ensure only authorised financial officers within designated roles can view or modify financial data.

3.7.1.26 Audit Trails: The system must maintain a complete, immutable audit log for all financial transactions, adjustments, and reconciliations (Proforma creation, Payment matching, Final Invoice generation). The audit trail must at a minimum, record information of who, what, when, with old and new values.

3.7.1.27 Regulatory Adherence: The financial module must comply with national financial regulations and cybersecurity standards.

3.7.2 IT requirements

3.7.2.1 Strategic Direction: ICASA has adopted a Cloud-First strategy prioritising cloud computing solutions over traditional IT infrastructure to enhance agility, scalability, and cost efficiency.

3.7.2.2 If the proposed ASMS solution can only be deployed on the OEM's data centre residing in South Africa, the bidder will be responsible for the network security, backups, disaster recovery and business continuity.

Cross-Functional Requirements

3.7.2.3 *Accessibility:* The system must be fully accessible via any modern browser, compatible with Windows, macOS, iOS, Android and other platforms. Must support seamless functionality on devices including desktops, laptops, mobile phones, and tablets.

3.7.2.4 *Availability:* Guaranteed minimum system uptime of 99.95%. Clearly defined processes for planned downtime, including communication protocols and scheduled maintenance

3.7.2.5 *Deployment Mode:* Public Cloud or Private Cloud or Hybrid and data residency requirements (data must remain in South Africa)

3.7.2.6 *Performance*: The system must deliver consistent, acceptable response times for typical user interactions under normal operating conditions and must be designed to scale effectively as user volumes and transaction loads increase. The system must support a minimum of 1000 concurrent users without material degradation of service. Response times for routine and business-critical activities, including application processing, normal transactions, invoice generation, engineering analysis functions, map-based operations, searches, reporting, and other standard system functions, must remain within agreed operational performance thresholds. The solution must include documented scalability options, capacity management processes, and performance monitoring capabilities to support increased user demand over time. It must also provide mechanisms for caching, temporary storage, and session recovery for transactions in progress, ensuring that users do not have to recapture application information or restart a transaction if the session is interrupted due to connectivity, system, browser, or other unexpected disruptions.

3.7.2.7 *Reliability:* The system must use a resilient, fault-tolerant architecture to minimise service disruption. Critical components must avoid single points of failure, including applications, databases, integrations, storage, networks, security services, and infrastructure. The solution must support high availability through redundancy, load balancing, automated failover, health checks, monitoring, and alerts. Components must recover gracefully from failures without compromising service availability or integrity. The system must include strong error handling, transaction integrity, retry processing, queuing, and duplicate-processing prevention. Reliability controls must be tested and evidenced during system acceptance, including failover, resilience, and fault-handling scenarios.

3.7.2.8 *Usability:* The system must provide an intuitive, accessible, and user-friendly interface that follows recognised UX/UI best practices and supports efficient, consistent, and error-minimising user interactions across all modules. The user interface must be designed in accordance with applicable usability and accessibility standards including the Web Content Accessibility Guidelines (WCAG) 2.1 AA. The interface must accommodate both internal and external users through clear navigation, consistent layouts, plain-language prompts, contextual guidance, meaningful error messages, logical workflow progression, and responsive design for commonly used devices and browsers.

3.7.2.9 Data Ownership and Portability: All data, including but not limited to operational, transactional, metadata, and derived data, stored, processed, or generated within the system shall remain the sole and exclusive property of ICASA at all times. No rights, title, or interest in such data shall transfer to the service provider under any circumstances. ICASA

shall retain unrestricted access to its data at all times, including during normal operations, transition periods, and upon termination or expiry of the agreement. The service provider shall ensure that ICASA can, at any time and without undue delay or additional cost, securely extract and export its data in full. Such data must be provided in commonly used, machine-readable, and non-proprietary formats to enable seamless portability and reuse. Upon termination or expiry of the agreement, the service provider shall provide full cooperation and support to facilitate the secure and complete transfer of all ICASA data to ICASA or its nominated third party, without vendor lock-in or degradation of data integrity.

3.7.2.10 *Software Licensing and Cost Transparency:* The service provider shall clearly define and document the software licensing model, including the basis of licensing (e.g., user-based, subscription-based, capacity-based, or enterprise-wide), and all applicable terms and conditions. The service provider shall provide a fully itemised and transparent pricing schedule, detailing all costs associated with the solution, including but not limited to: Initial acquisition and implementation costs, Recurring subscription or licensing fees, Maintenance and support fees, Upgrade and enhancement costs, Scalability and expansion costs. All fees, charges, and potential cost drivers shall be explicitly disclosed upfront. The service provider shall not impose any undisclosed, hidden, or additional charges beyond those expressly agreed to in the contract. All fees, charges, and potential cost drivers shall be explicitly disclosed upfront. The service provider shall not impose any undisclosed, hidden, or additional charges beyond those expressly agreed to in the contract. ICASA reserves the right to audit and verify all licensing and billing information to ensure compliance with agreed pricing terms and transparency obligations.

Security and architecture - IT

3.7.2.11 Regulatory Adherence: The system must comply with all applicable national laws, regulatory requirements, and organisational policies, including financial regulations.

3.7.2.11.1 Payments standard (PCI DSS) (mandatory).

3.7.2.11.2 Data protection legislation (POPIA), (mandatory).

3.7.2.11.3 ICASA cybersecurity Policies and standards (ISO 27001 framework, CIS controls for configurations standard) (mandatory).

3.7.2.11.4 Service provider must be able to provide ICASA with System and Organisation Controls 2 (SOC2) reports or equivalent and must be on an annual basis for the duration of the contract (mandatory).

3.7.2.12 The above compliance must be enforced across all system modules and supported by appropriate controls, monitoring, and reporting mechanisms. If the system is hosted at a 3rd party datacentre, the SOC2 report for the 3rd party datacentre must also be provided annually.

3.7.2.13 Security Monitoring: The system must be able to integrate with (SIEM) security incident management processes. Audit Trails: The system must maintain a complete, immutable audit log for all system activities, transactions, and data changes across all modules. This includes, but is not limited to, financial processes (e.g., proforma creation, payment matching, invoice generation), licensing actions, user administration, and configuration changes. The audit trail must, at a minimum, capture: the user identity (who), the action performed (what), the date and time (when), and the details of the change, including old and new values where applicable. Audit logs must be tamper-proof, securely stored, and retained in accordance with organisational policies and regulatory requirements.

3.7.2.14 The system must be able to produce regular reports on back-end administrative activities changes.

3.7.2.15 Patch Management: The service provider will be required to perform regular patch management to ensure all components remain secure and up to date. The Authority will perform regular vulnerability assessment and penetration tests and the Service Provider will be required to remediate the findings with no additional cost.

3.7.2.16 Session Management & Timeout: The system must enforce secure session management, including automatic session timeouts and re-authentication for sensitive actions.

3.7.2.17 API & Integration Security: All system integrations and application programming interfaces (APIs) must be designed, implemented, and managed using secure integration principles. Access to APIs must be strictly controlled through strong authentication and authorisation mechanisms, such as OAuth 2.0, RESTful API, API keys, or token-based security, and aligned with role-based access control (RBAC).

3.7.2.18 Access Control: Role-based access control (RBAC) must be implemented across all system modules to ensure that access to data and functionality is restricted to authorised users based on their assigned roles. Integrated with enterprise identity systems (e.g., Active Directory/Azure AD). Access rights must follow the principle of least privilege and enforce segregation of duties, ensuring users can only view or modify information necessary for the performance of their responsibilities, including but not limited to financial data.

3.7.2.18.1 Multi-Factor Authentication (MFA): The system must enforce multi-factor authentication (MFA) for both internal and external users to enhance access security. MFA must require users to provide two or more independent forms of authentication (e.g., something they know, have, or are) when accessing the system, particularly for sensitive functions and data. Supported authentication methods should include secure options such as authenticator applications (preferred), push notifications, hardware tokens, and, where necessary, SMS or email-based verification. MFA enforcement should be risk-based, with stricter controls applied to privileged users, remote access, and high-risk transactions.

3.7.2.18.2 Secure Password Management and Account Recovery: There should be robust mechanisms for secure password management, including guidelines for password complexity, history encryption & reuse, number of unsuccessful attempts for account lock, inactive account lock and expiration period. Additionally, the module must include a reliable account recovery process that enables users to regain access to their accounts securely in the event they forget their passwords or face other access issues.

Integration & Interoperability

3.7.2.19 The ASMS must include a dedicated Integration and Interoperability Module that enables secure, scalable, and standards-based integration with internal modules, external enterprise systems, financial platforms, monitoring systems, geospatial services, and future ecosystem partners.

3.7.2.20 The ASMS architecture must be agnostic of downstream external systems and must not contain hardcoded dependencies on any specific financial platform, including JDE, within the core application code. Integration with JDE must be implemented through a dedicated financial-system adapter, while the architecture must allow future adapters for other enterprise resource planning or financial systems, including SAP, Oracle Financials, or custom ERP platforms, to be developed and deployed with minimal or no changes to the ASMS core financial engine.

3.7.2.21 Communication with external financial systems must be resilient and asynchronous, using a message queue or equivalent integration mechanism. Temporary unavailability of an external financial system must not block or degrade the core ASMS application. The system must support retry mechanisms, exception handling, reconciliation controls, and idempotency keys to prevent duplicate transaction processing during retries.

3.7.2.22 The ASMS must provide, at a minimum, integration interfaces for the following:

3.7.2.23 Financial Systems: Integration with JDE for automated invoicing, payment status updates, payment reconciliation, receipts, credit notes, and related financial transaction processing, with support for future financial-system adapters.

3.7.2.24 External Spectrum Monitoring Systems: Integration with fixed spectrum monitoring stations, mobile monitoring units, and future monitoring platforms to support real-time and batch ingestion of monitoring data.

3.7.2.25 Geospatial Services: Support for standard geospatial protocols and formats, including Web Map Service (WMS), Web Feature Service (WFS), KML, KMZ, Shapefile, and other commonly used GIS data exchange formats.

3.7.2.26 Internal ASMS Modules: Integration across the Client Portal, Spectrum Planning, Spectrum Licensing, Service Licensing, Type Approval, Finance, Monitoring and Compliance, Technical Database, Reporting, Workflow, and System Administration modules.

3.7.2.27 Future Integration Interfaces: The architecture must support additional integrations without requiring major changes to the ASMS core application.

3.7.2.28 All integrations must be auditable, traceable, and monitored. The system must maintain complete integration logs, including message status, transaction references, timestamps, source and destination systems, success and failure outcomes, retries, exceptions, and reconciliation results. Integration failures must generate alerts and be available for reporting and operational support.

3.7.2.29 **System administration functionality**

3.7.2.30 User Account Management: The system must provide controlled and auditable user account management capabilities to support the full user lifecycle, including account creation, modification, and deactivation. All user account activities must be subject to appropriate approval workflows and governance controls. Each user must be assigned a unique user identity to ensure accountability and traceability; shared or multiple user accounts must not be permitted. User profiles and permissions must be centrally managed in alignment with role-based access control (RBAC), enforcing the principles of least privilege and segregation of duties. The system must maintain a complete audit trail of all user management activities, including account creation, role assignment, permission changes, and deactivation, and must support periodic access reviews to ensure continued appropriateness of access rights.

3.7.2.31 The system should be able to assign roles with set dates of start and expiry.

3.7.2.32 The system shall provide configurable, auditable reporting on all back-end administrative activities and configuration changes, with the ability to generate periodic and on-demand reports for governance, compliance, audit and security monitoring purposes.

3.7.2.33 The ASMS should provide the Authority with tools to manage users, system parameters, workflows, access controls, and overall governance, ensuring smooth operations, security, and compliance.

Database Administrator functionality

3.7.2.34 The system must maintain comprehensive, tamper-evident audit trails for all database administrator activities, including privileged access, database configuration changes, schema modifications, user and role administration, data creation, updates, deletions, backup and restore activities, patching, maintenance tasks, and any direct database-level changes. Audit logs must capture the database administrator identity, action performed, affected database object or record, date and time stamp, source location or device where applicable, and before-and-after values for data changes. These logs must be protected from unauthorised modification or deletion and must be available for security monitoring, compliance reporting, forensic investigation, and audit review.

Data Governance, Integrity, and Reporting Standards

3.7.2.35 Data Governance: The system must implement robust data governance frameworks to ensure that data is managed as a controlled organisational asset. Data access, usage, and distribution must be governed by established policies and aligned with role-based access control (RBAC) and regulatory requirements. The system must support controlled data import and export capabilities in standard formats (e.g., JSON, CSV, XML, GIS, Excel), ensuring that all data exchanges are secure, authorised, and auditable. Data classification and handling procedures must be enforced to protect sensitive and confidential information.

3.7.2.36 Data Integrity: The system must ensure high levels of data integrity, accuracy, and consistency across all system components. Appropriate validation rules and controls must be implemented to prevent invalid, duplicate, or inconsistent data entries. The database must support version control and maintain historical records for key entities, including frequency allocations, licences, and technical parameters, enabling full traceability of changes over time. All data changes must be captured in comprehensive audit trails, recording creation, modification, and deletion activities, including user identity, timestamps, and before-and-after values where applicable.

3.7.2.37 Reporting Standards: The system must provide standardised, accurate, and timely reporting capabilities to support operational monitoring, performance management, and strategic decision-making. Dashboards must provide real-time visibility into key performance indicators, including applications in queue, applications assigned per authorised user, processing times per service type, bottlenecks and workflow inefficiencies, SLA compliance and breaches, Trends in licence applications and issuance. The system must generate comprehensive reports, including technical evaluation logs, Spectrum assignments across frequency bands, Geographic distribution (province, district, local municipalities), Licence lifecycle statuses (issued, renewed, amended, rejected, surrendered, withdrawn). Reporting outputs must be consistent, auditable, and exportable in standard formats, and support integration with external reporting and business intelligence tools where required.

3.7.3 Workflow and Decision Making

3.7.3.1 This section describes some of the functionality related to application workflow and the recording of decision-making that is common to the Spectrum Licensing, the Type Approval, and the Service Licensing modules.

3.7.3.2 The design of a workflow pathway needs to be flexible in setting up. Changes to the workflow pathways should only be made by the system administrator.

3.7.3.3 The system must implement the prioritised tiering approach to allocate applications for processing upon applications having been verified for completeness and accuracy. The application tiering system is as follows:

3.7.3.3.1 Tier 1 – The modules should have an efficient way for automatically allocating applications to designated users equitably within a specific financial year, taking into account the applications already processed.

3.7.3.3.2 Tier 2 - Management users must be able to assign and reassign applications to their respective team members.

3.7.3.3.3 Tier 3 - The internal users should be able to take an application from a generic pool within their designated sub-module into their own task/pool.

3.7.3.4 Users will then be able to edit the application parameters and process the application further by selecting one of the following options:

3.7.3.4.1 Request corrective action from a preceding user or the applicant

3.7.3.4.2 Analyse and process the application by recommending approval or rejection. The Application, with the recommendation, will then follow the appropriate workflow, culminating in a decision.

3.7.3.5 Each type of application will be considered according to a predefined workflow that identifies the appropriate departmental units involved in processing the application without manual sorting.

3.7.3.6 The system should have the ability to send email or sms notifications to either internal or external users (if required) at certain handover points.

3.7.3.7 Based on the technical or administrative analysis during the processing of the application, the application will proceed in accordance with the prescribed workflow, which will include approval/rejection of the application in accordance with the Delegation of Authority Framework of the organisation. Licences/Certificates can be issued for applications that are approved, while rejection letters will be issued for applications that are declined.

3.7.3.8 In the case of a rejection, the system must have the functionality to automatically generate a rejection letter. The rejection letter will be generated according to a template that can be updated, and the letter should capture the specific reasons for rejection.

3.7.3.9 In the case of approval, Licence/Certificate issued by the respective modules must have a security feature like a QR Code so that the ICASA officials and other authorised persons can scan the certificate to retrieve all essential information and verify the validity of the Licence/Certificate.

3.7.3.10 For transfer applications, the respective modules must give licence/certificate holders the option to do transfers. The transferee must already be registered on the client portal, to provide the applicant (the transferor) the option to identify the transferee from a dropdown list.

3.7.3.11 The respective modules must have a workflow process to withdraw a Licence/Certificate.

3.7.3.12 The module must allow the manager/supervisor to cancel applications.

3.7.3.13 The system should allow for the upload of comments and documents by internal or external staff during the processing of tasks. These comments and documents should be available in subsequent tasks and downloadable.

3.7.3.14 The system should have the ability to search the database of licences/certificates on parameters such as: licence number, frequencies, call signs, stations, certificate numbers, equipment name, etc.

3.7.3.15 The system should accurately track and display or report the amount of time spent at each individual stage of the application workflow, providing insights into where delays may occur. Accordingly, managers should be able to view the workload of their team members in these reports.

3.8 Project Implementation and Support Requirements

3.8.1 The service provider must provide, as aligned to section 4 below:

3.8.1.1 Clear requirements for a detailed project implementation plan.

3.8.1.2 Formal implementation phases: planning, design, development, data migration, testing, deployment, training, go-live, and post-implementation embedment/remediation.

3.8.1.3 Explicit service provider responsibilities across the full project lifecycle; a comprehensive testing strategy covering functional testing, unit testing, system integration testing, regression testing, security testing, performance testing, data migration testing and UAT.

3.8.1.4 An implementation/deployment strategy including readiness, cutover, rollback and go-live approval.

3.8.1.5 A structured project phase table with activities and deliverables.

3.8.1.6 Project governance and reporting requirements.

3.8.2 Formal phase-gate approval and deliverable acceptance requirements. Upon appointment, the service provider shall be required to adhere to the Authority's policies, including the Application Life Cycle Policy and the IT Infrastructure and Systems Change Management Policy.

3.8.3 Change Management: All changes to the operating system, database, application, configuration, infrastructure, integrations, and security settings must be managed in accordance with the internal policies. Changes must be formally requested, assessed for risk and impact, tested in an appropriate non-production environment, approved by the relevant change authority, and scheduled before implementation in the production environment. Emergency changes must follow an approved emergency change process and be retrospectively reviewed and documented. The system must maintain a complete, tamper-evident audit trail of all change activities, including the requester, approver, implementer, nature of the change, affected component, date and time, reason for the change, test evidence, approval reference, implementation outcome, rollback actions where applicable, and before-and-after values for configuration or data changes. Change records and audit logs must be securely retained and made available for governance, compliance, audit, and security review.

Deployment/Customisation and implementation of software

3.8.4 Environment Security (Dev / Test / Prod): The system must enforce strict segregation between development, testing, and production environments, with controlled access and no use of live data in non-production environments unless properly masked.

3.8.5 The Service Provider shall customise, configure, test and implement the ASMS to align with the Authority's approved business processes, regulatory requirements, workflows, user roles, templates, reports, integrations and operational controls across all applicable modules.

3.8.6 Customisation shall prioritise the configuration of standard system functionality over bespoke development to minimise complexity, cost, risk and future maintenance effort.

3.8.7 All custom development shall be strictly controlled and must be formally documented, including functional and technical specifications, design approvals, configuration records and version control. Such customisations shall be subject to the Authority's approval prior to development and must undergo comprehensive testing, including unit testing, system integration testing and user acceptance testing, in accordance with the approved testing strategy.

3.8.8 All customised and configured functionality shall be supported under the agreed warranty, maintenance and support arrangements, including ongoing updates, defect resolution and compatibility with future system upgrades.

3.8.9 The Service Provider shall ensure that all customisation activities are executed in accordance with the approved project implementation plan, with clearly defined milestones, deliverables, roles and responsibilities, dependencies, testing criteria and acceptance criteria.

3.8.10 No customisation shall be considered complete until it has been formally reviewed, tested and accepted by the Authority. Payment milestones shall be linked to the Authority's formal acceptance of completed deliverables.

Data migration of existing data

3.8.11 The Service Provider must design and execute a comprehensive data migration strategy covering all approved legacy data sources (systems, tools, spreadsheets, repositories).

3.8.12 The migration must follow a structured lifecycle, including profiling, extraction, cleansing, deduplication, mapping, transformation, loading, validation, reconciliation, and formal user acceptance.

3.8.13 All business-critical datasets must be migrated, ensuring completeness, accuracy, integrity, traceability, and auditability.

3.8.14 The Service Provider must perform trial migrations and validations prior to final cutover, supported by detailed reports and exception logs.

3.8.15 Data security and compliance must be enforced throughout, including protection of personal and confidential information in line with legislation and organisational policies.

3.8.16 Migration must be formally validated and accepted by the Authority before go-live, with clear reconciliation between source and target systems.

3.8.17 Any defects identified post go-live must be remediated under warranty and support arrangements at no additional cost.

3.8.18 Data shall be migrated from the Authority's existing spectrum management system and other out-of-the-system records (e.g., Excel sheets) to the new system. The Service Provider shall make provision for the migration of all identified and approved data categories, as outlined below, to ensure continuity, integrity and operational readiness of the new system:

3.8.18.1.1 Legal entities: Legal entities registered within the old system are approximately 32000. The data comprises identity documents, company registration certificates, entity names, company details, and contact details.

3.8.18.1.2 Radio Frequency Spectrum Licences: All the radio frequency spectrum licences, frequency assignment plans and supporting technical information need to be transferred to the new system. At the time of drafting this document, the number of licences was as follows:

- Active – 292 licences
- Amendments in Progress– 12 licences
- Amendment Predecessor – 4 244 licences
- Up for Renewal – 5 670 licences
- Renewal in Process – 2 426 licences
- Renewal Predecessor – 35 976 licences
- Expired – 1 133 licences

3.8.18.1.3 Type Approval Certificates and equipment: All data of type-approved equipment, as well as copies of type approval certificates issued, must be transferred to the new system. The number of equipment and type approval certificates issued on the current system is 29 307 and 27 459, respectively as well as 11 308 legacy certificates.

3.8.18.1.4 Service Licensing: All the service licences, and supporting information need to be transferred to the new system. At the time of drafting this document, the number of licences was as follows

- Active Class Broadcasting licences - 388
- Active Individual Broadcasting licences- 62
- Individual I-ECNS and I-ECS licences
    - Active: I-ECNS = 444; I-ECS =447
    - Up for Renewal: IECNS = 444; IECS =447 in 2028/29

3.8.18.1.5 Callsigns: The ITU allocated several callsign ranges to South Africa for assignment of callsigns to users in the country. All assigned and unassigned callsigns must be transferred to a callsign database on the new system. There are more than one million call signs that need to be populated.

3.8.18.1.6 Maritime Mobile Service Identification (MMSI) Numbering Database: The Authority have a spreadsheet of all the MMSI numbers that were allocated for assignment in South Africa. From this list, manual assignments are made to qualifying applicants on request. These allocated and assigned numbers must be populated into an MMSI database on the system. MMSI has various Sections within Maritime (e.g., Ship station / maritime mobile, Coast Station (Port station,

pilot station, AIS base station, AIS repeater station, Assignment of identification to aircraft - Fixed-wing aircraft, Helicopters), examples used from the ITU.

Training, skill transfer and user awareness requirements

3.8.19 The Service Provider is responsible for delivering a comprehensive, role-based training programme covering all user groups involved in operating, administering, supporting and governing the system.

3.8.20 Training must be planned, structured and measurable, supported by an approved training plan, curriculum, schedule, materials, practical exercises, assessments and completion records.

3.8.21 The training must be practical and scenario-based, using realistic Authority business processes and data to ensure users are fully competent before go-live.

3.8.22 Training must cover end users, administrators, technical specialists, managers and external users, and include system functionality, technical tools, reporting, security, access control, and operational support procedures.

3.8.23 Training should be provided in a hybrid fashion, covering both physical and online formats.

3.8.24 Knowledge sustainability must be ensured through train-the-trainer sessions, knowledge transfer, and post-go-live refresher or coaching support.

3.8.25 All training outputs must be reusable, editable and formally accepted by the Authority, with training completion linked to payment milestones.

3.8.26 The Service Provider must conduct a formal and structured system hand-over to the Authority before final acceptance. This includes delivering complete, up-to-date documentation, system architecture, system configurations, custom source code, migration and testing outputs, operational and support procedures, and security settings.

3.8.27 The hand-over must ensure effective knowledge transfer so the Authority can operate and support the system independently. Formal acceptance of the hand-over marks the transition to warranty and support, without limiting the Service Provider's responsibility for defects or post-implementation remediation.

3.8.28 The Service Provider must ensure effective skills transfer to the Authority's personnel through structured knowledge transfer activities, enabling the Authority to independently operate, administer, support and maintain the system following implementation and hand-over.

3.8.29 A webinar(s) must be provided to the public (applicants and licensees) regarding how to use the system and apply for various types of applications in the client portal. User manual videos and recorded webinar(s) should be made available to the public, to further train applicants and licensees on the use of the client portal.

3.8.30 The service provider will be expected to transfer knowledge (skills/knowledge transfer) through formalised training to at least ninety (90) employees of the Authority**.**

System Warranties and Support

3.8.31 The service provider must provide a comprehensive warranty for the ASMS and all project deliverables for at least twelve (12) months from the Authority's formal acceptance of the implemented system.

3.8.32 The ASMS and all related deliverables must meet the approved functional, technical, security, performance, integration, data migration and operational requirements;

3.8.33 The warranty must cover standard software, configurations, customisations, integrations, migrated data, reports, workflows, security controls, user interfaces, documentation and training materials;

3.8.34 The service provider must fix all defects, faults, failures, vulnerabilities, data migration issues, integration issues, reporting errors, workflow defects, performance problems and documentation inaccuracies at no additional cost;

3.8.35 The ASMS must operate reliably, securely and efficiently, and meet agreed performance, availability, response time, scalability, backup, recovery and integration requirements;

3.8.36 The system must be free from known malware, backdoors, unauthorised access mechanisms and critical or high-risk vulnerabilities;

3.8.37 Migrated data must be complete, accurate, validated, reconciled, traceable, secure and fit for operational use;

3.8.38 Formal acceptance by the Authority does not remove the service provider's responsibility for latent defects or issues discovered after go-live; and

3.8.39 The service provider must maintain a warranty issue register and ensure that all fixes are tested, documented and formally accepted before closure.

Support

3.8.40 The Service Provider must deliver comprehensive, end-to-end system support to ensure the ASMS remains available, secure, performant and compliant. This includes operational, functional and technical support; incident and problem management with defined SLAs; security patching and vulnerability remediation; routine maintenance and upgrades; data integrity and reporting support; controlled change and enhancement support; ongoing knowledge transfer; service performance reporting; and business continuity support, including backup and disaster recovery assistance.

3.8.41 The bid should cover the support for a period of three years, with an option to renew support.

3.8.42 The operational support should cover:

3.8.42.1 Day-to-day system support to ensure availability, stability and performance.

3.8.42.2 Support for all modules, integrations, databases, workflows and reports.

3.8.42.3 Monitoring of system health, capacity and performance trends.

3.8.43 Incident and Problem Management:

3.8.43.1 A formal incident management process with defined severity levels, response times and resolution targets.

3.8.43.2 Root-cause analysis for recurring or high-impact incidents.

3.8.43.3 Proactive identification and prevention of systemic issues.

3.8.44 Functional and Technical Support:

3.8.44.1 Assistance to users with system functionality, workflows and business processes.

3.8.44.2 Technical troubleshooting across applications, integrations, databases and infrastructure.

3.8.44.3 Support for RF engineering tools, GIS functions, licensing workflows, Financial system and technical evaluations.

3.8.45 Security and Compliance Support:

3.8.45.1 Ongoing security patching and vulnerability remediation.

3.8.45.2 Support for access control, role management, MFA and audit logs.

3.8.45.3 Assistance during security reviews, audits or compliance inspections.

3.8.46 Maintenance and Upgrades:

3.8.46.1 Regular preventive maintenance, system tuning and optimisation.

3.8.46.2 Delivery and support of patches, hotfixes, version upgrades and compatibility updates.

3.8.46.3 Regression testing and controlled deployment through change management processes.

3.8.47 Data and Reporting Support:

3.8.47.1 Support for data integrity, correction of data issues and reconciliation queries.

3.8.47.2 Assistance with reporting, dashboards and ad-hoc data analysis requests.

3.8.47.3 Support for data governance and audit requirements.

3.8.48 Change and Enhancement Support:

3.8.48.1 Assessment and implementation support for approved system changes and enhancements.

3.8.48.2 Impact analysis, testing and documentation of changes.

3.8.48.3 Support for new regulatory or business requirements.

3.8.49 Knowledge Transfer and User Enablement:

3.8.49.1 Ongoing knowledge transfer to internal support teams.

3.8.49.2 Updates to documentation, support guides and operating procedures.

3.8.49.3 Post-go-live coaching and refresher support where required.

3.8.50 Service Management and Reporting:

3.8.50.1 Regular service performance reporting against SLAs.

3.8.50.2 Clear escalation paths and governance forums.

3.8.50.3 Continuous improvement recommendations based on support trends.

4 PROPOSAL

4.1 The proposal should give a breakdown of the project implementation plan. In this regard, please note the following:

4.1.1 In the scheduling of activities, a holiday break should be assumed from 15 December until 15 January.

4.1.2 The deployment and customisation of the system will end when the system is implemented in the live environment after ICASA accepts it, and this should not exceed 12 months from onboarding of the service provider.

4.1.3 The support of the system will follow after implementation in the live environment and will be for a period of 36 months. There should be an option to extend support on similar terms, following the 36 months.

4.2 Some of the expected activities will be as follows:

Main activities		**Duration**
On boarding		Start
Planning		12 Months Deploy no later than 12 months from start of contract
	Review project scope	
	Translate scope into a workable plan	
Requirements analysis		
	Review data to be migrated into the system	
	Review workflow processes to be implemented	
	Specify customised features required	
	Sign off business requirements document	
	IT Change Management Process	
Design		
	System architecture document	
	Data migration plan	
	Integration document	
	Sign off functional specification document	
Implementation		
	Prepare data servers	
	Deploy software	
	Customisation of features	
	Implement workflow pathways	
	Data cleaning and migration	
	Configuration document	
Testing	Testing of all modules including data migration, customisation, integration, workflows	
	Development of procedures	
	Training of users	

	UAT sign-off	
	Go live plan	
Deployment	Prepare production (PROD) environment	
	Copy system config to PROD	
	Final data migration from legacy systems	
	Sign-off on data migration	
	Go live Sign-off	
	Implementation in the live environment	
	Post implementation support for 1 month	
Maintenance phase	SLA support to be in place Ongoing monitoring	36 months from date of system implementation in the live environment

4.3 The proposal needs to cover all costs, and the costs need to be broken down according to:

4.3.1 Hardware, hosting services, software licences, customisation, support over the full 3 years after implementation, or any other relevant category.

4.3.2 Cost per module (Spectrum Planning, Spectrum Licensing, Service Licensing, Type Approval, Integration with Financial system, etc.)

4.3.3 When payment would be due. Typically, payments should be due only after User Acceptance, so any exceptions should be clearly justified.

5 BRIEFING SESSION

5.1 A virtual non-compulsory briefing session will be held.

6 BID EVALUATION

6.1 Bidders will be evaluated on:

6.1.1 Phase 1: Administrative Compliance

6.1.2 Phase 2: Mandatory Requirements

6.1.3 Phase 3: Functionality criteria

6.1.4 Phase 4: Live demonstration

6.1.5 Phase 5: Price and specific goals

Phase 1 Administrative Compliance:

6.2 Bidders must ensure that they complete and sign documents as indicated below, and the documents must be submitted as part of the bid document.

- SBD 1 – Invitation to Bid
- SBD 2 - Tax Clearance Certificate Requirements
- SBD 3.1 - Pricing schedule
- SBD 4 - Declaration of Interest
- SBD 5- The National Industrial Participation Programme
- SDB 6.1 - Preference Points claim form
- SBD 7.1 – Contract form (rendering of services)
- Declaration in terms of Fronting

PHASE 2: MANDATORY REQUIREMENTS EVALUATION

The following are the mandatory requirements for this tender. Failure to comply with any requirement will result in disqualification. When completing the table below, bidders must provide details or indicate, in the last column, where in the bid submission the information can be found.

No	Minimum Criteria	Yes	No	Provide details or indicate where on bid submission information can be found
1	Spectrum Licensing module supports the required application workflows (new, renewal, amendment, transfer, cancellation/surrender)			
2	Service Licensing module supports the required application workflows (new, renewal, amendment, transfer, cancellation/surrender)			
3	RF Engineering analysis tools support coverage analysis, interference analysis, propagation models, and digital topographical maps			
4	The type approval module supports the required application workflows (new, amendment, transfer, cancellation)			
5	Integration capabilities with Spectrum Monitoring systems			
6	Integration capabilities with ICASA's Finance system for invoicing, credit notes, payments, & generation of reports.			
7	Have an online client portal that the applicants/licensees can access			
8	The system must comply with data protection legislation (POPIA) and related security standards			

9	Active Directory authentication must be supported			
10	The system should have Audit trail capabilities			
11	The system is capable of generating reports and supporting analytics			
12	The system must comply with the Payment Standards (PCI DSS)			
13	The service provider must be able to provide ICASA with SOC 2 reports or an equivalent on an annual basis for the duration of the contract.			

PHASE 3: FUNCTIONALITY EVALUATION

Bidders' competence

This section evaluates the service provider's reliability, experience, reputation, and sustainability. Only bidders who meet the 70% functionality cut-off will be considered for further evaluation (phase 4, a live demonstration).

No	Functional Evaluation Criteria	WEIGHT
1	**Reference letters** Bidder must submit contactable reference letters not older than 7 years on a client letterhead for Automated Spectrum Management System (ASMS) services or similar product/services that were previously provided to a regulator responsible for radio frequency spectrum licensing (References to be verified by ICASA). The following requirements should be stipulated in the reference letters submitted: - Client name - Contact name and telephone number - System implementation date - Detailed description of services delivered - Client indicating their satisfaction with the delivered service	**40**

	Scoring: less than or equal to 3 references provided to fulfil all the requirements as stipulated = 1 4 or 5 references provided to fulfil all the requirements as stipulated = 2 6 or 7 references to fulfil all the requirements as stipulated = 3 8 or 9 references to fulfil all the requirements as stipulated = 4 10 or more references to fulfil all the requirements as stipulated = 5	
2	**Bidder's experience** Bidder's experience in implementing ASMS services (The bidder must provide a company profile, which will be used to assess the level of experience): **Scoring:** - Less than three (3) years of experience in providing ASMS = 1 - 3 to 4 years of experience in providing ASMS = 2 - 5 to 6 years of experience in providing ASMS = 3 - 7 to 9 years of experience in providing ASMS = 4 - 10 years or more of experience in providing ASMS = 5	**10**

3	**Implementation Plan** Provide a comprehensive plan that covers the following key areas: - Project phases - Project schedule with milestones - Risk management - Reporting mechanisms - Training plan **Scoring:** - Detailed and well-structured implementation plan covering all 5 key areas = 5 - Implementation plan adequately addresses 4 of the key areas = 4 - Implementation plan sufficiently addresses 3 of the key areas = 3 - Implementation plan sufficiently addresses 2 key areas = 2 - Implementation Plan does not sufficiently address any of the key areas or only 1 of the key areas, or no submission of implementation plan provided = 1	**5**

4	**Bidder's ability to deliver on functionality as per Annexure B below** This section evaluates the service provider's ability to meet ICASA's ASMS requirements. All 122 requirements listed in Annexure B should eventually be met; however, some of the requirements can be developed/customised in the first 12 months after the service provider is onboarded. ICASA requires that at least 70% (85 out of 122) of the requirements in Annexure B be complied with at the time of bid evaluation, and will award a higher score to bidders that comply with 85% (104 out of 122) or more of the requirements. The bidder should provide evidence of compliance with the requirements in its submission. The requirements in Annexure B are categorised for ease of reference, but the percentage should be calculated on all the total requirements, and <u>not</u> on a per-category basis. **Scoring**: - Comply with 85% or more of the requirements at the time of bid evaluation, and commit to comply with 100% of the requirements within the first 12 months of the project (before "go-live") = 5 - Comply with 70% to 84% of the requirements at the time of bid evaluation, and commit to comply with 100% of the requirements within the first 12 months of the project (before "go-live") = 3 - Comply with less than 70% of the requirements at the time of bid evaluation, and/or do <u>not</u> commit to comply with 100% of the requirements within the first 12 months of the project (before "go-live") = 1	**45**

Total score	**100**

Only the bidders who meet the cut-off of **70%** out of 100% in the Functional Evaluation will be considered for further evaluation (phase 4, which is a live demonstration)

350 Witch-Hazel Avenue,
Eco Point Office Park
Eco Park, Centurion
Private Bag X10,
Highveld Park 0169
Tel number: (012) 568 3000/1

ANNEXURE B: FUNCTIONALITY REQUIREMENTS *(to be completed by the service provider)*

FUNCTIONALITY REQUIREMENTS – AUTOMATED SPECTRUM MANAGEMENT SYSTEM (ASMS) (SCOPE OF WORK)

The requirements are categorised per module for easy reference.

B1. Client Portal Requirements

	When will the system support the following requirement?	Already supported	Will support within 1st 12 months of the project	Provide details or indicate where on the bid submission information can be found
1	Secure, user-friendly online environment where applicants and licensees/certificate holders can submit and track applications and manage licences/certificates			
2	Ability to allow stakeholders to create and modify user accounts as needed			
3	Real-time data validation checks and integrity checks when capturing applications			
4	Support multi-factor authentication to enhance security. This should include options for various authentication methods, such as SMS verification codes, email confirmations, or authenticator apps,			

	and require users to provide additional proof of identity when accessing their accounts.			
5	Ability to support the various applications as well as different features to manage licences/certificates for radio frequency spectrum licensing, type approvals and service licensing.			
6	Enforce mandatory fields/documents to be populated/uploaded, and application with incomplete information must not be allowed to be submitted.			
7	Capable of providing an up-to-date, real-time display of the status of each application such as submitted, awaiting information, under review, rejected/declined, approved, etc.			
8	Capable of presenting the total processing time that has elapsed since the initial submission of the application, giving applicants a comprehensive view of the duration of their application journey			
9	Ability to automatically identify licenses that are due for renewal based on their expiry dates and status, and it must provide an option to trigger the license renewal process before the license expires			
10	Allow users to edit and upload documents at any stage when the application is available to them.			
11	Provide an option for applicants to submit confidentiality requests through a configurable online form, together with the required supporting documentation.			

12	Capable of allowing users to create profiles for third parties, with the necessary proxy, and submit that for approval.			
13	Able to allow the licensee to log requests for interference investigations, should their assigned spectrum be affected by such during implementation.			

B2. Spectrum Planning Requirements

	When will the system support the following requirement?	**Already supported**	**Will support within 1st 12 months of project**	**Provide details or indicate where on the bid submission information can be found**
1	Capable of importing and maintaining the ITU-R Table of allocation and the updated National Radio Frequency Plan with the applicable footnotes			
2	Display the radio frequency assignment plans, band rules and recommendations aligned with each specific spectrum band			
3	Allow authorised users to capture and manage the spectrum migration plan and flag bands with services that need to be migrated out.			

B3. RFS Licensing Administration Requirements

	When will the system support the following requirement?	Already supported	Will support within 1st 12 months of the project	Provide details or indicate where on bid submission information can be found
1	Configurable workflow capable of catering for new, renewal, amendment, transfer/transfer of control, cancellation/surrender applications.			
2	Capable of receiving time-bound applications, which use an extended application procedure (i.e., Invitation to Apply or Invitation to Pre-Register (ITP-R) process)			
3	Allow for updating of registers for the E-band light licences and satellite space segment			
4	Temporary licensing for RFS licensing for state visits, special events and trial			
5	Ability to track each application throughout its lifecycle			
6	Fee calculation automation			
7	Ability to issue licences or rejection letters after application approval.			
8	Ability to accept applications for multiple fixed links in bulk			
9	The system should be able to direct the applications to the appropriate departmental unit according to the selected sub-module category			

10	Integration with RF Engineering analysis module			
11	Integration with the finance module			
12	Unique licence number generation			
13	Ability to assign Call sign numbers			
14	Ability to assign and search for Maritime Mobile Service Identity (MMSI) numbers			
15	Ability to display polygons, including for provincial, district and local municipal demarcations.			
16	The system should have functionality to make public records available			
17	The system should have an efficient way of automatically allocating applications to users			
18	Flag applications that are at risk of exceeding SLA timelines (internally)			

B4. RFS Engineering Analysis Requirements

	When will the system support the following requirement?	Already supported	Will support within 1st 12 months of the project	Provide details or indicate where on the bid submission Information can be found
1	A ready-made technical analysis tool that has been widely used by regulators worldwide			
2	Editable allotments which include frequency band, bandwidth, channel spacing, maximum transmitter power, and service types, in line with applicable ITU-R channel plans.			
3	Capable of calculating interference across all service types.			
4	Ability to scan frequency availability within a specific band.			
5	Ability to flag assignments outside national borders and those within coordination zones.			
6	Capable of doing coverage predictions using various ITU-R propagation models such as received signal strength, signal-to-noise ratio (SNR), and link budget analyses (including topographical link profile and Fresnel zone analysis)			
7	Ability to flag applications that fall in areas where prohibition to frequency use applies, such as radio astronomy protection areas.			

8	Capable of reading BR-IFIC data and facilitating the updating of MIFR with approved assignments.			
9	Ability to interface with client portal, technical database, spectrum planning module, and Monitoring and Compliance Module.			
10	Minimum 20m DEM maps covering the coordination zone of the neighbouring countries (200km from the border)			
11	The granularity of the digital terrain maps should at least be at 20m DEM, with an option of 100m DEM			

B5. Type Approval (Equipment standardisation) Requirements

	When will the system support the following requirement?	**Already supported**	**Will support within 1st 12 months of the project**	**Provide details or indicate where on the bid submission information can be found**
1	Configurable workflow capable of catering for new/Variant/Provisional/Simplified/Amendment/Certificate transfer applications			
2	The system should be able to direct all type approval applications to the type approval module			
3	Ability to automatically allocate applications to type-approval specialists equitably			
4	Ability to track each application throughout its lifecycle			

5	Automated update on the list of approved equipment			
6	Allow for the functionality to make a list of approved type-approved equipment public			
7	Ability to issue certificates or rejection letters after application approval/rejection.			
8	Integration with Spectrum licensing			
9	Flag applications that are at risk of exceeding SLA timelines (internally)			

B6. Service Licensing requirements

	When will the system support the following requirement?	**Already supported**	**Will support within 1st 12 months of the project**	**Provide details or indicate where on the bid submission information can be found**
1	Configurable workflow capable of catering for new, special event, exemption, temporary licences, renewal, amendment, transfer, cancellation/surrender applications.			
2	Capable of receiving time-bound applications (i.e., Invitation to Apply or Invitation to Pre-Register (ITP-R) process)			

3	Ability to track each application throughout its lifecycle			
5	Ability to issue licences or rejection letters after application approval/rejection.			
6	The system should be able to direct the applications to the appropriate departmental unit according to the application type and selected category			
7	Ability to cater for the spectrum licensing dependency by ensuring that the service licence, where applicable, is issued only when the spectrum licence is approved.			
8	Ability to produce a report regarding the issued licences (Class and Individual) and their location (for example, provincial, district and local municipal demarcations)			
9	The system should have functionality to make public records available			
10	Licence expiry reminders			
11	Status reporting on applications in progress			
12	Flag applications that are at risk of exceeding SLA timelines (internally)			

B7. Spectrum Monitoring Integration

	When will the system support the following requirement?	Already supported	Will support within 1st 12 months of the project	Provide details or indicate where on the bid submission information can be found
1	The system must be able to integrate with fixed spectrum monitoring stations and mobile monitoring units by supporting the ingestion of monitoring data from these.			
2	The module must be able to correlate monitoring data with active spectrum licences and technical parameters to detect and flag non-compliant transmissions.			

B8. Financial Requirements

	When will the system support the following requirement?	Already supported	Will support within 1st 12 months of the project	Provide details or indicate where on the bid submission information can be found
1	ASMS must establish a secure, real-time, and bidirectional integration with ICASA's Financial System			
2	No applications should reach the internal licensing module if the payments are not made			

3	ASMS should automate the calculation of fees and integrate the information into the financial system for the creation of proforma invoices and credit notes			
4	The application must have a mandatory field for proof of payment (PoP) attachment			
5	The module must allow for bulk payment approvals and bulk assignment of the approval tasks to the team members			
6	All applications with confirmed payments must be automatically assigned to the relevant licensing pool (Spectrum Licensing, Type Approval, or Services Licensing).			
7	The system should allow Finance to reject an invalid PoP by selecting predefined reasons such as invalid payment			
8	The system must provide automated reconciliation functionality between the licensing system and the financial system.			
9	The system must maintain a historical archive of all invoices, receipts, statements, debit notes, credit notes, payment records, and related financial correspondence			
10	The system must automatically calculate pro-rata fees on a monthly basis in accordance with ICASA business rules.			

B9. Security & Architecture Requirements

	When will the system support the following requirement?	Already supported	Will support within 1st 12 months of the project	Provide details or indicate where on the bid submission information can be found
1	POPIA compliance			
2	Encryption at rest			
3	Encryption in transit			
4	Active Directory integration/ Microsoft Entra ID			
5	Role-based access control			
6	Audit log of all actions			
7	Session management – Integration & Interoperability			
8	Password policy enforcement			
9	Disaster recovery capability (either by the OEM or ICASA's backup solution having access to the ASMS environment)			
10	If the system is hosted in OEM's data centre, ICASA must have access to back up the system on a daily basis			
11	High availability (99.95% per year)			
12	API gateway			

13	Firewall (either by the OEM or ICASA's on-premise or Azure existing firewalls)			
14	Threat detection capability (either by the OEM or ICASA's SIEM solution)			
15	Data retention/ archiving capabilities			
16	Multifactor authentication			
17	ISO 27001 or SOC 2 compliance			

B10. Integration & Interoperability

	When will the system support the following requirement?	**Already supported**	**Will support within 1st 12 months of the project**	**Provide details or indicate where on the bid submission information can be found**
1	Integration with internal modules, external enterprise systems			
2	The ASMS architecture is agnostic of downstream external systems and does not contain hardcoded dependencies			
3	Resilience and asynchronous			
4	Integration interface with Financial Systems			

5	Integration interface with External Spectrum Monitoring Systems			
6	Geospatial Services - Support for standard geospatial protocols and formats			
7	Integration interface - Internal ASMS Modules			
8	Integration Interface - Future Integration Interfaces			
9	All integrations must be auditable, traceable, and monitored			

B11. System administration

	When will the system support the following requirement?	**Already supported**	**Will support within 1st 12 months of project**	**Provide details or indicate where on the bid submission information can be found**
1	User account management capabilities to support the full user lifecycle, including account creation, modification, delegation and deactivation			
2	Role-Based Access Control (RBAC)			
3	Auditable reporting on all back-end administrative activities and configuration changes			

4	Reporting on user role assignments reflecting start and end dates			
5	Report on user account management activities.			

B12. Data Migration & Data Management

	When will the system support the following requirement?	Already supported	Will support within 1st 12 months of the project	Provide details or indicate where on the bid submission information can be found
1	Import of historical data from the legacy systems			
2	The migration must follow a structured lifecycle, including profiling, extraction, cleansing, deduplication, mapping, transformation, loading, validation, reconciliation, and formal user acceptance			
3	Perform trial migrations and validations prior to final cutover, supported by detailed reports and exception logs			
4	Migration must be formally validated and accepted by the Authority before go-live, with clear reconciliation between source and target systems			

5	Data shall be migrated from the Authority's existing spectrum management system and other out-of-the-system records (e.g., Excel sheets) to the new system			

B13. Workflow/Decision making

	When will the system support the following requirement?	Already supported	Will support within 1st 12 months of project	Provide details or indicate where on the bid submission information can be found
1	There should be flexibility in the design and setting up of workflow pathways			
2	The system is able to allocate applications automatically in an equitable fashion to the team members			
3	The system will allow for applications to be allocated to generic pools as well as accept them into its own tasks/pools			
4	Managers should have the ability to assign and reassign applications to team members.			
5	Assess during amendment applications if a fee impact requires the need to issue a Debit/Credit note			

5	Licences/certificates should have security features such as a QR Code that can be scanned to verify validity			
6	Automatic rejection letter generation			
7	The system should allow for SMS or email notifications at certain handover points.			
8	The system should allow capturing comments and uploading documents during task processing.			

PHASE 4: PRESENTATIONS AND DEMONSTRATIONS EVALUATION

This section assigns scores based on the information gathered from the live demonstration

LIVE DEMONSTRATION SCORING

This section evaluates the user interface and experience through live demonstrations. The service provider will demonstrate the following scenarios, and evaluators will score based on ease of use, intuitiveness, and functionality. The Demo will be 2 hours long, and thereafter 1 hour of questions will follow.

Demonstration Scenario	**Use cases**	**Evaluation criteria**	**Points**
Background: Demonstrate the processing of the example applications listed below from the			

perspective of various users of the system.			
Spectrum Licensing application Users: **Applicant** (External users interfacing via the client portal) **Finance Officer**: verify the proof of payment of the application/licence fee **Licensing Officer**: Review and analyse the application for completeness and regulatory compliance **Radio Frequency Engineer**: Evaluates whether interference will be experienced	Demonstrate how the following spectrum licensing applications will be processed: 1) new 2) amendment 3) renewal 4) cancellation/surrender Demonstrate this from the perspective of the identified users, and ensure that you refer to the following: 1) Register as external user 2) Application by Applicant via the Client Portal 3) Ensure proof of payment is verified by Finance Officer 4) Review and analyse application by Licensing Officer	1. Demonstrated the ability to process the following application types accurately and efficiently: o New (1 point) o Amendment (1 point) o Renewal (1 point) o Cancellation/surrender (1 point) 2. During the demonstration of the various application types, the following aspects were confirmed: o Register as external user (1 point) o Application by Applicant via the Client Portal (1 point) o Ensure proof of payment is verified by Finance Officer (1 point)	14

Approvers: verify and ratify the analysis and ultimately approve the application	5) Evaluation in the RF Engineering tool to verify that the assignment will not cause interference and conduct a coverage analysis 6) Multi-stage approval of application 7) Issue a downloadable spectrum licence/rejection letter 8) Demonstrate the security features of the generated licence document	○ Review and analyse application by Licensing Officer (1 point) ○ Evaluation in the RF Engineering tool to verify that the assignment will not cause interference and conduct a coverage analysis (1 point) ○ Multi-stage approval of application (1 point) ○ Issue a downloadable spectrum licence/rejection letter (1 point) ○ Demonstrate the security features of the generated licence document (1 point) 3. The look and feel of the GUI is user-friendly and efficient. (2 points)	
1) Type approval application	Demonstrate how the following type approval applications will be processed:	1. Demonstrated the ability to process the following application types accurately and efficiently:	11

Users: **Applicant** (External users interfacing via the client portal) **Finance Officer**: verify the proof of payment of the application/licence fee **Type approval Specialist**: Review and analyse the application for completeness and regulatory compliance **Approvers**: verify and ratify the analysis and ultimately approve the application	1) new 2) amendment 3) cancellation/surrender Demonstrate this from the perspective of the identified users, and ensure that you refer to the following: 1) Register as external user 2) Application by Applicant via the Client Portal 3) Ensure proof of payment is verified by Finance Officer 4) Review and analyse application by Licensing Officer 5) Multi-stage approval of application 6) Issue a type approval certificate/rejection letter	○ New (1 point) ○ Amendment (1 point) ○ Cancellation/surrender (1 point) 2. During the demonstration of the various application types, the following aspects were confirmed: ○ Register as external user (1 point) ○ Application by Applicant via the Client Portal (1 point) ○ Ensure proof of payment is verified by Finance Officer (1 point) ○ Review and analyse application by Licensing Officer (1 point) ○ Multi-stage approval of application (1 point) ○ Issue a type approval certificate/rejection letter (1 point) 3. The look and feel of the GUI is user-friendly and efficient. (2 points)	

3) Service Licensing application <u>Users</u>: **Applicant** (External users interfacing via the client portal) **Finance Officer**: verify the proof of payment of the application/licence fee **Licensing Officer**: Review and analyse the application for completeness and regulatory compliance **Approvers**: verify and ratify the analysis and ultimately approve the application	Demonstrate how the following type approval applications will be processed: 1) new 2) amendment 3) cancellation/surrender Demonstrate this from the perspective of the identified users, and ensure that you refer to the following: 1) Register as external user 2) Application by Applicant via the Client Portal 3) Ensure proof of payment is verified by Finance Officer 4) Review and analyse application by Licensing Officer 5) Multi-stage approval of application 6) Issue a service licence/rejection letter	1. Demonstrated the ability to process the following application types accurately and efficiently: o New (1 point) o Amendment (1 point) o Cancellation/surrender (1 point) 2. During the demonstration of the various application types, the following aspects were confirmed: o Register as external user (1 point) o Application by Applicant via the Client Portal (1 point) o Ensure proof of payment is verified by Finance Officer (1 point) o Review and analyse application by Licensing Officer (1 point) o Multi-stage approval of application (1 point)	11

		○ Issue a type approval certificate/rejection letter (1 point) 3. The look and feel of the GUI is user-friendly and efficient. (2 points)	
4) Reporting	Demonstrate the search and reporting features of the system, and ensure that you refer to the following: 1) Search the database of certificates/licences 2) Search the database of applications 3) Demonstrate the performance management report for internal users, indicating the amount of time spent on tasks by each individual. 4) Reports on the number of applications processed in a specific period that can be filtered per application type.	Demonstrated the ability to produce the following search and reporting features: 1) Search the database of certificates/licences (1 point) 2) Search the database of applications (1 point) 3) Demonstrate the performance management report for internal users, indicating the amount of time spent on tasks by each individual. (1 point) 4) Reports on the number of applications processed in a specific period that can be filtered per application type. (1 point)	4

Total			40

Only the bidders who meet the cut-off of **95%** out of 100% in the Presentation and Demonstration Evaluation will be considered for further evaluation (phase 5, price and special goals).

Phase 5: Price and Specific Goals Evaluation

6.3 Only bidders that passed the functionality evaluation will be further evaluated for price and specific goals.

6.4 Bidders who comply with the requirements of this bid will be evaluated according to the preference point scoring system as determined in the Preferential Procurement Regulations, 2022, pertaining to the Preferential Procurement Policy Framework Act, Act No 5 of 2000

No	Category	Weight
A.	Price	80
B.	Specific goals	20
	TOTAL	***100***

6.5 The maximum points for this bid are allocated as follows:

7 APPENDIXES

Appendix A_Standard Operating Procedure (SOP) – Radiocommunication

Appendix B1_SOP – Broadcasting Service Licensing and RFS (Individual)

Appendix B2_SOP – Broadcasting Service Licensing and RFS (Class)

Appendix C_SOP – Type Approval

Appendix D_SOP – Electronic Communication Service & Electronic Communication Network Service (Individual)

Appendix E_ SOP - Electronic Communication Service & Electronic Communication Network Service (Class)