REQUEST FOR PROPOSALS (RFP)

FOR THE SUPPLY

OF

A COMPLIANCE MONITORING AND REVENUE ASSURANCE TOOL

Contents

1.0 PREAMBLE

Lesotho Communications Authority (LCA) is the regulatory agency of the communications sector in Lesotho. It derives its mandate of regulating the telecommunications, broadcasting and postal sectors and other related matters from the Communications Act 2012 (the Act). This mandate entails amongst other things, to grant licences to operators, to promote fair competition, to promote sector development, to manage the radio frequency spectrum and numbering resources, to empower and protect consumers, to type-approve terminal equipment and to approve tariffs.

Since the adoption of the Act, the ICT sector experienced rapid transformation and became increasingly complex to regulate and harness in Lesotho. In light of this, LCA needs to have in place independent measurement and verification systems that would give it unfettered assurance of regulatory compliance in the telecommunications sector.

2.0 INTRODUCTION

There are two major players in Lesotho, Econet Telecom Lesotho and Vodacom Lesotho. Of the two, Vodacom dominates the mobile services market in Lesotho. As at March 2019, the number of mobile connections reached 1,584,739 and more than 96% of these are prepaid. Mobile Internet is also experiencing rapid growth with more than 400,000 active mobile social media users.

As mobile services continue to grow, so does Mobile Money that amounted to nearly 17% of the country's GDP in 2017. This is comparable to remittances that represented about 15.6% of Lesotho's GDP the same year, according to the World Bank.

These ecosystems, telecommunications and money transfer services, play an increasingly important role in Lesotho as key drivers of socio-economic development as well as enablers of financial and digital inclusion. LCA aims at promoting and protecting these vital ecosystems. Therefore, it now seeks to implement data systems that would effectively support this quest, while improving regulatory compliance monitoring and tax performance.

In its quest to verify the implementation by operators of the approved tariffs received, and in its pursuit of protecting consumers, LCA must monitor compliance with the implementation of approved tariffs. Therefore, LCA has identified a need to implement compliance monitoring and revenue assurance using a system based tool. The Authority plans to procure such a tool during the 2020/21 financial year.

In pursuit of its mandate and aforementioned goals, LCA invites proposals from suitably qualified companies for the design, supply and implementation of a Compliance Monitoring and Revenue Assurance Tool. The Compliance Monitoring and Revenue Assurance Tool should enable LCA to establish an accurate, real-time compliance monitoring and revenue assurance mechanism. The tool must integrate different

telecommunications & financial transactions metrics and provide oversight systems. The compliance monitoring and revenue assurance tool should be delivered and operated under a Build-Operate-Transfer (BOT) Model.

3.0 Required system overview

The solution should consist of different data systems integrated into a centralized platform. This platform, should modernize regulatory oversight and enforcement in order to ensure:

3.1 Compliance and security of the digital transaction ecosystem, including Mobile Money (MM);

3.2 Compliance and security of the telecommunications sector, including local service providers and Over-The-Top (OTT) services;

3.3 Improved revenue assurance in the above-mentioned sectors; and

3.4 Alignment with national policies and the Communications Act, 2012.

4.0 Objectives:

The objectives of the project are:

4.1 To independently measure and account for all telecommunication traffic traversing public networks operating in Lesotho, including but not limited to:

i) Incoming and outgoing international traffic;

ii) Off-net and on-net traffic;

iii) Transit traffic;

iv) SMS traffic;

v) Data traffic; and

vi) Roaming traffic;

vii) Mobile Money transactions; and

viii) SMS traffic.

4.2 To tackle illegal termination of international incoming traffic and prevent revenue losses due to this grey traffic;

4.3 To independently verify the revenue generated by the whole spectrum of telecom services sold on a prepaid and postpaid basis in Lesotho, including but not limited to:

i) Voice services;

ii) Data services: (SMS/MMS and data bundles);

4.4 To achieve comprehensive collection of taxes and fees applicable to different telecom services, including but not limited to accurate billing of regulatory fees and taxes on international calls termination;

4.5 To independently measure and account for all Mobile Money (MM) as processed by MM providers;

4.6 To ensure the traceability and compliance of all Mobile Money (MM) as processed by MM providers;

4.7 To tackle Money Laundering in MM;

4.8 To achieve effective regulatory control of the handset population in Lesotho and be able to use device information to block non-compliant, stolen and counterfeited devices and also form part of different types of investigations (anti-fraud, security, etc.); and

4.9 To independently monitor the Internet for cybersecurity and verification of compliance with relevant laws and regulation of Lesotho, including the capacity to detect potential threats and block online sites and/or services.

5.0 SCOPE OF PROJECT

The scope of the project is to establish a regulatory platform that is capable of meeting or exceeding the objectives above.

6.0 Technical Requirements

General Technical Requirements:-

6.1 Technical Deliverables

Bidders shall supply the Authority with documents (written in English) of system elements with detailed drawings, flow diagrams and specifications. The documentation shall also have detailed troubleshooting procedures of different subsystems.

6.2 Language Supported:

The system shall support English language only, for use and reports purposes. The system manuals shall also be in English.

6.3 Environmental:

6.3.1 Unless otherwise specified, all equipment must be robust and able to operate at a temperature ranging from –5 to 45 degree Celsius and 20 to 80 percent relative humidity.

6.3.2 Unless otherwise specified, all equipment must operate at noise levels no greater than 65 decibels.

6.3.3 All electronic equipment that emits electromagnetic energy must be certified as meeting US FCC class B or EN 55022 and EN 50082-1 or equivalent, emission standards.

6.4 **Capability to work with Multiple Technologies**

The system shall be capable of operating with the existing two (2) Mobile Network Operators (MNOs), and Internet Service Providers (ISPs) as well as Mobile Money Services Providers.

6.5 **Capability to work with Multiple Gateways**

The system shall have the capacity to interconnect with multiple telecommunications operators with multiple international gateways.

6.6 **Capability to work independently**

The system shall have the capability of collecting detailed Circuit Switched (CS) and Packet Switched (PS) Call Detail Records (CDRs) from the signalling information at the international gateways and national gateways of the Mobile Network Operators (MNOs), Public Switched Telephone Network (PSTN) and Internet Service Providers (for VoIP) without interfering with the flow of telecommunication traffic.

The system shall be capable of EXTRACTING signalling messages in PASSIVE MODE, using probes installed on the national and international interconnection gateways of all operators.

The system shall support all signalling protocols such as SS7, IP (SIP), and SIGTRAN etc. and generate Call Detail Records (CDRs) which are transmitted to the mediation centre for processing.

The following indicates a summary of the type of information to be collected:

#	CDR Type (Raw)
1	International incoming traffic information
2	International outgoing traffic information
3	National interconnect traffic
4	Roaming in MO/MT

6.7 **System Capacity:**

6.7.1 The system shall be designed to cater for the current traffic from all the MNOs', PSTN and Internet Service Providers inclusive future growing telecommunications traffic volumes.

6.7.2 The supplier shall indicate the System Capacity in terms of the number of International and national Routes the system is capable of monitoring.

6.8 **System Security and Up-Time:**

6.8.1 The proposed system shall be secure and protected with a Firewall system and Anti-virus.

6.8.2 All databases must be encrypted.

6.8.3 The system shall have an up time of 99.999%.

6.9 **Real Time Measurements**

6.9.1 The Tool shall operate in Real-time for the measurement of International Incoming, International Outgoing Traffic, national interconnect traffic, Mobile Money transactions and fraud detection.

6.9.2 The Tool shall be capable of reporting all the monitored parameters in Real-time.

6.10 **System Engineering Design**

6.10.1 The system shall be modular, flexible and easy to upgrade.

6.10.2 The System shall be able to start with a basic configuration allowing for extension at any time when the need arises. New system components must be easy to integrate. Supplier shall also ensure that highly specialized modules for specific new tasks are available when so required e.g. for the analysis of new mobile system technologies from the IMT family.

6.11 **System Features**

6.11.1 The System shall be able to work on all telecom technologies, vendors, mobile, fixed, International Gateway, Voice over Internet Protocol (VoIP), Next Generation Network (NGN), and WiMAX among others.

6.11.2 The System shall be easy to use, simple to configure, flexible and easy to customise.

6.11.3 The system shall have a functionality of checking data integrity to ensure correctness and completeness of data, prevent loss of data during transmission, adopt multi-check mechanism in the modules, and provide full process monitoring function.

6.11.4 The system must be reliable, and able to meet the existing and future IMT requirements.

6.11.5 The proposed system shall support robust Databases.

6.11.6 The system shall provide system/application fallback and recovery options and methodology.

6.11.7 The system shall have self-diagnosis mechanism and tools for identifying internal faults, loss of transmission links, malfunctioning or inconsistent operations.

6.11.8 The system shall be able to keep data for not less than 6 months.

6.11.9 The system shall have a Graphical User Interface (GUI) and capable to conduct at least the following actions:-

1	Display data
2	Create and display dashboards
3	Monitor parameters
4	Process scheduled tasks
5	Flexible and user friendly
6	Use Web Based GUI or windows-based GUI platforms

6.11.10 The system shall support multi-layered data reconciliation.

6.12 **Revenue Assurance**

6.12.1 The system shall be capable of performing Real-time measurement and billing of international incoming and outgoing telecommunication traffic flows between international carriers and operators in Lesotho from CDRs collected from the gateways.

Traffic should be measured and monitored as well as include circuit switched (CS) voice, Packet Switched (PS) voice, VoIP, Data and Internet traffic among others.

6.12.2 Billing for national interconnect will be used for national settlement purposes.

6.12.3 The system shall have a module capable of inputting tariff tables and creation of invoices for both international and national routes.

6.12.4 The system should be able to track cleared and un-cleared invoices.

6.13 **Capacity to generate statistics for national and international traffic**

6.13.1 The telecommunications traffic monitoring system shall have the capability to provide statistics as well as reports on local and international gateway traffic volumes per route.

6.13.2 The system shall be capable of producing and storing statistical data for both international and national interconnect traffic per route and destination countries. The statistical data shall include but not limited to:

a) Number of calls

b) Traffic Volumes (minutes)

6.14 **Capability to measure Quality of Service (QoS) of international interconnection telecommunication and national interconnect traffic in real time**

6.14.1 The system shall be capable of real-time monitoring and measuring of Quality of Service (QoS) at the Interconnection points. The Quality of service (QoS) shall be integrated into the monitoring system or a stand-alone solution.

6.14.2 The QoS solution shall provide customised reports and statistics and retain information for a period not less than 12 months.

6.14.3 Benchmarking shall be for all operators and integration done at network level.

6.14.4 The Supplier shall list the QoS key performance Indicators / Parameters the system can perform.

6.15 **Fraud Detection, Tracking and Analysis**

6.15.1 The traffic monitoring system shall have the capacity to detect 99.9% of fraudulent traffic into Lesotho. Any form of fraud detection may be acceptable as long as it guarantees 99.9% fraud detection rate. The supplier shall explicitly give a detailed description of how the fraud detection system works.

6.15.2 The preferred system shall have a module capable to originate test calls from probes worldwide and terminate them on a local unit. The module shall be capable of detecting, tracking and localising all forms of traffic bypass or traffic refiling into networks in Lesotho.

6.15.3 The system shall be capable of accurately identifying the routing path of the unofficial grey routes and identity both the local and international gateways involved in the routing of grey traffic.

6.15.4 The system shall be capable of sending alert SMS messages, e-mails to designated Fraud Management personnel from the regulatory authority and the operators within a specified time duration [e.g. 5 minutes]. The SMS messages or e-mails shall include the Calling Line Identification (CLI) of the Number, Origin, Destination and possible location.

6.15.5 The system shall be capable of storing the log-sheets for all fraud routes, list of countries generating fraud calls and a list of third parties assisting in fraud.

6.15.6 The fraud system shall have SIMBOX location or detection mechanism, which allows for the tracking of fraudulent operations across the country. The SIMBOX location or detection mechanism shall be capable of locating the SIMBOX's precise locations within Lesotho. The SIM locator shall be capable of extracting various types of information from SIM cards, such as MCC (Mobile Country Code), MNC (Mobile Network Code), and cell ID, IMEI number for identifying the location of SIM Boxes.

6.15.7 The system shall be capable of providing SIM card profile and generating automatic reports for 24/7.

6.15.8 The Tool shall have the capability to provide Terminal Equipment Identification details of fraudulent gateways.

6.16 **Reporting and service**

6.16.1 The Tool shall provide reports for both traffic volumes and settlement figures. Below are the minimum requirements of the system:

1	Real-time route traffic reports/graphs with clear colours distinguishing different routes/carriers.
2	Real-time QoS reports/graphs with clear colours distinguishing different routes/carriers.
3	Monthly aggregated report containing all results shall be provided
4	Daily list of Mobile Subscriber International Subscriber Identity Number (MSISDN) found shall be provided (fraud services)
5	Hourly list of MSISDN found shall be provided
6	Daily, Hourly and Weekly automatic e-mail reports containing charts & tables
7	Access to a dedicated online report

6.17 **Device Identification Module**

6.17.1 The system shall be able to collect information (i.e. International Mobile Equipment Identity (IMEI), international Mobile Subscriber Identity (IMSI)) of all devices connecting to Lesotho's networks and to create a centralized device identification database.

6.17.2 The system shall be capable of detecting stolen and counterfeited devices that need to be blocked.

6.17.3 The system shall allow for the management of white, grey and blacklists of devices.

6.18 **Telecom Revenue Auditing Module**

6.18.1 The system shall provide aggregated and detailed revenue-related data for all types of telecom services, continuously updated, in total and per operator, per type of services, and for prepaid and post-paid accounts.

6.18.2 The system shall be capable of monitoring and measuring the following types of traffic and services with associated revenues:-

1	On-net traffic
2	Off-net traffic
3	International incoming and outgoing traffic
4	Voice services
5	Messaging services
6	Data services
7	Roaming

6.18.3 The system should be able to collect comprehensive data on the following types of prepaid transactions:-

1	Electronic top-ups via USSD, API and Web services
2	Scratch card top-ups via SMS and USSD
3	Mobile money top-ups via SMS and USSD

6.19 **Data Services Monitoring Module**

6.19.1 The system shall provide aggregated and detailed data on mobile data services in Lesotho, including but not limited to the following:-

1	Bandwidth consumption in total and broken down per operator, OTT, application etc.
2	Detailed and continuously updated statistics on OTT usage and browsing
3	Source and destination users of the network/cloud applications

6.19.2 The system shall be capable of detecting potential cyber threats and/or non-compliant/illegal sites and services;

6.19.3 The system shall allow for the blocking of non-compliant/illegal sites and services.

6.20 **Mobile Money Transactions Module**

6.20.1 The system shall be capable of measuring and tracking all mobile money transactions and ensuring that all the mobile money transactions are legitimate.

6.20.2 The system shall be capable of tracking and differentiate National Mobile Money Transactions from International (Cross Border) Mobile Money Transactions.

6.20.3 The system should be able to raise alarms on suspicious transactions within a specified time – not less than one (1) Hour.

6.20.4 The system shall be capable of tracking statutory levies.

6.20.5 The system shall be capable of implementing a set of approved rules and regulations such as monitoring daily limits and enforcing full compliance with the rules.

6.20.6 The system shall be capable of addressing all of the following Mobile Money Transactions risks:-

1	Money laundering (identify frequent suspicious transaction)
2	Identifying transactions to blacklisted countries [Specifically Designated Nations] and blacklisted accounts.
3	Identifying suspicious activities for all subscriptions such as duplication of customer accounts, customer names or National Identity Numbers. This behaviour is associated with identity theft.
4	Identifying smurfing or transaction patterns intended to avoid the creation of certain records and reports. Smurfing involves breaking up a transaction involving a large amount of money into smaller transactions that are below the reporting threshold
5	Identifying transactions inconsistent with the regulatory requirements, such daily limits.
6	Identifying dormant accounts which are re-activated with due process
7	Cyber security attacks

6.20.7 The system shall be capable of creating management reports for the suspicious activities, Account activities, Money transfer by region and transaction trends. The reports shall include but not limited to:-

1	Name of Subscriber
2	Initiating Subscriber Number
3	Recipient Name and Subscriber Number
4	Amount Transferred
5	Transaction History

Suppliers are required to provide detailed information/description on how the system will achieve the above capabilities.

6.21 **Remittance Transactions**

6.21.1 The system shall be capable of measuring and tracking all remittance transactions processed by licensed Money Transfer Operators (MTO)s (e.g. Western Union, MoneyGram, etc.) and ensuring that all the remittance transactions are legitimate.

6.21.2 The system shall be capable of tracking and differentiating National Remittance Transactions from International (Cross-Border) ones.

6.21.3 The system shall be capable of raising alarms on suspicious transactions within a specified time – not less than one (1) Hour.

6.21.4 The system shall be capable of tracking statutory levies.

6.21.5 Identify frequent suspicious transaction (i.e. money laundering).

6.21.6 Identify transactions to blacklisted countries [Specifically Designated Nations] and blacklisted accounts.

6.21.7 Identify suspicious activities potentially linked to Money Laundering, based on predefined thresholds.

6.21.8 Identifying smurfing or transaction patterns intended to avoid the creation of certain records and reports. Smurfing involves breaking up a transaction involving a large amount of money into smaller transactions that are below the reporting threshold.

6.21.9 Identify transactions inconsistent with the regulatory requirements, such as daily limits.

6.21.10 The system shall be capable of implementing a set of approved rules and regulations such as monitoring daily limits and enforcing full compliance with the rules.

6.21.11 The system shall be capable of addressing all of the following Remittance Transactions risks:-

6.21.12 The system shall be capable of creating management reports for the suspicious activities, Account activities, Money transfer by region and transaction trends. The reports shall include but not limited to:

1	Name of sender
2	Recipient Name
3	Amount Transferred
4	Date and time of the transaction
5	Transaction History

6.21.13 Suppliers are required to provide detailed information/description on how the system will achieve the above capabilities. Suppliers should include schematic drawings or flowcharts.

6.22 Network Operations Centre (NOC)

6.22.1 The Network Operations Centre (NOC) shall consist of at least two (2) separate rooms. One room shall be the existing server room, which will house all the hardware equipment, and the second separate room shall house computers and monitoring screens.

6.22.2 The supplier shall provide drawings and description of NOC functional units, computers and display monitors. Each module of the DTCP shall have dedicated computers and display monitors (mounted on the walls or on desks).

6.22.3 The display monitors shall be a minimum of 32 inches and shall be dedicated to each functional unit (such as Billing, QoS, Self-health check etc.).

6.22.4 The NOC shall be capable of displaying dashboards for different user groups (Managers of Operational staff).

6.22.5 System Self Health Check functionality - Assessment of the functional status of all hardware (equipment) and software installed at both the operator's premises and at CLIENT premises.

6.22.6 The NOC should show logical and schematic architecture of all the equipment and interconnections points. RED colours shall be used to indicate faulty routes or unit while GREEN shall be used to indicate proper functionality.

6.22.7 All data and configuration information shall be entered in the NOC and all displays, reports and statistics are extracted from the NOC.

6.23 Network And Communication Specifications

6.23.1 All the links between the Network Operation Centre (NOC) and the Operator Gateways shall be Optical fibre and shall have redundancies. Redundancy may be in the form of multiple links or ring networks. Probes or interface with the gateways shall be designed to minimise loss of data in the event of failure. Link capacity must be increased once the link utilisation gets to 80% of available capacity.

6.23.2 The transmission network design shall ensure network availability exceeding 99.999%. There shall be sufficient transmission redundancy to achieve the desired 99.999% network availability.

6.23.3 SSL or IPSEC VPNS should be used to secure data in transit.

6.23.4 For Local Area Networks (LAN) and Wide Area Networks (WAN) equipment and software: Cisco switches and routers at a speed of 100/1000 Mbps and others at 1Gbps shall be used.

6.23.5 TCP/IP protocols suite and CISCO IOS of compatible latest versions shall be used.

6.24 **Training and Knowledge Transfer:**

6.24.1 The Authority considers training as a critical component to better utilise and operate the system. Bidders should make provision to train the relevant Authority's staff. A training schedule, including the duration should be provided.

6.24.2 The supplier shall provide suitable training to at least five (5) persons designated by the Authority in the use of the supplied System. Only qualified trainers with first-hand experience shall conduct the training.

6.24.3 The first training session shall be prior to Factory Acceptance Testing. This training shall be done at the suppliers' facilities.

6.24.4 The second session shall be carried out after Provisional Acceptance Testing. The training shall be conducted at the Authority's facilities. The Supplier shall be responsible for cost of living expenses and accommodation for its instructor.

6.24.5 Any necessary IT system administrator's training should be offered. For all the training, the supplier should indicate minimum qualifications for the attendees and shall supply the training schedule and modules for each course.

6.25 **Timeline for deployment and implementation of System**

6.25.1 The supplier shall clearly outline the post-contract award implementation timelines. Below are the proposed timelines:

1	System design	3 Months
2	Factory Acceptance Testing and Training	1 Month
3	Delivery [Shipment and Clearance]	1
4	Establishment of interconnect with operational telecom licensees	2 Months (Processes to run concurrently)
5	System Installation	
6	Testing and Commissioning	2 Weeks

6.26 **Computer Hardware Requirements**

The supplier shall provide detailed technical specifications of the hardware and software supplied.

6.26.1 Servers to be deployed shall have adequate capacity and processing power and support at least ten (10) years life expectancy.

6.26.2 The system shall have sufficient RAM and high processing speed.

6.26.3 Servers shall be rack mounted. Standard 19-inch server rack cabinets shall be used [typically 42 inches height, 19 inches wide]. The server rack cabinets shall have adjustable mounting rails.

6.26.4 Only modern equipment based on advanced technologies in terms of design shall be used. It should adopt the technologies and products which are currently advanced, mature and reliable, and able to meet the existing requirements, grasp the trend of development, and support the accomplishment of the advanced operation conceptions.

6.27 **Software Specifications**

6.27.1 **Operating Environment:** The Authority has standardised on Microsoft Windows operating systems both for users and server. Furthermore, the adopted database management system is Microsoft SQL Server. The vendors are required to specify a solution that will work in this environment. To the extent possible, the new system should automate workflows and notifications between user roles.

6.27.2 Web based GUI.

6.27.3 The system should have an availability of 99.999%.

6.27.4 The system shall provide system/application fallback and recovery options and methodology.

6.28 **Factory Acceptance Testing**

6.28.1 The supplier shall arrange for comprehensive training for purchaser technical staff at the suppliers' premises. The training materials, venue, trainers will be at the expense of the Supplier.

6.28.2 After training, the technical staff shall carry out Factory Acceptance Test to independently verify and prove functionality, quality and integrity of all the system modules. The Supplier shall provide a comprehensive checking process that should be agreed by both parties.

6.28.3 The Factory acceptance testing shall also be used to verify all-important documents, such as manuals, instructions, drawings and instrumentation diagrams.

6.28.4 Bidders shall provide certificate of conformity to warrant that the products have been tested and are compliant with the requirements set out in this RFP.

6.29 **Provisional Acceptance Testing**

6.29.1 Provisional Acceptance Testing shall be carried out after installations before the Authority accepts any module of the system. Provisional Acceptance Testing shall be used to verify system performance or confirmation that the system is performing in accordance to all technical requirements.

6.29.2 The Authority and supplier shall sign the Provisional Acceptance Certificate to evidence this step.

6.29.3 The Supplier shall provide a provisional acceptance-testing checklist that shall be agreed to by both parties.

6.30 **Final Acceptance Testing/Testing and Commissioning**

6.30.1 Final Acceptance Testing shall be carried out at the expiry of the warranty period. Final Acceptance Testing shall be used to verify system performance or confirmation that the system is performing accordance to all technical requirements after the warranty.

6.30.2 The purchaser and supplier shall sign the Final Acceptance Certificate.

6.30.3 The supplier shall provide a Final Acceptance Testing checklist that shall be agreed to by both parties.

6.31 **Warranty, Operations and Maintenance Support.**

6.31.1 The goods and services supplied under this specification shall be unconditionally warranted against any defects. The goods and services shall be used under normal local conditions and reasonably maintained in accordance with manufacturer's recommendations.

6.31.2 Bidders shall warrant (software & hardware) that all materials and workmanship are free from defect. The warranty period must be clearly stated in the bid documents.

6.31.3 The warranty period shall commence immediately after signing the Provisional Acceptance Certificate. The warranty shall run for the entire period until the transfer of the system to the Authority. During the warranty period, the supplier shall be responsible for operational costs, maintenance and support for the system.

6.31.4 The warranty period shall be agreed to by both the supplier and the Authority and shall coincide with the period that the supplier operates the system to recover supply costs.

6.31.5 The supplier shall be required to provide support services during the warranty period after the provisional acceptance testing of the system.

6.31.6 This will give Authority time to understand the system. Maintenance support agreement may be signed after Final Acceptance testing to be done at the end of warranty period.

6.32 **Maintenance Procedures**

6.32.1 A concise description of preventative, repair, maintenance and calibration procedures of the System shall be provided.

6.32.2 The bidder shall give details of all the recurrent costs (licenses).

6.33 **Installation, Measurement and Test Tools & Instruments**

6.33.1 The bidder shall include, in its offer, the tools and instruments that are required in order to properly maintain and operate the system and that must be part of the mandatory proposal items for supply.

6.34 **Documentation, Operation and Maintenance Manuals**

6.34.1 The supplier shall provide as-built system drawings and diagrams. Any changes between the original drawings and the actual installation drawings shall be highlighted.

6.34.2 The successful bidder shall supply the following operation and maintenance manuals, in English language:

a) 3 x Hardcopies of the System Operational Manuals and electronic version of the manuals

b) 3 x System Software Manuals and electronic version

c) Help features integrated within the systems software.

d) Any documentation that may assist in the smooth operations of the system.

6.35 **Power Back-Up/Battery Bank**

The bidder shall provide a Backup power Uninterruptible Power Supply (UPS) for the entire system in case of commercial power outages. The backup system shall be capable of providing autonomy power for up to twelve (12) hours.

6.36 **Mains Power Supply**

6.36.1 All active equipment must adhere to the mains power standard used in Lesotho (i.e. 220V 50Hz alternating current).

6.36.2 All active equipment must include power plugs in the standard used in Lesotho.

6.36.3 The supplier shall give notice of power requirements in advance.

7.0 CONDITIONS

Submissions of bids should be at the LCA Premises on or before the set deadline**. No electronic submissions will be allowed**. Submissions MUST meet all the conditions indicated below:-

7.1 BID REQUIREMENTS

7.1.1 The technical proposal shall indicate the full details of what will be supplied, with at least four (4) references where a similar assignment was undertaken. This should include contact persons, telephone numbers, physical address and other salient details pertaining to the delivery.

7.1.2 Service Provider profile – the service provider must submit its profile.

7.1.3 Current Tax Clearance Certificate of the country of domicile.

7.1.4 Certified copy of Traders License in the country of domicile.

7.1.5 Certified copies must be certified by the issuing Authority.

7.1.6 The above documents must accompany the technical proposal.

7.2 LCA'S RIGHTS

7.2.1 This invitation to tender does not commit the Authority to pay for any expenses incurred by the bidder in preparation of responses to this invitation.

7.2.2 The Authority reserves the right to accept or reject any response to this invitation to tender.

7.2.3 The Authority reserves the right to cancel or withdraw this request for proposals as a whole or in part without furnishing any reasons and without attracting any liability.

7.2.4 The Authority shall not be bound to accept the lowest bidder.

7.3 OTHER CONDITIONS

7.3.1 Lesotho Tax Laws SHALL be applicable.

7.3.2 The financial proposal shall indicate unit prices and total tender prices of the goods it proposes to supply.

7.3.3 The financial proposal shall clearly state the total bid price in Lesotho Loti (LSL). All prices shall include VAT if applicable.

7.3.4 The proposal must be valid for 60 working days from the submission date.

7.3.5 Late submissions shall not be accepted.

7.4 BID SUBMISSION FORMAT

7.4.1 The bidder must submit one (1) Original clearly marked "ORIGINAL" and seven (7) copies clearly marked "COPIES" as appropriate for both technical and financial proposals;

7.4.2 The envelope containing the technical proposal must be sealed, clearly marked "TECHNICAL PROPOSAL", and the envelope containing the financial proposal must be sealed, clearly marked "FINANCIAL PROPOSAL";

7.4.3 Both envelopes must be placed in one outer envelope clearly marked "TENDER FOR SUPPLY AND DELIVERY FOR THE SUPPLY OF A REVENUE ASSURANCE TOOL". Envelopes should not bear any identification of the bidder;

7.4.4 The technical proposal should NOT include any financial information.

7.5 TIME FRAMES AND OTHER DETAILS

7.5.1 Any requests for clarification on the RFP must be addressed in writing to the Chief Financial Officer at admin@lca.org.ls at least five days prior to the deadline. The Authority will respond to written inquiries or queries only.

7.5.2 The bids must be submitted at LCA Offices at 30 Princess Margaret Road, Old Europa, Maseru on or before the Tuesday 14 April 2020 at 12:00hrs. No proposals will be received after the closing time.

7.5.3 Opening of bid documents will be on the 14 April 2020 at 14:30hrs at LCA premises. Interested bidders are invited for the bid opening. Only one representative from a bidder may attend.

7.5.4 The selected company will be notified in writing and invited for contract negotiations.

7.5.5 Lesotho Taxation Laws SHALL be applicable. Bidders should therefore, familiarise themselves with the tax requirements of Lesotho.

7.5.6 The financial proposal should clearly state the total bid price in Lesotho Loti.

7.5.7 Late submissions shall not be accepted.

7.6 DISCLAIMER

7.6.1 This RFP does not commit LCA to pay for any expenses incurred by the bidder in the preparation of responses to this invitation.

7.6.2 LCA reserves the right to accept or reject any response to this RFP.

7.6.3 All proposals shall be signed and LCA shall not be bound to accept the lowest bidder.

7.6.4 Bids shall remain valid for three (3) months following the closing date.

7.7 **All submissions must be addressed to:-**

Lesotho Communications Authority
30 Princess Margaret Road, Old Europa
P. O. Box 15896
Maseru 100
LESOTHO

7.8 **The closing date for submission of proposals:**

Tuesday 14th April 2020.