KENYA REVENUE AUTHORITY

ISO 9001:2015 CERTIFIED

INTERNAL

TERMS OF REFERENCE FOR LABORATORY INFORMATION MANAGEMENT SYSTEM (LIMS)

Delivery, implementation, commissioning, maintenance and support of laboratory information management system (LIMS) at Kenya Revenue Authority Inspection & Testing Centre.

Background

Kenya Revenue Authority has a laboratory (Inspection &Testing Centre) within the Kenya Revenue Authority Offices at Times Tower and another satellite laboratory at the southern region, Mombasa, the laboratory is charged with drawing and analysis of samples of suspicious chemical shipments that are intercepted by Customs, I&ED, LMT & MST officers leveraging on prior intelligence reports and profiling done by the Investigation unit and other Departments within the Kenya Revenue Authority, the samples are analysed for purposes of identification to mitigate the risk of mis-declaration, Mis-classification and risk of revenue losses.

The LIMS System is expected to facilitate sampling, registration of samples, analysis of samples for purposes of tariff classification of samples, reporting on the findings to the requesting Departments in order to facilitate trade. Training of the users on the functionality of the System. Currently this processes are done manually and acquisition of the Laboratory Information Management System will enhance the efficiency of the Inspection and Testing Centre processes by mitigating the risks encountered when the process is done manually.

The Inspection &Testing Centre seeks to enhance the laboratory processes by implementing Laboratory Information Management System (LIMS) which is also recommended for a testing laboratories implementing ISO/IEC 17025:2017 a reference standard for accredited testing laboratories.

The Central Testing Laboratory in Times Tower Nairobi carries out the following activities;

- Sampling of trade commodities mostly chemical in nature.
- Registration of the sampled commodities
- Analysis of the sampled products.
- Reporting on the laboratory findings of the sampled products.
- HS Code classification of the sampled products after analysis.
- Issuing the laboratory reports to user department (Customs & I&ED, LMT & MST)

The Satellite Laboratory in Mombasa carries out the following activities:

- Sampling of trade commodities
- Analysis of alcoholic Beverages
- Analysis of Fats & Oils

Currently all these processes are done manually; acquisition of LIMS will enhance the efficiency of the process.

Scope of work

Successful bidder will be required to undertake the following at minimum to ensure that LIMS solution is secure, effective and compliant with organizational and regulatory requirements.

a) Define security needs, risks and compliance requirements to be addressed by the LIMS
b) Review the existing Inspection &Testing Centre business process model for the purpose of supplying a desired solution, while meeting the Inspection & Testing Centre identity management objectives and industry best practice.
c) Supply Laboratory Information Management System that addresses the needs of both the existing and future models of operations of the Inspection &Testing Centre.
d) Build capacity in the KRA-Inspection & Testing Centre team to competently implement and maintain the Laboratory Information Management System.
e) Train KRA-Inspection &Testing Centre teams on Laboratory Information Management System components.
f) Support the KRA-Inspection &Testing Centre team on maintenance and support of the Laboratory Information Management System on a need basis.
g) Evaluation of process flow and lab activities to establish requirements,
h) Software installation and configuration, system verification and validation, staff training and knowledge transfer on the system operation and administration, and maintenance

Expected Deliverables

The LIMS is expected to deliver the following:

a) Track the sample status once samples have been received at the Inspection & Testing Centre.
b) Account for all reports issued by the Inspection &Testing Centre.
c) Track quantity, location, and vendor information for Laboratory Items such as chemicals and consumables.
d) Integrate with other KRA Systems & laboratory equipment

1.0 Comprehensive List of Technical Requirements for Supply, Delivery, Installation, Testing and Commissioning of Laboratory Information Management System

The bidder must provide substantive response or a commitment to provide the services as per the stated requirement. Response by use of YES or NO is not allowed.

	LABORATORY INFORMATION MANAGEMENT SYSTEM (LIMS) REQUIREMENTS.		
1.1	Provide deliverable to fulfill the corresponding user requirement specification under the response column	**Bidders' response (Please provide a Relevant narrative response)**	**Evaluation Remark (PASS or FAIL)**
1.1.1	The laboratory information management system (LIMS) shall be COMMERCIAL-OFF-THE-SHELF (COTS) solution designed for small to large scale chemical testing operations, and shall be; 1) Configurable, scalable and adaptable to changes over time 2) Modular allowing addition of functions 3) Capable of meeting the current and the changing needs of the Kenya Revenue Authority, Inspection and Testing Centre.		
1.1.2	The laboratory management system shall provide the following features as a minimum; 1) Workflow automation to reduce human error 2) Centralized access and storage of quality control data 3) Integrate with other lab instruments and system 4) Track reagents and lots from sequencing runs 5) Perform instrument run monitoring 6) Manage downstream data analytics		
1.1.3	The system should allow integration with the following systems but not limited to: 1) Microsoft office suite 2) Email 3) SAP ERP (Enterprise Resource Planning) 4) Customs Management System (ICMS) 5) Other relevant systems used by the Kenya Revenue Authority		

1.1.4	The Laboratory Information Management System (LIMS) processing functions shall cover the laboratory processing phases, but not limited to the following: 1) Sample reception and registration 2) Assignment of tests, scheduling of work and tracking of sample 3) Quality control of the sample, solutions and instruments. 4) Recording, processing and storage of data 5) Review and approval of sample analysis results, and reporting			
1.1.5	The bidder shall provide Manufactures Authorization if they are not the manufactures.			
1.2	**TECHNICAL REQUIREMENTS**			
1.2.1	**Sample Registration**			
1.2.2	Sample log-in	The system shall enable manual and automatic recording of relevant sample data. The Laboratory Information Management System should be able to produce timely and accurate analytical data and reports. The key features shall include, but not limited to the following: 1. Sample log-in 2. Sample identification 3. Barcode labeling 4. Sample distribution 5. Sample tracking 6. Chain of custody and audit trail 7. Assigning work 8. Status monitoring 9. Data entry and storage 10. Electronic data transfer 11. Data import and export 12. Quality control 13. Data analysis 14. Data validation 15. Review and approval of results 16. Reporting results 17. Data queries 18. Document management 19. Personnel Management 20.Inventory management 21.Customer relationship management		

		22.Billing for laboratory services 23.Regulatory compliance		
1.2.3	Batch sample login	The system shall allow single and multiple registration of a set of samples in a single operation, and assign unique sample identification number to each sample in the batch		
1.2.4	Sample identification	The system shall automatically assign unique identification number to each sample		
		In the case where a sample is split or subdivided, the system shall assign and associate subsequent identification numbers with the original sample		
1.2.5	Sample labels	The system shall generate sample identification labels, with bar codes, for affixing to sample containers		
1.2.6	Routine sample scheduling	The system shall automatically log-in routine samples according to schedule, including hourly, daily, weekly, monthly or yearly		
1.2.7	Sample information	The system shall capture and store information including sampling, purpose for analysis, sample comments, and requesting address. The system shall support digital picture and document uploading and attachment, and associate with the sample		
1.2.8	Transmission of requests	The system shall be capable of receiving sample analysis requests from remote locations using the web and third party software		
1.2.9	Sample turnaround time	The system shall update sample due date based on receiving date and sample holding time.		
1.3.0	**Sample Tracking**			
1.3.1	Sample tracking	The system shall have ability to follow the sample processing status through the laboratory.		
1.3.2	Chain-of-custody documents	The system shall produce chain of custody documents for each sample collected, and maintain a complete history of sample transfers from receipt to disposal.		
1.3.3	Audit Trail	The system shall maintain records of changes, when the change was made, who made the change, and why it was changed		

1.4.0	**Assigning Work**			
1.4.1	Select and assign tasks	The system shall allow for the selection and assignment of tests to analysts and laboratory sections		
1.4.2	Sample procedures and tests	The system shall associate appropriate procedures with tests required for specific type of sample		
1.4.3	Standard tests per sample type	Each test shall be uniquely identified with a code, and association of multiple test components with the test code		
1.4.5	User identificatio n	The system shall identify the laboratory analyst who performed the test, and who entered the results		
1.5.0	**Data Entry and Storage**			
1.5.1	Test result entry	The system shall allow the user to view, enter, validate, approve, and report results		
1.5.2	Instrument data entry	The system shall enable automated data entry from interfaced instruments		
1.5.3	Data validation	The system shall validate data and indicate warnings and reruns		
1.5.4	Test data modification	The system shall allow authorized users to modify and delete test data		
1.5.5	Calculations	The system shall support calculations for the generations of sample test results		
1.5.6	Statistical analysis	The system shall enable statistical data analysis		
1.5.7	Graphics	The system shall have graphics capabilities for display of charts and plots and reporting of statistical information		
1.5.8	Special result values	The system shall record special result values such as: not detected, not measured, <, or null in mathematical computations		
1.5.9	Result limits	The system shall allow users to enter test data results limits used for checking the results entered, and indicate the results that are out of limits		
1.5,10	Comments	The system shall allow entry of comments to explain test results		
1.5.11	Check test results	The system shall enable checking of tests results, and data entry operations		
1.5.12	Review test results	The system shall allow peer review of test results and indicate review actions, including agreement, disagreement, re-		

		test or re-collection of sample for re-run of test		
1.5.13	Approval test results	The system shall enable approval of test results, as quality assurance approval, in order to make the data available to customers		
1.5.14	Protection of test results	The system shall prevent any further modifications to the sample and its associated data after approval		
1.5.15	Data archiving	The system shall enable moving of old data to archive database and viewing of the data without restoring into active location		
1.5.15	Data backup	The system allows automated backup and restore capability, as well as manual backup		
1.6.0	**Quality Control**			
1.6.1	Quality control data	The system shall track quality control data, including sample replicates, matrix spikes, quality control check standards, and blanks		
1.6.2	Quality control calculations	The system shall generate precision and accuracy data from replicate samples and quality control standards.		
1.6.3	Quality control charts	The system shall generate and update quality control charts using quality control data		
1.6.4	Quality control limits	The system shall calculate quality control results and indicate data not within the defined quality control limits		
1.7.0	**Reporting Results**			
1.7.1	Types of reports	The system shall develop various types of reports including analytical reports, sample status reports and other reports		
1.7.2	Sample reports	The system shall generate single sample analysis reports, batch analysis reports or multi-sample analysis reports		
1.7.3	Certificate of analysis	The system shall provide certificate of analysis report formats for different products and customers		
1.7.4	Report development	The system shall allow development of templates for different types of reports		
1.7.5	Management reports	The system shall provide work assignment and turnaround time reports		

1.7.6	Cost accounting reports	The system shall generate client billings for work orders Indicating test(s) performed and test charges		
1.7.7	Ad-hoc reports	The system shall enable the user to generate various types of reports		
1.7.8	Reports recipients	The system shall electronically deliver reports to single or multiple recipients.		
1.8.0	**Electronic Data Transfer**			
1.8.1	Testing instruments	The system shall enable interface with at least two (2) testing instruments, including analytical balance		
1.8.2	Portable testing devices	The system shall enable data transfer from portable field laboratory testing devices		
1.8.3	Data processing	The system shall receive and process analytical and quality control sample results from personal computers		
1.8.4	Web-based access	The system shall allow remote accesses using portable devices, including telephones, tablets, laptops and desktops		
1.8.5	Electronic notebook	The system shall have integrated electronic notebook solution to replace laboratory paper registers		
1.8.6	Data transfer to clients	The system shall have data import and export capabilities		
1.8.7	System integration	The solution MUST Provide for integration with other systems for data and information exchange based on standards such as XML, JSON		
1.9.0	**Data Queries**			
1.9.1	Ad-hoc queries	The system shall enable users to retrieve logically related data in an interactive environment		
1.9.2	Standard queries	The system shall provide queries for a specific sample data, results for a specific sample location, status of samples, status of tests, and administrative or static data		
1.9.3	Multiple query criteria	The system shall enable retrieval of sample data based on identification number, description, location, analyst name, date received, section, test, sample type, and status		
1.9.4	Query facility	The system shall have structured query language (SQL) facility		

1.9.5	Multiple output options	The system shall enable display of query results in appropriate file format		
1.10.0	**Laboratory Management**			
1.10.1	Document management	The system shall enable capture, storage, viewing and editing of documents, including standard operating procedures, certificate of analysis, logbooks, and test sheets		
1.10.2	Customer relationship management	The system shall maintain customer records, and manage enquiries and track actions taken towards resolution of complaints. The system shall allow customer to retrieve analytical reports		
1.10.3	Personnel management	The system shall maintain employee training and testing proficiency, including history of tasks performed		
1.10.4	Supplies inventory management	The system shall create purchase requisitions for laboratory chemicals, supplies, equipment, instruments, standards and other laboratory supplies, and receive and update supplies records, with ordering level alert		
1.10.5	Equipment management	The system shall enable tracking of equipment calibration and preventive maintenance schedules and repairs status, with due date alert		
1.11.0	**Regulatory Compliance and security**			
1.11.1	Compliance with ISO 17025:2017	The system shall support compliance with Good Laboratory Practice (GLP), including with ISO 17025:2017		
1.11.2	Security	The system shall support login security, periodic password changes, and electronic signature		
1.12.0	**System Management**			
1.12.1	License	Specify requirements for licensing and renewal, and clarify one-off payment options, and post-license data management		

1.12.2	Concurrent users	The system shall be accessed based on the number of concurrent users, including number of interfaced instruments, and with provision for more users according to need		
1.12.3	System management tools	Specify system management tools for safe and secure management of the application, including application security, data audit trail, database backup and recovery, data archival and restoration		
1.12.4	Security	Specify security features and access levels to restrict use of the system functions, including users defined by roles and permissions		
1.12.5	Data archiving	The system shall enable archiving of data automatically after a period of time or at the request of the system administrator		
1.12.6	Static information	The system shall maintain static administrative information, such as but not limited to, procedures and safety information		
1.13.0	**Management system Database**			
1.13.1	Database management	The system shall utilize relational database management system (RDBMS) for information storage or retrieval		
1.13.2	Graphic user interface	The system user interface and all interactive database management tools shall be based on Graphical User interface (GUI) or equivalent		
1.13.3	Data export	The system shall be able to extract and convert data elements into EXCEL, ASCII, XML or other equivalent format.		
1.13.4	Data import	The system shall be able to import an EXCEL, ASCII or other data file, convert, and store the data in the database		
1.13.5	Interoperability	The system shall be based on Open Database Connectivity (ODBC) or equivalent, to enable systems and databases communications		
1.14.0	**System Infrastructure**			
1.14.1	Leverage on existing infrastructure	The proposal shall include options to utilize the existing platform(s), systems, hosting server and hardware used at the Kenya Revenue Authority		

1.14.2	System components	The system components shall have open architecture, modular or extensible to facilitate addition of new functions		
1.14.3	System architecture	The vendor should provide the proposed system architecture configuration, and include drawing		
1.14.4	Server	The vendor should provide the required server specifications in terms of CPU cores, Memory and storage requirements		
1.14.5	Database Platform	The solution should be compatible with leading server database platforms, such as Oracle, postgres, MSSQL, MySQL.		
1.14.6	Operating system	The client application should be compatible with various operating systems such as Windows, Linux & Mac.		
1.14.7	Server operating system	The server application should be compatible with various operating systems such as Windows &Linux.		
1.14.8	Browser	The system shall be compatible with world wide web browsers (Mozilla, Chrome, Edge, Opera, Safari as a minimum)		
1.14.9	Hardware	Specify hardware configurations for running the Laboratory Information Management System clients and servers		
1.15.0	**Installation Services**			
1.15.1	Start-up services	Provide installation and start up services, including populating all the laboratory information management system with the laboratory static data, loading required software on the system server, client workstations, and instrument PCs, and creating all necessary command files to activate the system upon startup		
1.15.2	Implementation	The solution MUST be implemented on premise		
1.15.3	Loading system software	Load the required software on the server delivered as part of the system, with option to use hosting server at the Kenya Revenue Authority		
1.15.4	Install system hardware	Install hardware components required for operation of the laboratory information management system		
1.15.5	Documentation	Provide complete documentation of the system application software and instrument interfaces		

1.16.0	**System Configuration**			
1.16.1	Software configuration	The system shall allow on-site configuration and generation of application related programs, including displays, tables and reports		
1.16.2	System flexibility	The system shall allow users to make changes to meet the workflow requirements and accommodate the way in which the laboratory does business		
1.16.3	Additional functions	The system shall have ability to add functions to the program menu and screen in line with user needs		
1.17.0	**Training**			
1.16.1	Course outlines	Provide course outlines for user and administrator training		
1.16.2	Training materials	The training shall include provision of training manuals, workbooks, administrator training guides, training aids, and technical manuals		
1.16.3	Initial user training	Initial training shall be conducted on-site at the Kenya Revenue Authority		
1.16.4	Follow-up training	Follow-up training shall be provided on-site or at any other location		
1.16.5	System administration training	Provide training on proper installation, configuration, system administration and maintenance of the system		
1.17.0	**Functional and acceptance testing**			
1.17.1	Verification Testing	System testing shall be tested after installation to demonstrate operation of the components, performance and functionality of the system and all the features		
1.17.2	Acceptance Testing	The acceptance test shall run for 120 days or specified number of days, to test stability and completeness over time. The users shall be trained and start using the system in day- to-day operations, with assistance		
1.17.3	Final Acceptance	Final acceptance shall be upon successful testing and completion of the test period.		
1.18.0	**Product support**			

1.18.1	Technical Support	Specify provision of first three (3) year unlimited technical support for all products included under this contract		
1.18.2	24/7 support	The bidder MUST provide for 24/7 support arrangements within agreed SLA framework		
1.18.3	software updates	The bidder MUST include vendor premier support AT NO COST that include; 1) Software/system updates 2) Direct access to manufacturers technical support team 3) Online troubleshooting/support tools 4) Proactive diagnosis services		
1.18.4	Version updates	Provide software version updates, upgrades and enhancement, and bug fixes at no cost.		
1.18.5	System maintenance	The bidder to provide SLA for support and maintenance.		

TABLE 2.0: MINIMUM TECHNICAL AND IMPLEMENTATION REQUIREMENTS

Instructions to Bidders:

1. Bidders <u>MUST</u> complete the Table below in the format provided.
2. Bids MUST meet all mandatory (MUST) requirements in the Tables below in order to be considered for further evaluation.
3. Bidders MUST provide a substantial response or clear commitment to meeting the requirements for all features irrespective of any attached technical documents in the table format (bidders Response) below. Use of Yes, No, tick, compliant, blank spaces etc. will be considered non-responsive.
4. Bidders who do not comply with any of the below requirements will NOT be considered for further evaluation

S/No	Feature	Minimum Specification	Bidder Response (Narrative answers score)
1.1	**Key System Features**	a) The laboratory information management system (LIMS) **MUST** be COMMERCIAL-OFF-THE-SHELF (COTS) solution designed for small to large scale chemical testing operations, and shall be;	
		b) LIMS **Must** Configurable, scalable and adaptable to changes over time	
		c) LIMS **MUST** be Modular allowing addition of functions	
		The laboratory management system **MUST** provide the following features as a minimum; 1) Workflow automation to reduce human error 2) Centralized access and storage of quality control data 3) Integrate with other lab instruments and system 4) Track reagents use 5) Perform instrument run monitoring 6) Manage downstream data analytics	
		The Laboratory Information Management System (LIMS) processing functions **MUST** Perform following: 1) Sample reception and registration 2) Assignment of tests, scheduling of work and tracking of sample 3) Quality control of the sample, solutions and instruments. 4) Recording, processing and storage of data 5) Review and approval of sample analysis results, and reporting	
2.1	**Integrations**	The LIMS System MUST be able to integrate with: 1) Microsoft 2) Email 3) SAP ERP (Enterprise Resource Planning) 4) Customs Management System (ICMS)	

3	**Data Base Platform**		
3.1	Database management	The system MUST utilize relational database management system (RDBMS) for information storage or retrieval	
3.2	Graphic user interface	The system user interface and all interactive database management tools MUST be based on Graphical User interface (GUI) or equivalent	
3.3	Data export	The system MUST be able to extract and convert data elements into EXCEL, ASCII, XML or other equivalent format.	
3.4	Data import	The system MUST be able to import an EXCEL, ASCII or other data file, convert, and store the data in the database	
3.5	Interoperability	The system MUST be based on Open Database Connectivity (ODBC) or equivalent, to enable systems and databases communications	
4.0	**System Infrastructure**		
4.1	Leverage on existing infrastructure	The proposal MUST include options to utilize the existing platform(s), systems, hosting server and hardware used at the Kenya Revenue Authority	
4.2	System components	The system components MUST have open architecture, modular or extensible to facilitate addition of new functions	
4.3	System architecture	The vendor MUST provide the proposed system architecture configuration, and include drawing	
4.4	Server	The vendor MUST provide the required server specifications in terms of CPU cores, Memory and storage requirements	
4.5	Database Platform	The solution MUST be compatible with leading server database platforms, such as Oracle, postgres, MSSQL, MySQL.	

4.6	Operating system	The client application MUST be compatible with various operating systems such as Windows, Linux & Mac.	
4.7	Server operating system	The server application MUST be compatible with various operating systems such as Windows &Linux.	
4.8	Browser	The system MUST be compatible with world wide web browsers (Mozilla, Chrome, Edge, Opera, Safari as a minimum)	
4.9	Hardware	MUST Specify hardware configurations for running the Laboratory Information Management System clients and servers	
5.0	**Installation Services**		
5.1	Start-up service	MUST Provide installation and start up services, including populating all the laboratory information management system with the laboratory static data, loading required software on the system server, client workstations, and instrument PCs, and creating all necessary command files to activate the system upon startup	
5.2	Implementation	The solution MUST be implemented on premise	
5.3	Loading system software	LIMS software MUST be loaded on the server delivered as part of the system, with option to use hosting server at the Kenya Revenue Authority	
5.4	Install system hardware	Install hardware components required for operation of the laboratory information management system	
5.5	Documentation	Provide complete documentation of the system application software and instrument interfaces	
6.0	**System Configuration**		

6.1	Software configuration	The system shall allow on-site configuration and generation of application related programs, including displays, tables and reports	
6.2	System flexibility	The system shall allow users to make changes to meet the workflow requirements and accommodate the way in which the laboratory does business	
6.3	Additional functions	The system shall have ability to add functions to the program menu and screen in line with user needs	

TABLE 3: Vendor Evaluation Criteria

Item	**Requirement**	**Evaluation Criteria**	**Maximum score**
1	**Company Experience** Demonstrated experience through Previous execution of at least three (3) Laboratory Information Management System.	Demonstrated experience through Previous execution of at least three (3) Laboratory Information Management System projects. **6 marks** In order to be awarded marks bidders MUST: a) Submit a copy of executed Contract or LSO, supported by a brief description of the project delivered **(1 mark)** **b)** Completion Certificate/Reference/Recommendation Letter from the Customer confirming successful completion of the project**. (2 marks)**	9

		c) Full contacts; address, telephone and email of customer where assignments/ projects were executed.	
	Lead Expert Qualifications	Academic & Professional Qualifications **Bachelor's degree in:** Laboratory Sciences (Analytical Chemistry, Industrial Chemistry, Biochemistry, Forensic Science), or Information Systems / Computer Science with strong laboratory systems experience **(3marks)** **Master's degree in Laboratory** Management, Information Systems, Analytical Chemistry, or Forensic Sciences is an added advantage Relevant Professional certifications (**1 mark)** LIMS Administration or Implementation certification **(1 Mark)** Project Management (PRINCE2, PMP) – **(1 Mark)**	3
	Lead Expert Experience **Minimum 5 years' experience** working in an analytical, forensic, customs, or regulatory laboratory or Computer Science with strong laboratory systems experience	**Proven experience supporting laboratories in any of the following:** ▪ Chemical analysis ▪ Environmental, forensic, or customs-related testing ▪ Handling hazardous or controlled substances ▪ Experience working in multi-site laboratory environments (main lab + satellite labs) ▪ Computer Science with strong laboratory systems experience Qualified Staff Relevant experience • Over 5 years– **3 Marks** • 5 years – 2 Marks • Less than 5 Years - 0 Mark	3

		Note: Bidders MUST provide CV for each staff clearly indicating the years of experience in supporting an LIMS implementation.	
2	**Technical staff Qualifications.** Minimum of two (2) Technical staff with the following academic and professional qualifications: 1) *Academic Qualifications:* A minimum of Relevant University Degree or Diploma. (Computer Science, IT, electronics or related fields)	**3 Marks** for each Qualified Staff (1 mark for degree, 2 marks for relevant professional qualification) **Note:** Bidders MUST attach CV of each staff supported by Academic and professional certificates in order to be scored.	6
3	**Staff Relevant experience** Each Qualified staff (refer to clause 2 above) should preferably have minimum of two (2) years of experience in implementation, support and maintenance of a Laboratory Information Management System.	Qualified Staff Relevant experience • Over 2 years– **3 Marks** for each qualified staff • Above 2 years – 2 Marks • 2 Years - 1 Mark **Note**: Bidders MUST provide CV for each staff clearly indicating the years of experience in supporting an LIMS implementation.	6
4	Technical Approach/Methodology	Bidders to demonstrate/provide evidence of a clear and detailed understanding of the solution, including: a) Project delivery Approach and Methodology for implementation and support of the solution – **3 Marks** b) Provide a Work plan (Bidder MUST provide a work plan Implementation and support for the solution – **3 Marks**	6

5	Proposed Design & Architecture of the LIMS	Bidders MUST submit a proposed design and architecture for the LIMS demonstrating how they propose to deploy the LIMS. (5 Marks)	5
	Total Score		**38**
	Cut Off		**32**

Financial Requirement

- **N/B: Bidders to provide a breakdown of how they have arrived at the total cost**
- **Grand Total Cost –To be carried Forward to the FORM FIN 2 Summary of Costs**

Post-Qualification/Due Diligence

The Procuring Entity reserves the right to conduct post-qualification and due diligence on the lowest evaluated bidder before the award of the contract. This process may include, but is not limited to:

1. Verification of Documentation – Confirming the authenticity of certifications, reference letters, and any other supporting documents submitted with the bid.
2. Site Visits and Inspections – Conducting physical or virtual inspections of the bidder’s premises, data centres, or operational facilities to assess capability, infrastructure, and compliance with the technical requirements.
3. Reference Checks – Engaging with past and current clients to verify performance, service delivery, and adherence to contractual obligations.
4. Financial Capability Assessment – Evaluating the financial strength of the bidder to ensure their ability to sustain the project, including a review of audited financial statements.
5. Technical Evaluation – Reconfirming the ability of the bidder to provide the required LIMS Solution, including implementation, support, and maintenance in accordance with the stated service levels.
6. Regulatory and Legal Compliance – Ensuring that the bidder complies with relevant national and international laws, industry regulations, and standards applicable to cybersecurity protection.

Failure to satisfactorily pass the post-qualification and due diligence process may result in the disqualification of the bidder, and the Procuring Entity reserves the right to consider the next lowest evaluated bidder or take any other appropriate action in accordance with procurement laws and regulations

General Rule: The solution must implement API-first design for integration i.e. API-first design for integration is a development strategy where APIs are designed, documented and defined before any application code is written, treating the API as a core product, not an afterthought.	
	ANNEX I - API Security Requirements
	Review Area
1	**Governance**
1.1	Ensure the API is properly versioned. Versioning helps in keeping track and maintainance of the API.
1.2	Ensure that the API conforms to the orgnization set style and design guidelines such formatting of headers for consistency.
1.3	Ensure that the API is included as part of the organization's APIs inventory for Discoverability and Reusability
2	**Authentication**
2.1	Ensure that every request to the API or web service is authenticated.
2.2	Ensure a strong authentication mechanism is used; Required authentication mechanisms allowed for APIs/Web services in KRA are OAuth 2.0 and JWT
2.4	Ensure implementation of anti-brute force mechanisms on authentication endpoints such as account lock-outs, use Max Retry and jail features in Login.
2.6	When JWT is used, ensure: 1. Use a random complicated key (JWT Secret) to make brute forcing the token very hard. 2. Don't extract the algorithm from the header. Force the algorithm in the backend (HS256 or RS256). 3. Make token expiration (TTL, RTTL) as short as possible. 4. Don't store sensitive data in the JWT payload, it can be decoded easily.
2.7	When OAuth 2.0, ensure: 1. Always validate redirect_uri server-side to allow only whitelisted URLs. 2. Always try to exchange for code and not tokens (don't allow response_type=token). 3. Use state parameter with a random hash to prevent CSRF on the OAuth authentication process. 4. Define the default scope, and validate scope parameters for each application.
2.8	Ensure no sensitive authentication details, such as auth tokens and passwords are sent in the URL through GET requests.
3	**Authorization**
3.1	Ensure a proper authorization mechanism is implemented that checks if the authenticated subject has access to perform the requested action.
3.2	Ensure that the issued authentication and authorization tokens have a set expiry time.
3.3	Ensure the use of random and unpredictable values as Globally Unique Identifiers (GUIDs) for records identification. Auto-incrementing IDs should never be used.

3.4	Ensure the use of proper HTTP method for each API operation: GET (read), POST (create), DELETE (to delete a record). No request should be processed if the method is not appropriate for the requested resource.
3.5	Ensure the intergrating components only access the objects they require from the integrating systems. Responses should only return the data necessary to fulfill a request
4	**Data Protection**
4.1	Ensure that the responses from the API provide only legimate requested data that is not excessive.
4.2	Ensure sensitive information such as access tokens, bearer tokens, pins, passwords etc are not being returned in request responses or stored in logs in clear text.
4.3	Error messages must ensure that sensitive information about the integrating systems is not disclosed
4.4	Ensure sensitive data parameters such as passwords, PINs, Credit card numbers etc. being passed to the APIs are hashed
4.5	Ensure minimization/masking of customer PII such as MSISDN and ID Numbers when such are returned in request responses and displayed in logs.
4.6	Ensure the communication channel is encrypted. The Endpoints should make use of HTTPS and not of HTTP
4.7	Ensure proper implementation of HTTPS; i.e current secure TLSV
5	**Resource and Rate Limiting**
5.1	Ensure implementation of a limit on how often a client can call the API within a defined timeframe. This helps mitigate DoS attacks by throttling or blocking IP addresses after making concurrent requests within a very short period of time.
5.2	Define and enforce maximum size of data on all incoming parameters and payloads such as maximum length for strings and maximum number of elements in arrays.
5.3	For APIs processing large amounts of data, ensure data is processed asynchronously. Processing large amounts of data synchronously can prevent the API from responding in a timely manner forcing clients to wait.
6	**Secure Configuration**
6.1	Ensure implementation of the **X-Content-Type-Options: nosniff** header to protect API against MIME sniffing vulnerabilities.
6.2	Ensure implementation of the **X-Frame-Options: deny** header.
6.3	Ensure implementation of the **Content-Security-Policy: default-src 'none'** header.
6.4	Ensure that fingerprinting headers such as **X-Powered-By**, **Server**, **X-AspNet-Version**, etc are not present
6.5	Force content-type for your response. If you return application/json, then your content-type response is application/json.
6.6	Return the proper status code according to the operation completed. (e.g. 200 OK, 400 Bad Request, 401 Unauthorized, 405 Method Not Allowed, etc.).
7	**Vulnerability Management**
7.1	Ensure that the API supports use of updated and vendor supported dependencies and libraries.
7.2	If the API is externally facing, ensure that it's behind a Firewall
7.3	Ensure that unused dependencies, unnecessary features, components, files, and documentation are deleted in production APIs
8	**Data/Input Validation**
8.1	Perform data validation using a single, trustworthy and actively maintained library.

8.2	Validate, filter and sanitize all client-provided data, or other data coming from integrated systems.
8.3	Special characters should be escaped using the specific syntax for the target interpreter.
8.4	Prefer a safe API that provides a parameterized interface.
8.5	Always limit the number of returned records to prevent mass disclosure in case of injection.
8.6	Validate incoming data using sufficient filters to only allow valid values for each input parameter.
8.7	Define data types and strict patterns for all string parameters.
9	**Auditing and Logging**
9.1	Log all failed authentication attempts, denied access, input validation errors and rate limit errors
9.2	Ensure all requests and responses are logged
9.3	Ensure the logs are in a format that is consumable by SIEM systems
9.4	Ensure the log contains sufficient details including the actual source IP instead of a Load balanced IP in cases where the service is hosted behind a load balancer.
9.5	Ensure both the raw http access logs as well as the transactional logs are sent to a SIEM
9.6	Based on the functionality provided by the API define usecases for monitoring at the SOC
9.7	A facility should exist to allow Manual triggering of transactions/actions under special circumstances (eg Intergration breakdown, compromise etc) There must be audit trail on the facility
10	**Network controls**
10.1	All network communications between intergrating components must be authenticated, and must not explicitly trust other network devices
10.2	API's must not connect to a database as a privileged user, such as the SA account in SQL Server or SYSTEM account in Oracle
10.3	All function calls between applications should implement digital signatures to verify authenticity of the invoking application (eg tokens, SSL)
11	**Encryption**
11.1	API Authenticating tokens must be randomn and unpredictable
11.2	Data sent between intergrating systems must be encrypted in transit. Recommended algorithms (with minimum bit lengths), in order of preference, are: Hashing: SHA -512, SHA -256, RIPEMD160. Symmetric: AES256, AES192, AES128, 3 -DES (168 bits), Blowfish(minimum 128 bits), Twofish (minimum 128 bits), IDEA (128 bits),and RC4 (128 its). Public key: RSA(minimum 2048 bits) and DSA(minimum 2048 bits), ElGamal (minimum 2048 bits)
11.3	Encryption keys must be protected during transit and while stored in file system
11.4	A key used to decrypt data must not be stored in the same location as data encrypted with the key
11.5	Site certificates must be current and issued by a well-known certificate authority
12	**Documentation**
12.1	A design blue print with data flow or flow chart diagrams should be present as part of the integrating application system/module/component documentations
12.2	Signed user requirements/specifications document should be present as it forms the basis for the development of a new application or modification of an existing system

	ANNEX II - Application Security Requirements
1	**Application Architecture**
1.1	Applications hosted in a shared hosting environment should be logically isolated from other applications in the same environment
1.2	Anti-virus scanning must be performed real-time on any file transmitted to the server
1.3	All network communications between components must be authenticated, and must not explicitly trust other network devices
1.4	If an application stores highly confidential information, data must be physically separated from other applications' data stores
1.5	Applications handling highly confidential data must not be hosted in a shared hosting environment or store its data in a shared database server
1.6	If an application shares a data store with another application, the data store must be segmented logically or physically. Logical segmentation should be implemented with access control mechanisms. Physical segmentation should be accomplished with a separate instance of the data store or a separate data store server
1.7	Any administrative functions that are not meant to be accessed by users from the Internet must be located in a private DMZ, which prevents direct Internet access to the servers
1.8	Systems directly facing the Internet must not store or cache confidential data, even for a short duration. This includes file uploads and downloads, source code, etc
1.9	Internet-facing systems must be placed behind a firewall that protects against network-based denial of service attacks, blocks ports that are not required for external access, and other network attacks
1.1	Applications must not connect to a database as a privileged user, such as the SA account in SQL Server or SYSTEM account in Oracle
1.11	Applications that connect to a database, application server, or any system that utilizes application IDs must do so using an account that has been granted access to only objects and functions needed for operation of the application
1.12	All function calls between application tiers should implement digital signatures to verify authenticity of the invoking application
1.13	Applications must be designed to enforce the least privilege principle for all processes
1.14	Application server interfaces must not be accessible from the Internet. This includes Web Services, DCOM, CORBA, SOAP, EJB, RPC, and any other method of invoking remote procedure calls
1.15	All application resources must require authentication for every call to each resource, and must be kept in compliance with the recommended password policies
1.16	All servers should be kept in sync with a time synchronization mechanism
2	**Network Communication and Session Management**
2.1	Sensitive information must be transmitted via a secure channel (SSL, SSH, etc.) or encrypted prior to transmission (PGP, etc.), using KRA approved methods
2.2	All communication sessions must use secure protocols
2.3	All transactions communication sessions must enforce session expiry so that after an unacceptable period of inactivity the session must terminate to guard against session hijacking
2.4	Any vendor proprietary protocols used must be well documented (i.e. the vendor must provide comprehensive documentation on the protocols such as technical specifications or white papers). Any vendor proprietary encryption algorithms must be FIPS-140 certified
2.5	Session IDs must use strong, non -predictable algorithms

2.6	All relevant session information should be captured and stored in a secure & auditable location
2.7	Only one session should be allowed per user operating from a single computer unless a specific business case has been established for allowing multiple sessions per user
2.8	Sessions should expire after a maximum set duration, regardless of activity
2.9	Session state must be maintained on the server for web-based applications, and be associated with a single client through the use of a session ID
2.1	Session state must be tied to a specific browser session through the use of a session cookie
2.11	Sessions must not be allowed to span both secure and non-secure connections
2.12	Applications must allocate session-based resources only after successful authentication. Allocating resources prior to this can lead to denial of service attacks, session fixation attacks, and others
2.13	Synchronization of time between servers and other relevant equipment must be implemented. This is instrumental in tracking time stamps between different systems particularly where systems share/exchange data
3	**Identification and Authentication**
3.1	Each user must be authenticated with a unique user-id and password on the application
3.2	User authentication data must be stored and maintained securely in a centralized location on the system
3.3	The application must support password expiry features with a configurable frequency. Parameterize this to allow flexibility in adjusting this value as required
3.4	The password must be secure on entry, at no point must the password be in clear text
3.5	All new user accounts must have a system-generated random password when created. A secure way of communicating the initial password to the user should be utilized e.g. via KRA e-mail account
3.6	All new user accounts must be created with reference to existing authoritative databases of approved persons e.g. identifying numbers in KRA's active staff database (HR) and National PIN certificate database
3.7	Users must be prompted to change their passwords the first time they log on to the application
3.8	Newly created accounts should be set to expire if not used for a configurable period of time. Parameterize this to allow flexibility in adjusting this value as required
3.9	The application must support password lockout after a configurable number of unsuccessful attempts. Parameterize this to allow flexibility in adjusting this value as required
3.1	The application must lockout a user account after the system is idle for a configurable period of time. Parameterize this to allow flexibility in adjusting this value as required
3.11	The application must support a password change notification and a configurable number of grace logins
3.12	The application must support the ability to disable / remove / delete a user, after a number of days of inactivity, the number of days should be configurable
3.13	The application must not allow the re-use of a past password until a set number of password changes have been made. Parameterize this to allow flexibility in adjusting this value as required
3.14	The application must be flexible and enforce a minimum password length of 8 characters
3.15	The application must enforce the usage of strong alphanumeric passwords
3.16	Default / developer passwords should not reside within the application
3.17	No identification and authentication information must be hard-coded or scripted into the application
3.18	The application must provide last logon information
3.19	Backward process flows must clear all authentication fields

3.2	The application must support time-based access control
3.21	Login failure measures must not indicate which component of the username/password pair submitted was incorrect
3.22	During password changes the application must force the user to enter the new password twice
3.23	The application must support Multi Factor Authentication with at least 3 factors to choose from (OTP, TOTP, Mail)
3.24	The application should support Single Sign On at a minimum through Identity Directories for Non-Revenue systems
4	**Authorization and Access Control**
4.1	The application must support an additive access model which means by default no access is granted
4.2	Access control must be granular to facilitate adequate separation of duties, for example:
	· There should be separation of duties e.g. data entry, authorisation and final approval
	· Data entry staff should have the minimum access levels required to enter data
	· Authorisation staff should have an access level that allows them to authorise but not necessarily change the data that was entered
	· Final approval staff should have the required access level to finalise the process/transaction
4.3	Access control information should be securely stored and must be secure from unauthorized changes within and outside of the application
4.4	Reporting on all the access permissions per user must be available in the application
4.5	User must be able to explicitly terminate (logout) a session
5	**Operations**
5.1	Intrusion detection systems must be in place to detect intrusions of production systems that are Internet facing
5.2	Patch management software must be installed and regularly updated on all servers
5.3	Anti-virus software must be installed and regularly updated on all servers
5.4	A formal incidence response process plan should be in place for production systems
6	**Auditing and Monitoring**
6.1	Provision must be in place for application logs
6.2	All application logs must be in a user-friendly readable format and in English
	They should be delimited using space and allow activities to be captured per line of text Each user transaction such as printing, viewing, updates, inserts and other data manipulation should capture to the minimum the date and time, userID, the URL accessed the and source IP & remote IP. They should indicate the parameters passed where possible
6.3	All application logs must be secure from intentional or accidental modification under all circumstances by all users including administrators. Access to the logs must be restricted to authorized users only so as to ensure their integrity
6.4	It should NOT be possible for the Application Audit logs to be suppressed or modified
6.5	All logs must be viewable and printable
6.6	The application must have incident alerting capability e.g. in the event of system violations or when the audit logs are getting full
6.7	All utility or non-standard based access to the application must be captured in the logs
6.8	For all application audit logs, the log files must bear the following information:
	a) User-id

	b) Date & Time of event
	c) The source and remote IP
	d) Type of event / action performed by the user
	e) Module accessed by the user
	f) Success or failure of the event
	g) Source of the event
	h) Before and after values (where applicable, i.e. master files)
	i) Modifications to the application
	j) Account creation, lockouts, modification, or deletion
	k) Modifications of privileges and access controls
	l) Application alerts and error messages
	m) Accesses to sensitive information
	n) URL of the web page(s) accessed by a user for Internet facing applications
	o) Program used to access the system
	p) The userID at the application log should be tracked up to the database logs
6.9	The application must have a logging mechanism to log all transactions and exceptions
6.1	A violation log must exist to track any attempted unauthorized access to the application and should bear the following information:
	a) Particular action intended by the user
	b) Workstation-id or IP address of access
	c) Date & Time of event
6.11	All valid and failed login attempts must be logged with meaningful information that is actionable for investigative purposes if fraud is detected. However, passwords must not be logged
6.12	All password recovery reset attempts must be logged with meaningful information that is actionable for investigative purposes if fraud is detected
6.13	All security policy changes and attempts must be logged
6.14	All user and account management changes and attempts must be logged
6.15	Database audit trails should be present for all dynamic & static tables of interest e.g. Parameter tables, Transaction Tables etc.
6.16	Application logs should be implemented independent of database audit trails for purposes of correlation i.e. application servers should maintain their own application logs separate from database audit trails.
7	**Input – Processing – Output Controls**
7.1	Predictive input / menu based input functionality should be provided where possible, minimizing user interaction
7.2	Error messages should be standard and not provide too much application information eluding to the reason for the error allowing an attacker to deduce effective attack methods
7.3	Copy and paste must not work for data entry especially when authenticating to the application
7.4	All user input parameters must be validated by the server, and must be validated to accept only values pertinent to the values in the field in accordance with the data dictionary
7.5	Any sensitive content sent to the client machine must not be cached, unless encrypted using approved methods. The application is responsible to set the proper directive to cause the client to not cache the sensitive data
7.6	Sensitive information must not be presented to unauthenticated users

7.7	Sensitive information must not be stored in a persistent cookie, or other location on the client computer that does not have enforceable access control mechanisms.
7.8	Highly confidential data must be stored encrypted
7.9	Confidential data that is stored outside the systems that comprise the application must be encrypted by a firm approved method, such as PGP. This includes file shares, ftp servers, and e-mail
7.1	Functions should not be allowed execute on both encrypted and non-encrypted connections. If functions are required to exist on both encrypted and non-encrypted connections, then the user sessions must not be allowed to span both connections
7.11	Sensitive information must not be stored in hidden fields if the application is web-based
7.12	If data is supplied to the application from an authoritative source, the application must not allow users to modify this data
7.13	The application must not use a credential repository of a trust level less than what is required by the application's data
7.14	User credentials in one repository must not be synchronized with any other repositories unless their trust levels are equal
7.15	If an application uses more than one method or credential store for authentication, all methods and stores used must be at the same trust level
7.16	Web based interfaces should use a secure method to transmit data e.g. Using the HTTP POST method instead of the less secure GET method
8	**Cryptographic Key Management**
8.1	Cryptographic functions must be selected from an approved list. Any cryptographic functions used that are not previously approved require an exception
	Recommended algorithms (with minimum bit lengths), in order of preference, are:
	a) Hashing: SHA -512, SHA -256, RIPEMD160.
	b) Symmetric: AES256, AES192, AES128, 3 -DES (168 bits), Blowfish(minimum 128 bits), Twofish (minimum 128 bits), IDEA (128 bits),and RC4 (128 its).
	c) Public key: RSA(minimum 2048 bits) and DSA(minimum 2048 bits), ElGamal (minimum 2048 bits)
8.2	Any use of hashing must be salted. Values used for salting must be protected
8.3	Encryption keys must be protected during transit and while stored in file system
8.4	Encryption keys must not be disclosed to anyone who does not need access to them
8.5	If using public key cryptography, private keys must be protected by a pass-phrase
8.6	Pass-phrases protecting private keys or used as a share d secret with a symmetric key algorithm must be a minimum of 14 characters in length, and contain at least one upper case letter, one lower case letter, and one number
8.7	A key used to decrypt data must not be stored in the same location as data encrypted with the key
8.8	Site certificates must be current and issued by a well-known certificate authority
9	**Documentation**
9.1	A user manual should be developed as part of the application system/module/component documentation
9.2	A technical manual should be developed as part of the application system/module/component documentation
9.3	An online help facility should be present wherever possible and form part of the application system/module/component documentation
9.4	Signed user requirements/specifications document should be present as it forms the basis for the development of a new application or modification of an existing system

9.5	A Data dictionary should be developed as part of the application system/module/component documentation
9.6	A design blue print with data flow or flow chart diagrams should be present as part of the application system/module/component documentation
10	**Other Considerations**
10.1	A facility should exist to allow rolling-back of transactions/actions under special circumstances clearly documented in the user-specifications. There must be audit trail on the roll-back facility
10.2	Applications should be configurable to securely send audit data/Logs to a centralized data store that is external to the Application Server
10.3	Applications should reliably verify a user's identity using defined multi factor authentication techniques, and capable of secure communication with an external KRA E-directory service for centralized management of authorization and authentication of users to access functionality using security groups defined within the directory service
10.4	Applications should support service monitoring by logging all information that is required for effective monitoring of services based on defined service monitoring parameters
10.5	Applications should have a provision for incorporation of biometrics and related biometric solutions. The next generation of application security would be dependent on biometric identification, authorization and authentication of application users.
10.6	Security for People with Disabilities. Design of Applications should have considerations for people living with disabilities. Varied disabilities calls for design of elaborate mechanisms to enable these group of people to amicably, adequately and elaborately interact with applications. For instance, braille enhanced applications would aid the blind in interacting and using the applications in their endeavors.
10.7	The application should inco-operate certified and legitimate digital certificates, which are used to verify that a particular public key (online identity). A PKI is a technical infrastructure that comprises of a Root Certification Authority (RCA) and a Certification Authority (CA), referred to as an Electronic Certification Service Provider (E-CSP) in Kenya's legal and regulatory framework. The generation and usage of the PKIs on an application should be provisioned by the National Public Key Infrastructure for global trust and recognition.
10.8	Personal Identification data(Information) is to be kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected; and. Personal data shall not be transferred or shared outside the application unless there is proof of adequate data protection safeguards or consent from the data subject. The guidelines for this subject matter are provided by the Kenya Cyber Security Act on Personal Identifiable Information (PII).Ensure the rules of data integrity, confidentiality and availability are adequately adhered to.