KENYA REVENUE AUTHORITY

ISO 9001:2015 CERTIFIED

TERMS OF REFERENCE FOR LEGAL SERVICES MANAGEMENT SYSTEM

Contents

1) Executive Summary

This document proposes the implementation of an AI- and API-driven platform for the transformation of Legal and Board Services (L&BS), including key processes such as Litigation, Legal Research, Alternative Dispute Resolution (ADR), Independent Review of Objections (IRO), Tax Dispute Resolution (TRU), Registry, Conveyancing, and Board Affairs.

The platform will automate manual processes, introduce AI-driven drafting & classification and ensure legal matter visibility from initiation at audit stage to closure at appeal and post appeal stage.

2) Background

The Legal Services Management System (LSMS) aims to implement a set of tools that will facilitate automation of current manual processes within the Legal and Board Services Department that include: Preparation/review of legal documents, Board papers and instruments (agreements/contracts, Service Level Agreements, leases and memoranda of understanding etc.), provision of legal opinions, compliance with statutory requirements within its mandate area, legal matters/ Documents Management (storage, retrieval and archival) and reporting, analysis of data & information.

Automating the legal department of the KRA will enhance efficiency, reduce costs, and strengthen compliance by eliminating manual processes and leveraging AI-powered legal assistants. Automation will streamline tax dispute resolution, legal matters management, contract review, and compliance tracking of a matter from audit stage to close at appeal as well as post appeal processes, enabling all stakeholders to focus on high-value tasks rather than administrative burdens. AI-powered tools will provide intelligent legal research, predictive analytics, and automated document review, reducing errors and accelerating decision-making. This will improve risk management, enhance collaboration with other departments, and scale legal operations without significantly increasing costs.

Ultimately, legal automation ensures faster legal case resolution, better regulatory compliance, and a competitive edge in managing tax-related legal complexities efficiently.

Additionally, automating KRA's legal process will enable the generation of smart reports that provide real-time insights and updates into KRA core business, provide litigation trends, tax dispute resolution efficiency, and compliance risks. AI-driven analytics can identify patterns in tax-related cases, detect potential revenue leakages, and assess the effectiveness of various dispute resolution mechanisms. These reports support data-driven decision-making, allowing legal teams and relevant stakeholders to proactively address tax compliance risks, streamline enforcement actions, and improve policy recommendations.

By integrating automation and AI, KRA will enhance the speed and efficiency in decision making as well as providing an ability to detect correlations that may be undetectable by the human brain and ensuring that decisions are more systematic, consistent and coherent. It will enhance transparency, optimize legal workflows, and ensure more effective enforcement of tax laws while maintaining accuracy, accountability, and efficiency in tax dispute management.

3) Objectives

The main reason for undertaking this project is to come up with a Legal services management system whose fundamental purpose is to enhance efficiency in the Legal Services process in KRA. The system is expected to have friendly and Intelligent interactive capabilities that aim to eliminate redundant processes, automate manual and semi-manual processes. Besides, the system shall address performance challenges as well as security gaps identified in the current system/subsystems.

On successful implementation of this project, the L&BS Department will improve on efficiency in its mandate in terms of the following:

3.1 Intelligent legal matters & Customizable Workflow Automation

Implement smart workflow automation that dynamically assigns matters eg legal matters, tracks progress, and escalates matters based on urgency, risk levels, and regulatory deadlines, ensuring efficiency and compliance.

3.2 Predictive Analytics & Smart Reporting

Deploy AI-powered predictive analytics to anticipate litigation risks, compliance gaps, and dispute resolution outcomes, while offering customizable, real-time smart reports for data-driven decision-making.

3.3 Knowledge-Driven Legal Advisory

Develop a centralized AI-enhanced knowledge base that intelligently retrieves relevant legal precedents, advisory opinions, and regulatory updates, empowering KRA staff with instant, data-backed legal advisory as well as judgement analysis.

3.4 Seamless System Integration

Achieve real-time interoperability with other KRA's systems to ensure end to end visibility of Taxpayers information and to ensure monitoring of Compliance & Enforcement of legal matter outcomes and contracts eliminating data silos.

4) Scope of Work

4.1 Modules

The project scope covers the implementation of a Legal Services Management System covering legal and Board business processes and categorized as follows into the following modules:

4.1.1 Document Management and Registry Automation Module

To provide an automated process that allows for maintenance (recording, retrieval, storage and archival) of all legal documents.

Among the deliverables in this module would include but not limited to the following:

i. Automated allocation of files to teams based on metrics such as Nature of Dispute, Amount of tax disputed, tax obligation disputed, complexity of issues and the clients departments.
ii. Retention and Disposal Schedule (File Life Cycle: Opening/Referencing/Appraising and Closing of Files) – To avoid duplication of file references/different files with the same reference number and recommend files to be closed.
iii. Document Storage & Organization – Secure digital repository for storing legal documents, contracts, and case files.
iv. Version Control & Tracking – Maintains document history, allowing rollback to previous versions.
v. Access Control & Permissions – Role-based access for users to ensure security and compliance.
vi. Document Indexing & Tagging – Enables quick searching using metadata, keywords, or categories.
vii. Audit Trail & Activity Logs – Tracks who accessed, edited, or shared a document for accountability.
viii. Automated Workflow & Approvals – Supports review, approvals, and signing processes.
ix. File Requisition/Retrieval – Online request of files.
x. File Tracking – To include the officer with the file and the maximum number of days an officer should have the file.
xi. Bring Up (BU) Tracking – To facilitate tracking of active documents/correspondences on a real-time basis. This will enable the Department monitor and get to know the status of each document at any given time in line with the statutory and internal standards regulations.
xii. Inventory - List of all documents and files.

xiii. Archival – To provide a mechanism for archival of documents based on a set of rules and standards to the statutory and internal standards.

4.1.2 Repository Module

It is envisioned that this module shall provide a repository for statutes, regulations, guidelines, legal precedents, case laws, advisory opinions, tax regulations, policy interpretations and informative articles. The Module will have all the statutes and should be able to reflect any amendments made to the statutes. The System should be able to intelligently feed the repository module.

The system should support AI-powered search and categorization, allowing users to retrieve relevant information based on keywords, case types, or legal issues. Additionally, it should include automated updates and notifications, ensuring that changes in tax laws, court rulings, and regulatory amendments are reflected in real time. A version-controlled document management system should track updates, maintaining a clear history of modifications.

4.1.3 Conveyance Module

The Conveyance module should seamlessly integrate with KRA's Enterprise Resource Planning (ERP), Supply Chain Module to facilitate the efficient review of draft contracts by the legal team. This integration should enable automated contract routing, allowing procurement-related agreements, leases, and asset transfer documents to be directly accessible within the Legal and Board Department's Legal Services Management System.

By linking with the ERP, supply chain module the legal team can receive real-time notifications when new contracts require review, track contract amendments, and provide legal input before final approval. The system should also support version control, audit trails, and automated approval workflows, ensuring that contract negotiations align with legal and regulatory requirements. Additionally, AI-powered contract analysis can identify potential risks, flag non-compliant clauses,

and suggest standard legal provisions, improving accuracy and reducing review time.

4.1.4 Legal Opinions and Advisory Module

The Legal Opinions and Advisory Module should be designed to streamline the provision of legal guidance within KRA by enabling efficient request submission, tracking, and response management for legal opinions on tax laws, regulatory compliance, and policy matters.

It should support automated workflows, allowing different departments to submit legal opinion requests electronically, track their progress, and receive responses within predefined timelines.

Additionally, the module should incorporate AI-powered legal research tools that analyze tax laws, court rulings, and past legal opinions to provide data-driven insights and enhance the accuracy of legal advisory services.

4.1.5 Calendar Module

The System should contain a calendar that will be used for diarizing activities and that will also be integrated with current lotus email calendar and judiciary cause list. The activities should display on the daily dashboard.

4.1.6 Rulings Portal

An open and searchable webpage that allows a view of all legal matters closed with their respective information such as (Parties Involved, Type – whether tribunal, court appeal etc., Litigating/Prosecuting Officer, Revenue/Liability Implication, Presiding Magistrate /Judge/Authority etc.).

4.1.7 Administration Module

To manage system use across the varied services and allow for configuration of parameters related to system usage for example when/who to get a notification, alerts etc.

4.1.8 Reports Module

The Reports Module should provide comprehensive, real-time analytics and reporting capabilities to support data-driven decision-making within KRA's Legal and Board Services Department. This module should generate customizable reports on key legal metrics, including legal case trends, real time legal case status, Taxpayers behaviours on disputes, tax dispute resolution efficiency, contract turnaround times, and legal advisory response times.

The system should support automated report generation, allowing legal teams to schedule and receive periodic updates on ongoing legal cases, pending legal opinions, and enforcement actions. Interactive dashboards should provide visual insights using charts, graphs, and heat maps to highlight litigation risks, legal case backlogs, and emerging tax-related legal issues.

The module should also support AI-driven analytics, enabling predictive insights into legal case outcomes, compliance trends, and areas of potential legal exposure. Additionally, reports should be exportable in multiple formats (PDF, Excel, CSV) for ease of sharing with senior management, policymakers, and other stakeholders. This ensures transparency, accountability, and continuous improvement in legal service delivery within KRA.

4.1.9 Board Services

The Board Services module should facilitate the centralized receipt, logging, categorization, tracking, and dispatch of all Board and Committee meetings documents in real time, while supporting the secure storage, retrieval, and

archiving of Board papers, minutes, statutory records, resolutions, and legal instruments. The module must provide comprehensive action-tracking capabilities to monitor progress and ensure closure of tasks arising from Board and Committee resolutions. It should also support the secure custody, sealing, and verification of statutory records and legal documents in full compliance with governance and legal requirements, ensuring the integrity, traceability, and security of corporate registers and legal instruments.

The solution should enable digital or automated tracking of sealing requests, approvals, and audit trails to promote accountability and process transparency. Additionally, the module should provide tools to support end-to-end meeting management, including agenda preparation, approval workflows, document circulation, meeting scheduling, logistics planning, digital meeting pack generation, and structured dissemination of meeting materials.

It must further support accurate recording of minutes, comprehensive follow-up of Board resolutions, and continuous monitoring of pending action items. To uphold regulatory compliance, the module should support alignment with national governance frameworks and requirements issued by bodies such as the State Corporations Advisory Committee (SCAC), the National Treasury, and the Office of the Attorney-General. It should also enable seamless integration of governance data with internal KRA systems and relevant external oversight entities. Finally, the solution must provide capabilities for generating compliance reports, statutory updates, governance summaries, and audit-ready documentation to enhance transparency, accountability, and informed decision-making within the Authority.

5 Integrations

The System should integrate with the following KRA's internal systems, in order to enhance data sharing between the various stakeholders:

i. KRA Customs Systems
ii. KRA Tax Systems
iii. Enterprise case/workflow management solution
iv. Document Management System
v. ERP Supply Chain Module
vi. Mail Server
vii. SMS Gateway
viii. Active Directory
ix. Any other applicable system

The System should integrate with the following external systems, in order to enhance data sharing between the various stakeholders:

i. Judiciary e-Filing System
ii. Kenya Law Reports
iii. Business Registration Service (BRS) System
iv. Lands registry System
v. Any other relevant systems

6 Documentations and Non – functional requirements

The project scope includes provision of project documentations and Non-functional requirements falling under the following broad categories

i. Training manuals

ii. System installation manuals

iii. Technical manuals and documentations

6.1 Non-functional requirements

i. Platform Compatibility (Access of the system via Mobile Platform)

ii. Standardized Look and Feel

iii. Standardized and specific error messages

iv. Browser Compatibility

v. Acceptable response time for different operations with low latencies.

7 Expected Results (Deliverables)

On successful implementation of this project, the L&BS Department will improve on efficiency in its mandate. A key outcome will be data-driven decision-making through real-time smart reports that provide insights into litigation trends, enforcement efficiency, and compliance risks.

AI-powered analytics will help anticipate legal challenges, optimize resource allocation, and improve policy recommendations. Additionally, the system will enhance transparency and accountability with digitized records, automated notifications, and audit trails while reducing operational costs by minimizing manual legal work and external legal expenses. Ultimately, it will transform KRA's legal operations into a more efficient, technology-driven, and strategically informed function.

8 Time frame

The vendor is required to provide the estimated timelines for both the system and support

9 Detailed Specification/Requirements

Include requirement for maintenance and support/licences

TABLE 1: MANDATORY TECHNICAL REQUIREMENTS.

Note: Bidders MUST COMPLY WITH ALL THE MANDATORY requirements in TABLE 1 (Below) in order to be considered for further evaluation.

Instructions to Bidders:

- Bidders MUST complete the Table below in the format provided.
- Bids MUST meet all mandatory (MUST) requirements in the Tables below in order to be considered for further evaluation.

- 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.
- Bidders who do not comply with any of the below requirements will NOT be considered for further evaluation

NB: Bidders who shall meet the cut-off score for the technical and demonstration requirements shall be evaluated at the financial evaluation stage.

S/No	Requirement	Mandatory Specifications	Bidders' response (Please provide a Relevant narrative response)
1	Product	The Proposed Legal and Board Services Management Solution MUST be a reputable and widely deployed international brand. ALL products, Licenses and services MUST be sourced through the authorized OEM channels. Bidders MUST ensure that ALL components of the proposed solution **ARE NOT** scheduled to reach their end of life/support within 5 years from the date of bid submission In this regard, Bidders MUST submit a Product introduction brief that includes the following details: Specific Brand, product, series, model etc. and relevant supporting brochures.	
2	Key solution Components	The proposed Legal and Board Services Management solution MUST be inclusive of the following components:	
		The system should allow authorized users to create new legal matters (Objections, litigation, contracts, ADR, etc.) by entering essential details.	

		The system should automatically classify matters based on predefined categories and assign unique reference numbers instantly upon creation.	
		The System should support Automated allocation of files to teams based on metrics such as Nature of Dispute, Amount of tax disputed, tax obligation disputed, complexity of issues and the client's departments.	
		The system should integrated with other KRA core systems to support end-to-end legal matter/case tracking, from initiation at audit stage to closure at appeal stage and post appeal stage. This to be visible to all relevant stakeholders.	
		Must provide automated workflows for legal matter/case allocation, status updates, and resolution tracking.	
		Should allow secure document management, including version control, access logs, Document Indexing & Tagging and Automated Workflow & Approvals.	
		1.2 Contract & Conveyance Management	
		Should integrate with the KRA's ERP Supply Chain Module to enable real-time legal review of procurement contracts and conveyance documents.	
		Should have AI-powered contract analysis to flag potential risks and ensure compliance.	
		Must provide automated alerts for contract renewals and milestone tracking.	
		Must allow electronic submission, tracking, and management of legal opinion requests.	
		Should provide AI-powered legal research capabilities, leveraging historical case laws and advisory opinions.	

		The system should integrated with other KRA core systems including an enterprise case/workflow management solution to support end-to-end tracking, of legal opinions and must include a centralized repository for easy retrieval and reference of past legal opinions.	
		Should generate real-time, customizable reports on legal case trends, tax disputes, contract reviews, and legal case outcomes.	
		Must support AI-driven predictive analytics to identify potential litigation risks and dispute patterns.	
		Should allow data export in multiple formats (PDF, Excel, CSV) and automated scheduling of reports.	
		Should provide interactive customizable dashboards for legal performance insights.	
		Must have a centralized repository for storing legal case precedents, legal interpretations, and tax law updates.	
		Should support full-text search, document categorization, and AI-powered recommendations.	
		Must allow secure document sharing, annotations, and archiving.	
		1.6 Board Services	
		Must facilitate the centralized receipt, preparation categorization, tracking, and dispatch of all Board and Committee meetings documents in real time.	

		Must ensure that recording sessions can only be started or stopped by users with the appropriate access rights.		
		Must automatically encrypt all audio recordings during capture, storage, and transmission.		
		Must securely store all completed recordings in an encrypted repository.		
		Must provide a secure portal through which only authorized transcribers can access recorded files.		
		Must include an embedded AI transcription engine for automatic transcript generation.		
		Data Encryption	All data, both at rest and in transit, must be encrypted using industry-standard encryption algorithms to prevent unauthorized access. Any vendor proprietary encryption algorithm must be FIPS-140 certified.	
		Access Control	The system must implement robust access control mechanisms, including multi-factor authentication, role-based access controls, and the principle of least privilege.	

		Auditing and Logging	Comprehensive audit trails must be maintained for all system activities, enabling traceability and accountability. Ensure the logs are in a format that is consumable by Security information and event management (SIEM) system.	
		Incident Response	An effective incident response plan must be established by the vendor to address security breaches or incidents promptly and minimize impact.	
		Data Integrity	Mechanisms must be in place to ensure the integrity of data, including checksums, digital signatures, and blockchain technology where applicable.	
		Continuous Monitoring	The system must have continuous monitoring capabilities to detect and respond to security threats in real-time.	
		Security Training	Vendors must provide security training for system users and administrators to	

			foster a culture of security awareness.	
		Secure Development	" The solution must be developed following secure coding practices, and vendors must demonstrate a commitment to security throughout the software development lifecycle.	
		Authentication	No identification and authentication information must be hard-coded or scripted into the application.	
		Compliance to Detailed KRA Security Requirements	The solution must be implemented in compliance with the detailed KRA Application Security requirements (Annex I) and API Security requirements (Annex II). The detailed requirements will form part of the Information Security testcases.	
		The system must be web-based, accessible via on-premise deployment.		
		Should support API integrations for seamless data exchange with ERP Supply chain Module, KRA Tax Systems and Customs Systems, case/workflow management system, document management system		

		as well as Judiciary System Business Registration Service System, lands registry system and all other applicable systems.	
		Must be scalable to accommodate increased caseloads and user demands.	
		The solution must be deployable both on-premises and in a cloud-ready architecture.	
		2.2 User Access & Interface	
		Should support role-based user management for different levels of access.	
		Must have a user-friendly and intelligent interface accessible via web browsers and mobile devices.	
		The vendor must provide ongoing technical support, including user training, software updates, and 24/7 helpdesk services.	
		Must include detailed system documentation, covering API integration and user guides.	
		Should have a Service Level Agreement (SLA) with clear response times for issue resolution.	
3	Hardware and Software Requirements	The proposed solution MUST be based on dedicated OEM Hardware and/or software appliances deployed in High Availability (HA) across Data Center(s) (Primary, Secondary and DR). The hardware appliance must be rack-mountable in standard 42U Rack.	
4	Training and capacity building	Successful bidder MUST provide Manufacturer Authorized administrator training (classroom) for hundred (100) KRA staff, leading to professional certification in the solution. Training proposals MUST include Course outline to be covered and duration.	

5	Vendor Support	Successful bidder MUST provide Unlimited Vendor onsite and online Implementation, Maintenance and Support Services covering the entire solution throughout the contract period on a 24*7*365 Basis. The vendor's staff providing support MUST have attained relevant OEM certifications. Bidder MUST demonstrate competence in delivering the solution by having acquired a high product partnership level with the OEM. The successful bidder MUST also be backed by professional technical support from the OEM throughout the contract period. In this regard, Bidders MUST provide a letter from the OEM certifying the partnership Levels and commitment from the OEM referencing this tender and indicating OEM's willingness to provide oversight and support through the contract period.	
6	Licensing	The bidder is required to state the licensing model used by the product and other related licenses required by the product.	
7	OEM Support & Local Presence	KRA runs mission critical services on a 24*7*365 basis. In order to guarantee availability of OEM online and onsite support on a 24*7*365 basis, OEMs for quoted products are required to have Local presence in Kenya and MUST have qualified technical staff with relevant professional training, experience and certifications in the implementation and support of the solution. Bidders MUST provide details of the Local office including location and staffing. Successful bidder MUST ensure that ALL products (Hardware, Equipment, interfaces, accessories, Software and Services) MUST be covered under OEM technical support services throughout the contract period, including direct access to	

		Manufacturer's technical assistance team, online troubleshooting / support tools.	
Remarks: Complied / Not Complied. Bidders who do not comply with any of the above requirements will NOT be considered for further evaluation			

TABLE 2: MINIMUM TECHNICAL AND IMPLEMENTATION REQUIREMENTS

Note: Bidders MUST attain a minimum of 80% score in TABLE 3 (below) in order to be considered for further evaluation.

S/No	Feature	Minimum Specification	Max Score	Bidder Response (Narrative answers)
	Legal Services			
1	**Key Legal Services Features**	The system should allow authorized users to create new legal matters (Objections, litigation, contracts, ADR, etc.) by entering essential details.	2	
		The system should automatically classify matters based on predefined categories and assign unique reference numbers instantly upon creation.	3	
		The System should support Automated allocation of files to teams based on metrics such as Nature of Dispute, Amount of tax disputed, tax obligation disputed, complexity of issues and the clients departments.	2	
		The solution should support end-to-end legal matter/case tracking, from initiation to closure.	2	
		The solution should provide automated workflows for legal matter/case allocation, status updates, and resolution tracking.	3	

		The solution should allow secure document management, including version control, access logs, Document Indexing & Tagging and Automated Workflow & Approvals.	3	
		The solution should support real-time notifications and alerts for legal matter/ case deadlines, updates, and approvals	1	
		The solution should provide automated alerts for contract renewals and milestone tracking.	1	
		The solution should have AI-powered contract analysis to flag potential risks and ensure compliance.	3	
		The Solution should support Legal Document Templates – Standardized formats for contracts, legal opinions, and legal case documents.	1	
		The solution should allow electronic submission, tracking, and management of legal opinion requests.	2	
		The solution should provide AI-powered legal research capabilities, leveraging historical case laws and advisory opinions.	4	
		The solution should include secure data migration from the existing legal and related systems to the new system.	4	
		The solution should generate real-time, customizable reports on legal case trends, tax disputes, contract reviews, and legal case outcomes.	2	
		The solution should support AI-driven predictive analytics to identify potential litigation risks and dispute patterns.	4	
		The solution should allow data export in multiple formats (PDF, Excel, CSV) and automated scheduling of reports.	2	
		The solution should provide interactive dashboards for legal performance insights.	2	
		The solution should have a centralized repository for storing legal case precedents, legal interpretations, and tax law updates.	1	

		The solution should support full-text search, document categorization, and AI-powered recommendations.	3	
		The solution should allow secure document sharing, annotations, and archiving.	2	
		The solution should integrate with all relevant KRA applications including the core tax and customs systems, Case/workflow management system, document management system and ERP, supply chain module. This is for both KRA internal users and select external users.	5	
Board Service Services				
2.	**Key Board Services Features**	The solution should allow only authorized users to securely log in before initiating any recording session.	1	
		The solution should ensure that recording sessions can only be started or stopped by users with the appropriate access rights.	2	
		The solution should automatically encrypt all audio recordings during capture, storage, and transmission.	3	
		The solution should securely store all completed recordings in an encrypted repository.	2	
		The solution should provide a secure portal through which only authorized transcribers can access recorded files.	2	
		The solution should include an embedded AI transcription engine for automatic transcript generation.	2	
		The solution should allow transcribers to review, edit, refine, and approve transcripts within the system.	2	
		The solution should maintain a comprehensive audit trail capturing all user activity for compliance and governance purposes.	1	
		The solution should restrict export, download, or external transfer of transcripts to only those users with explicit authorization.	1	

		The solution should ensure that transcripts can be reviewed and approved in a controlled, secure workflow environment.	2	
		The solution should provide AI-assisted capabilities including tagging, summarization, keyword extraction,	1	
		The solution should provide secure playback, pause, navigation, and editing tools for transcription workflows.	1	
		The solution should support multi-language transcription, including legal terminology enhancements and domain-specific lexicons.	1	
		The solution should restrict access to transcription functionality to users with defined "Transcription Rights" under role-based access control (RBAC).	2	
		The solution should provide capability for secure storage including use of modern technologies for document storage such as Blockchain Technology, document versioning, and archiving of transcripts and associated metadata.	3	
		Integrations		
3	**Integrations**	The solution should integrate and authenticate Active Directory user identities.	2	
		The solution should support the creation, import and export of bulk users using CSV files or any other mechanism where applicable.	2	
		The solution should support Virtualized Environment Setup (VMware or Hyper-V).	2	
		The solution should integrate with all relevant KRA applications to ensure visibility of case tracking from initiation at audit stage to closure at appeal stage and post appeal stage.	2	
		The solution should integrate with SMS gateway for token delivery.	2	
		The solution should integrate with SIEM solution.	2	
		The solution should use SSL certificates/Encryption techniques to secure communication.	2	

		The solution should support the following standards Security Assertion Markup Language (SAML) System for Cross-domain Identity Management (SCIM) OAuth 2.0 OpenID Connect	2	
Implementation Overview				
4	**Implementation Overview**	The bidder **MUST** provide an implementation approach including a complete process overview and architecture designs showing the interrelation of all the components of the integrated solution to be implemented. This should include an implementation approach and schedule.	2	
		Successful bidder is required to: Review the existing Business process model for the purpose of developing a desired model, while meeting the KRA legal and board services management objectives and best practice. Design an enterprise legal services Management solution architecture that addresses the needs of both the existing and future models of operations. Lead the implementation of the designed architecture that meets the KRA requirements and the requirements of this bid Work closely with stakeholders to ensure that risks are collected, prioritized, and mitigated throughout the life cycle of the project. Lead the implementation of legal and Board services Management Solution and build capacity in the KRA internal team to competently implement and maintain the solution Hand hold KRA internal implementation team in maintenance and support of the Solution on a need basis.	2	
Warranty				
	Warranty	Should be supplied with a minimum warranty of 18 Months from the date of Inspection and acceptance	2	
TOTAL MARKS			100	

Total score for Technical Requirements		
NB The pass mark shall be 80% of the Key Legal and Board Services solution features (item 1 and 2) and 80% of the rest of the features (item 3 and 4).		

TABLE 3: SOLUTION DEMONSTRATION

	Requirement	**Score**	**Bidders Response**
Solution Demonstration	Bidders will be required to demonstrate their proposed solution, showcasing its functionality and compliance with the RFP requirements. The demonstration should provide a clear and practical illustration of the solution's capabilities in regards to the key solution features as specified in the technical and functional requirements.	10	
TOTAL MARKS		10	
Total score for Solution Evaluation			
NB The pass mark shall be 80%			

TABLE 4: VENDOR EVALUATION

Item	**Requirement**	**Evaluation Criteria**	**Max Score**	**Bidder Response (Narrative answers)**
1	**Company Experience** Demonstrated experience through Previous execution of at least one (1) legal services management solution project.	Demonstrated experience through Previous execution of at least one (1) legal and board services management solution project. In order to be awarded marks bidders MUST submit a copy of executed Contract or LSO, supported by:	5	

		A brief description of the project delivered Full contacts; address, telephone and email of customer where assignments/ projects were executed. Completion Certificate/Letter from the Customer confirming successful completion of the project.		
2	**Technical Capacity Evaluation** Minimum of three (3) Technical staff with the following academic and professional qualifications: 1)*Academic Qualifications:* A minimum of Relevant University Degree (Data Science, IT, electronics or related fields) 2)*Professional Qualifications:* Valid OEM Certification in Data Storage, Cyber Recovery or equivalent certification for the specific proposed product in a cyber-recovery solution.	4 Marks for each Qualified Staff (1 mark for degree, 3 marks for product professional qualification) **Note:** Bidders MUST attach CV of each staff supported by Academic and professional certificates in order to be scored.	12	
3	**Project/Team Lead – 7 marks** **1. Academic Qualifications:**	**1. Academic Qualifications** 2 marks	7	
		2. Professional Certifications		

	Bachelor's degree in Computer Science,Data Science, Software Engineering, or related field **2. Professional Certifications:** PMP, PRINCE2, or equivalent project management certification; ITIL or COBIT – **3. Experience:** At least 8 years in ICT project implementation, including at least 3 years managing secure digital recording, transcription, or document management solutions in large organizations. Note: Bidders MUST provide CV for each staff clearly indicating the years of experience in supporting an legal services management solution and implementation.	3 marks. 3. **Experience** 8 years and above – **2 Marks** Between 5 and 7 years – **1 Mark** Less than 5 Years – **0 Marks**		
	Software/Application Developers – 7 Marks **Academic Qualifications:** Bachelor's degree in Computer Science, Software Engineering, Data Science, or related field **Professional Certifications:** Relevant programming, database, or cloud platform certifications, AI(e.g., Microsoft, AWS, Oracle, or equivalent) **Experience:** Atleast 5 years in software development, with at	1. **Academic Qualifications** 2 marks 2. **Professional Certifications** 3 Marks 3. **Experience:** 5 years and above – 2 Marks Between 3 and 5 years – 1 Mark Less than 3 Years – 0 Marks	7	

	least 1 years in secure or compliance-critical applications. Note: Bidders MUST provide CV for each staff clearly indicating the years of experience in supporting an legal services management solution and implementation.			
4	**OEM Partnerships** Bidder should have attained Industry proven and OEM certified capacity to sell, implement, support and maintain the proposed solution. In this regard, the bidder should have acquired Tier 1 or Tier 2 Partnership Level with the OEM.	Relevant OEM Partnership Tier 1 (or equivalent) Partnership - 5 Marks Tier 2 (or equivalent) Partnership – 3 Marks Note: Bidders MUST attach copies of partnership certification or a letter from the OEM indicating his partnership Level.	5	
5	Technical Approach/Methodology	Bidders to demonstrate/provide evidence of a clear and detailed understanding of the solution, including: Project delivery Approach and Methodology for implementation and support of the solution – 3 Marks Work plan (Bidder MUST provide a three (3) year work plan Implementation and support for the solution –2 Marks	5	
6	Proposed Design & Architecture of the Solution.	Bidders MUST submit a proposed design and architecture for the solution demonstrating how they propose to deploy the solution/appliances in both the Primary and Secondary, and	4	

		Disaster Recovery Data Centres, including High Availability (HA) Configuration		
	TOTAL MARKS		45	
Cut Off			36	
NB The pass mark shall be 80% of the vendor evaluation				

FINANCIAL REQUIREMENT

• N/B: Bidders to provide a detailed 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

TABLE 6: OVERALL TENDER EVALUATION CRITERIA

No	Criteria	Maximum Score:	Weight	Cut-Off Score
1	Mandatory Technical Requirements.	Mandatory	P/F	All Mandatory
2	Minimum Technical and Implementation Requirements	100	75%	80
3	Solution Demonstration	10	5%	8
4	Vendor Evaluation	45	20%	36
5	Financial Evaluation	Award to the lowest evaluated bidder.		

	ANNEX I - API Security Requirements
	Review Area
1	**Governance**
1.1	Ensure the API is properly versioned. Versioning helps in keeping track and maintenance of the API.
1.2	Ensure that the API conforms to the organization 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:
	a)	Use a random complicated key (JWT Secret) to make brute forcing the token very hard.
	b)	Don't extract the algorithm from the header. Force the algorithm in the backend (HS256 or RS256).
	c)	Make token expiration (TTL, RTTL) as short as possible.
	d)	Don't store sensitive data in the JWT payload, it can be decoded easily."
2.7		"When OAuth 2.0, ensure:
	a)	Always validate redirect Uri server-side to allow only whitelisted URLs.
	b)	Always try to exchange for code and not tokens (don't allow response type=token).
	c)	Use state parameter with a random hash to prevent CSRF on the OAuth authentication process.
	d)	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 integrating components only access the objects they require from the integrating systems. Responses should only return the data necessary to fulfil a request.
4		**Data Protection**
4.1		Ensure that the responses from the API provide only legitimate 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.

	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, user ID, 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 user ID 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 endeavours.
10.7	The application should incooperate 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.