KENYA REVENUE AUTHORITY

ISO 9001:2015 CERTIFIED

TERMS OF REFERENCE FOR THE ENTERPRISE DOCUMENT MANAGEMENT SYSTEM

Executive Summary

This document proposes the implementation of an enterprise-wide Document Management System (DMS) for the Kenya Revenue Authority (KRA). The current document management practices remain partly manual, with records stored across fragmented and siloed repositories. This decentralized approach presents several challenges, including limited audit trails on document movement, duplication of taxpayer audits, inefficiencies in accessing information, and the burden placed on taxpayers who must repeatedly submit the same documents to different KRA units. These gaps reduce operational effectiveness, hinder decision-making, and increase the risk of revenue leakage.

To address these challenges, KRA seeks to deploy a centralized, secure, and compliant DMS that will support the full lifecycle management of records across all business units. The proposed solution will incorporate Business Process Reengineering (BPR) principles, ensuring that the Authority not only digitizes existing processes but also transforms documentation workflows into strategic assets. The DMS will enhance efficiency, strengthen auditability, improve traceability of taxpayer information, and reinforce stakeholder confidence in KRA's operational integrity.

Background

The Kenya Revenue Authority (KRA) manages extensive volumes of operational, compliance, and taxpayer-related documents that are essential for accurate revenue administration and informed decision-making. However, much of this information is currently dispersed across manual files, isolated repositories, and unstructured digital platforms, limiting visibility, slowing service delivery, and constraining the Authority's ability to enforce compliance efficiently.

To address these challenges and align with KRA's digital transformation agenda, the Authority proposes the implementation of an enterprise-wide Document Management System (DMS). The solution will establish a centralized, secure, and compliant platform for capturing, organizing, and managing corporate records. Beyond digitizing existing processes, the DMS will lay the foundation for the adoption of modern, AI-enabled capabilities such as intelligent document classification, automated metadata extraction, predictive analytics, and workflow optimization. These features will support faster decision-making, improve accuracy in taxpayer engagements, and strengthen compliance monitoring.

By integrating the DMS with core revenue systems, KRA will transform documents into actionable data streams that directly support revenue assurance—reducing duplication of effort, minimizing disputes arising from inconsistent records, and improving traceability across audit, legal, and enforcement functions. The platform will also enhance collaboration between departments, support statutory and governance requirements, and safeguard institutional memory through structured information management.

Objectives

The key objectives of the DMS solution are to:

1. **Centralize and Secure Document Management**
   Provide a unified repository for all corporate and taxpayer-related documents to enhance accessibility, security, and compliance.
2. **Automate and Streamline Workflows**
   Digitize and standardize document-centric processes to improve turnaround times, reduce manual errors, and enhance service efficiency.
3. **Enable AI-Driven Capabilities**
   Establish an AI-ready platform that supports intelligent document classification, data extraction, advanced search, and predictive analytics for improved operational insights.

4. **Enhance Revenue Assurance**
   Improve document traceability and accuracy across compliance, audit, enforcement, and legal processes to reduce revenue leakages and strengthen oversight.
5. **Support Informed Decision-Making**
   Convert unstructured documents into actionable data that supports analytics, forecasting, and performance reporting.
6. **Improve Interdepartmental Collaboration**
   Facilitate seamless sharing of records across business units to eliminate duplication and support integrated case and taxpayer management.
7. **Strengthen Governance and Institutional Memory**
   Ensure compliance with statutory and regulatory requirements while preserving historical records for organizational continuity.

Key Deliverables

MVP Deliverable	Description (What It Must Include)
Core Document Repository & Search Functionality	• Central document storage • Document indexing, metadata & tagging • Version control & audit trails • Templates & naming conventions • Advanced search & filtering • Check-in/check-out features
Workflow Automation for Document Processes	• Automated review & approval workflows • Routing rules & notifications • Deadline triggers & alerts • Escalation paths for delayed processes • Digital approval tracking
Security, Access Control & Compliance Tracking	• Role-based access control (RBAC) • Authentication (SSO/MFA) • Encryption at rest & in transit • Audit logs for all document actions • Compliance rule enforcement
Integration with Email & Key Enterprise Systems	• Email capture • Integration with ERP, Tax, Customs, Legal systems • REST/SOAP API connectors • Centralized authentication with AD

Expected Benefits

The implementation of the Document Management System (DMS) is expected to deliver significant operational, compliance, and strategic benefits to the Authority. The solution will improve efficiency by digitizing and automating document workflows, leading to faster turnaround times, reduced manual errors, and lower processing overheads. Centralized storage will enhance accessibility, ensure secure information sharing, and eliminate duplication of documents across departments.

The AI-ready capabilities of the DMS will enable intelligent classification, automated data extraction, and advanced search tools, improving accuracy and enabling timely decision-making. The system will strengthen auditability and compliance by providing reliable document trails, standardized governance controls, and adherence to statutory retention requirements. Enhanced document traceability across audit, enforcement, compliance, and legal processes will help reduce revenue leakages and support timely follow-up on taxpayer matters. The platform will also improve collaboration between departments, preserve institutional memory, and support knowledge continuity.

Scope of Work

The project scope covers the implementation of a modern DMS as detailed below:

Scope Area / Module	Description	Expected Activities / Deliverables
DMS Platform Deployment	Provision and setup of the enterprise-wide Document Management System.	• Supply, installation, and configuration of the DMS platform. • Setup of repository structures, taxonomies, metadata, and retention rules. • Configuration of user roles, permissions, and security policies.

Core Document Repository	Central storage for capturing, indexing, storing, and retrieving documents.	• Define document categories, templates, and naming conventions as per KRA guidelines. • Configure advanced search and filtering capabilities. • Setup automated version control, audit trails, and check-in/check-out features.
Workflow Automation Module	Automated workflows for document creation, review, approval, and archival.	• Map existing manual workflows and redesign them for automation. • Implement approval routing, deadline triggers, and notifications. • Enable escalation paths for time-sensitive processes.
AI-Enabled Document Intelligence	Intelligent automation and analytics to enhance document processing.	• Implement OCR •Intelligent capture, and auto-classification. • Configure AI for metadata extraction and document tagging. • Set up predictive analytics dashboards for compliance and audit functions.
Integration with Enterprise Systems	Seamless interoperability with existing KRA systems.	• Integrate with ERP,Tax systems, AD,Customs Systems,Legal systems • Implement REST/SOAP APIs for data exchange. • Enable SSO and centralized authentication.
Email & Communication Integration	Automated capture of emails and attachments into the DMS.	• Configure email ingestion rules. • Enable capture of correspondences from Lotus or other mail systems.
Records Management & Archival Module	Policy-driven document lifecycle management.	• Setup retention schedules and disposal policies. • Configure automated archival workflows.

		• Implement long-term preservation formats (e.g., PDF/A).
Collaboration & Sharing Module	Secure document sharing and controlled access.	• Configure internal and external sharing controls. • Enable secure links, document commenting, and co-authoring (if applicable).
Audit & Compliance Module	Ensure traceability, accountability, and regulatory adherence.	• Configure audit logs and reporting features. • Implement compliance rules for statutory and governance requirements.
Data Migration from Legacy Repositories	Moving existing digital and manual documents into the new system.	• Assess all current repositories (shared drives, emails, departmental folders). • Digitize manual documents through scanning. • Cleanse, deduplicate, index, and tag migrated documents.
Data Transformation & Digitization	Standardizing and converting unstructured and manual documents.	• Apply OCR to scanned files. • Convert documents to standardized formats (PDF, PDF/A). • Apply metadata rules and classification structures.
Change Management & Capacity Building	Training and support to ensure effective adoption.	• Conduct user training, admin training, and system handover. • Develop user manuals, SOPs, and training materials. • Provide change management support and awareness campaigns.
Reporting & Insights Dashboard	Real-time visibility on document operations.	• Build dashboards for workflow status, turnaround times, archive usage, and audit trails. • Enable AI-driven insights for compliance and process optimization.

Security, Access Control & Encryption	Ensure information confidentiality and system integrity.	• Implement encryption at rest and in transit. • Configure RBAC, MFA, and SSO. • Conduct vulnerability assessment and penetration testing.
System Testing & Quality Assurance	Ensuring reliability, performance, and compliance.	• Conduct SIT, UAT, performance testing, security testing. • Resolve issues and refine configurations.
Support, Maintenance & SLA Management	Post-deployment support and continuous optimization.	• Provide Tier 1–3 support, system updates, and patches. • Monitor performance and optimize workflows. • Deliver periodic training refreshers and documentation updates.
Unique Document Referencing Code (Document ID Module)	Automated generation of unique, tamper-proof reference codes for each document to support tracking, auditability, and retrieval across all departments.	• Design a standardized document coding structure aligned with KRA's classification and taxonomy rules. • Configure system-generated unique identifiers for every document captured, uploaded, or created in the DMS. • Ensure IDs persist across workflows, versions, and archives. • Enable barcode/QR code generation for physical or digitized records. • Integrate the reference codes with search, reporting, audit logs, and integration endpoints.
AI-Ready Data Storage & Emerging	Design and implementation of data storage structures and formats that support AI, analytics, and other emerging	Configure structured and semi-structured data storage formats suitable for AI/ML processing. • Ensure metadata, indexing,

Technology Integration	technologies such as blockchain for enhanced security, traceability, and intelligent automation.	and tagging standards support machine learning, predictive analytics, and natural language processing. • Design and implement APIs or connectors for AI-driven insights and blockchain integration. • Enable document immutability and tamper-proof storage using blockchain for critical records. • Standardize formats (e.g., JSON, XML, PDF/A, CSV) to ensure interoperability with AI and analytics tools. • Provide system documentation detailing AI-ready structures, blockchain implementation, and data governance policies.

2.2 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 System
ii. KRA Tax Systems
iii. Supply Chain Management System
iv. Mail Server
v. SMS Gateway
vi. Active Directory
vii. CRM
viii. Any other relevant systems

Functional and non-functional requirements documentation

Requirement	Future State
Functional Requirements	i. Provide a centralized repository for storing, indexing, and retrieving all corporate and taxpayer-related documents. ii. Generate unique document referencing codes for traceability and auditability. iii. Support document version control with full version history. iv. Maintain audit trails for all document activities, including creation, access, modification, approval, and deletion. v. Enable role-based access control (RBAC) for all users. vi. Automate workflows for document creation, review, approval, and archival. vii. Include OCR and automated metadata extraction for digitized documents. viii. Support bulk upload and migration of legacy digital documents from existing repositories. ix. Provide tools for migration and transformation of manual or unstructured legacy documents into standardized, AI-ready formats. x. Support secure import and export of documents in standard formats (PDF, PDF/A, Word, Excel, XML, JSON, CSV). xi. Enable document retention scheduling and automatic archival/disposal according to statutory and organizational policies. xii. Provide search and retrieval using keywords, metadata, full-text search, filters, and document type. xiii. Integrate with existing enterprise systems such as ERP, HRMS, iTax, email, and AD. xiv. Include AI-based intelligent document classification. xv. Provide predictive analytics and dashboards for workflows, compliance, operational KPIs, and decision-making. xvi. Support multi-level approval workflows, configurable by department and document type. xvii. Facilitate secure interdepartmental collaboration, including document sharing and co-authoring. xviii. Enable metadata tagging and categorization based on predefined taxonomies. xix. Allow rollback or recovery of accidentally deleted or modified documents. xx. Provide notifications and reminders for pending approvals, actions, or deadlines. xxi. Maintain historical records for compliance, reporting, and legal purposes.

	xxii. Support mobile access for authorized users. xxiii. Provide document creation templates and standardization for contracts, agreements, legal instruments, and other official documents. xxiv. Provide reporting capabilities for audit, compliance, workflow status, and operational performance. xxv. Support interoperability with emerging technologies such as AI and blockchain for intelligent automation and tamper-proof record-keeping.
Non-Functional Roles	**System Response Time** **Document Retrieval:** Response Time: < 2 seconds **Document Upload:** Response Time**:** < 5 seconds for documents up to 10 MB document sizes. **Document Indexing and Metadata Entry:** Response Time**:** < 3 seconds **User Authentication:** Response Time: < 2 seconds **System Navigation (e.g., moving between different sections, opening menus):** Response Time: < 1 second **Document Preview:** Response Time: < 3 seconds for previewing documents up to 10 pages The system must support up to 10,000 concurrent users across all departments without performance degradation. The DMS should handle at least 1,000 document transactions per minute during peak hours. **Reliability and Availability**

	Uptime: The system should maintain an uptime of 99.9%, ensuring high availability for all departments. **Failover Mechanism to be implemented:** Define a comprehensive failover mechanism(multiple nodes/instances **Data Integrity:** Ensure data consistency and integrity across all transactions and storage. **Usability:** User Interface: Provide an intuitive and user-friendly interface that accommodates users with varying technical expertise. User Training: Provide comprehensive training materials and support to facilitate user adoption. **Maintainability:** Modularity: Design the system with modular components to facilitate easy updates and maintenance. Documentation: Provide thorough documentation for all system components, including design, development, and user manuals. Error Handling: Implement robust error handling and logging mechanisms to aid in troubleshooting and maintenance. **Interoperability:** Integration: Ensure seamless integration with existing systems used by customs, domestic taxes, and corporate support services. Standards Compliance: Adhere to industry standards for data formats and communication protocols to facilitate interoperability. **Scalability:**

	Horizontal Scaling: Design the system to support horizontal scaling to accommodate increasing user loads and data volumes. Vertical Scaling: Ensure the system can scale vertically with hardware upgrades to improve performance. **Legal and Regulatory Compliance:** Data Privacy: Comply with data privacy regulations ensuring user data is protected and managed appropriately. Regulatory Compliance: Ensure the system meets all regulatory requirements specific to customs, domestic taxes, and corporate support services Backup Frequency: Perform daily backups of all critical data and system configurations. Recovery Time Objective (RTO): The system should be recoverable within 2 hours in the event of a failure. **Incident Resolution Time:** Ensure incidents are resolved within 4 hours for high-priority issues and 24 hours for lower-priority issues. **User Experience:** Design user-friendly interfaces and workflows. Ensure accessibility for all relevant staff. **Integration Needs:** Identify systems that need to integrate with the DMS. Specify data migration requirements/strategy.

Expected Results (Deliverables)

DMS Module / Scope Area	Key KPIs	Expected Deliverables
Enterprise DMS Platform	System uptime (%), user adoption rate (%)	Fully deployed and operational DMS (on-premise/cloud-ready), AI-enabled, integrated with KRA core systems (ERP, HRMS, iTax,Cuustoms, email, AD)

Centralized Document Repository	% documents digitized, search accuracy, document version accuracy	Central repository with structured taxonomy, metadata, classification, and unique document referencing code
Workflow Automation	Workflow turnaround time, workflow completion rate, manual intervention reduction	Digitized workflows for document creation, review, approval, archival, and exception handling
Data Migration & Transformation	% of legacy documents migrated, data integrity rate	Legacy documents scanned, digitized, cleansed, indexed, and transformed into AI-ready formats
AI & Emerging Technology Modules	AI classification accuracy, metadata extraction accuracy, predictive insights utilization	OCR, automated metadata extraction, predictive analytics dashboards, blockchain-enabled document immutability (optional)
Reporting & Analytics Dashboards	KPI monitoring accuracy, timely report generation	Dashboards for workflow status, document usage, audit trails, compliance monitoring, and AI-driven insights
Training & Documentation	User satisfaction rate, training completion rate	User manuals, SOPs, administrator guides, AI/ML usage guides, end-user and admin training sessions
Support & Maintenance	SLA compliance (%), security incident rate, backup & recovery success rate	Tier 1–3 support, system updates, patching, performance monitoring, and optimization
Audit & Compliance Module	Audit trail coverage, regulatory compliance rate, document integrity	Periodic compliance reports, tamper-proof audit trails, and adherence to statutory retention policies
Change Management & Collaboration	Interdepartmental sharing frequency, user adoption rate, user satisfaction	Awareness campaigns, adoption strategies, feedback mechanisms, secure document sharing and collaboration features

Time frame

A three (3) year contract period applies for ALL products and Services (where applicable)

Detailed Specification/Requirements

Include requirement for maintenance, warranty and support/licences

TABLE 1: MANDATORY TECHNICAL REQUIREMENTS.

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 Document 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 Document Management solution MUST be inclusive of the following components: **Functional Requirement** i. The system must provide a centralized repository for all corporate and taxpayer-related documents. ii. The system must provide unique document referencing codes for traceability and auditability. iii. The system must support document version control with full version history. iv. The system must provide audit trails for all document activities (creation, access, modification, approval, deletion). v. The system must enable secure, role-based access control (RBAC) for all users. vi. The system must support workflow automation for document creation, review, approval, and archival. vii. The system must provide OCR and automated metadata extraction for digitized documents. The system must allow bulk data migration from existing digital repositories. viii. The system must allow bulk data migration from existing digital repositories. ix. The system must support integration with existing enterprise systems (ERP, HRMS, iTax, email, AD/LDAP). x. The system must allow secure Upload,import and export of documents in standard formats (PDF, PDF/A, JPEG,JPG,Word, Excel, XML, JSON, CSV). xi. The system must ensure document retention scheduling and automatic archival/disposal in line with statutory and organizational requirements. xii. The system must allow search and retrieval by keywords, metadata, document type, or other filters	

xiii. The system be able to compress and decompress of stored documents information .

1.6 Security & Compliance

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.

2. Technical Requirements

i. The system must be **deployable on-premise and cloud-ready** (hybrid deployment).
ii. The system must ensure **encryption of data at rest and in transit** (industry-standard protocols).
iii. The system must provide **high availability and redundancy**, ensuring minimum 99.5% uptime.
iv. The system must support **Single Sign-On (SSO) and Multi-Factor Authentication (MFA)**.
v. The system must provide **secure mobile access** for authorized users.

		vi. The system must comply with **data protection, privacy, and regulatory requirements**. **3.Implementation Requirements** i. The supplier must provide **migration and transformation of legacy documents**, ensuring integrity and standardization. ii. The supplier must provide **training for end-users and administrators**, including manuals and SOPs. iii. The supplier must perform **system testing** (unit, integration, user acceptance, and performance testing). iv. The supplier must provide **post-deployment SLA-backed support and maintenance**.	
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.	
5	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.	
6	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.	
7	Licensing	The bidder is required to state the licensing model used by the product and other related licenses required by the product.	
8	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 3: 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)
1	**Key Solution Features**	i. The system should support AI-based intelligent document classification.	4	
		ii. The system should provide predictive analytics and dashboards for workflows, compliance, and operational KPIs.	3	
		iii. The system should support multi-level approval workflows, configurable by department and document type.	5	
		iv. The system should enable interdepartmental collaboration with secure sharing and co-authoring.	5	
		v. The system should support bulk digitization of physical documents.	4	
		vi. The system should support metadata tagging and categorization according to defined taxonomies.	4	
		vii. The system should allow rollback/recovery of accidentally deleted or modified documents.	3	
		viii. The system should enable notifications and reminders for pending approvals or actions.	4	
		ix. The system should maintain historical records for compliance and reporting.	2	

		x.	The system should support AI-ready data structures for machine learning and analytics.	4	
		xi.	The system should support blockchain or tamper-proof storage for critical documents.	4	
		xii.	The system should provide batch processing for document ingestion and transformation.	4	
		xiii.	The system should provide detailed dashboards for system health, performance, and user activity.	2	
		xiv.	The system should provide user-friendly interfaces with intuitive navigation and accessibility compliance.	3	
		xv.	The system should allow system configuration by administrators (workflows, taxonomies, templates) without vendor intervention.	5	
		xvi.	The system should support performance monitoring, alerts, and reporting.	2	
		xvii.	The supplier should provide change management support, including awareness campaigns and adoption strategies.	1	
		xviii.	The supplier should provide documentation of AI, integration, and workflow configurations.	4	
		xix.	The supplier should perform security validation and penetration testing prior to handover.	2	
		xx.	The supplier should ensure integration with emerging technologies where applicable.	4	
Integrations					

2	**Integrations**	a) The solution **MUST** integrate and authenticate Active Directory user identities.	3	
		b) The solution **MUST** support the creation, import and export of bulk users using CSV files or any other mechanism where applicable.	2	
		c) The solution **MUST** support Virtualized Environment Setup	2	
		d) The solution **MUST** integrate with all relevant/applicable KRA applications	4	
		e) The solution **MUST** integrate with SMS gateway for token delivery.	3	
		f) The solution **MUST** integrate with SIEM solution.	2	
		g) The solution **MUST** use SSL certificates/Encryption techniques to secure communication.	4	
		h) The solution **MUST** support the following standards • Security Assertion Markup Language (SAML) • System for Cross-domain Identity Management (SCIM) • OAuth 2.0	2	
Implementation Overview				
3	**Implementation Overview**	a) 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.	5	
		b) Successful bidder is required to: • Review the existing Business process model for the purpose of developing a desired model, while meeting the KRA legal services	4	

		management objectives and best practice. • Design an enterprise Document 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 the Document 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.		
TOTAL MARKS			**100**	
Total marks for Technical Requirements				
NB The pass mark shall be 80% of the key solution features (item 1) and 80% of the rest of the features (item 2-10).				

Table 4: 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	10	

	capabilities, aligning with the the key technical and functional features criteria specified.		

Table 5: Demo Key Areas of focus for Document Management System

Minimum Viable Product Deliverable	Description (What It Must Include)	Score
Core Document Repository & Search Functionality	• Central document storage • Document indexing, metadata & tagging • Version control & audit trails • Templates & naming conventions • Advanced search & filtering • Check-in/check-out features	4
Workflow Automation for Document Processes	• Automated review & approval workflows • Routing rules & notifications • Deadline triggers & alerts • Escalation paths for delayed processes • Digital approval tracking	2
Security, Access Control & Compliance Tracking	• Role-based access control (RBAC) • Authentication (SSO/MFA) • Encryption at rest & in transit • Audit logs for all document actions • Compliance rule enforcement	2
Integration with Email & Key Enterprise Systems	• Email capture • Integration with ERP, Tax, Customs, Legal systems on identified integration points and workflows. • REST/SOAP API connectors • Centralized authentication with AD	2

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) Document management solution project.	Demonstrated experience through Previous execution of at least one (1) document management solution project. In order to be awarded marks bidders MUST submit a copy of executed Contract or LSO, supported by: a) A brief description of the project delivered **b)** Full contacts; address, telephone and email of customer where assignments/ projects were executed. **c)** Completion Certificate/Letter from the Customer confirming successful completion of the project.	5	
2	**Technical Capacity Evaluation** Minimum of three (3) Technical staff with the following academic and professional qualifications:	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	12	

	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.	professional certificates in order to be scored.		
3	**Project/Team Lead – 7 marks** **1. Academic Qualifications:** 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	**1. Academic Qualifications** 2 marks **2. Professional Certifications** 3 marks. 3. **Experience** • 8 years and above – **2 Marks** • Between 5 and seven years – **1 Mark** • Less than 5 Years – **0 Marks**	14	

	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.			
	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 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	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		

	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, Tier 2 or Tier 3 Partnership Level with the OEM.	Relevant OEM Partnership • Tier 1 (or equivalent) Partnership - 4 Marks • Tier 2 (or equivalent) Partnership – 3 Marks • Tier 3 (or equivalent) Partnership – 2 Marks Note: Bidders MUST attach copies of partnership certification or a letter from the OEM indicating his partnership Level.	**4**	
5	Technical Approach/Methodology	Bidders to demonstrate/provide evidence of a clear and detailed understanding of the solution, including:	**5**	

		a) Project delivery Approach and Methodology for implementation and support of the solution – 3 Marks b) Work plan (Bidder MUST provide a three (3) year work plan Implementation and support for the solution –2Marks		
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 Disaster Recovery Data Centres, including High Availability (HA) Configuration	**5**	
	TOTAL MARKS		**45**	
	CUT OFF		**36**	

FINANCIAL REQUIREMENT

Vendors are required to provide a breakdown to how they arrived at the total costs.

TABLE 6: OVERALL TENDER EVALUATION CRITERIA

No	Criteria	Maximum Score:	Cut-Off Score
1	Mandatory Technical Requirements.	Mandatory	All Mandatory
2	Minimum Technical and Implementation Requirements	100	80

3	Solution Demonstration	10	8
4	Vendor Evaluation	45	36
5	Financial Evaluation	Award to the lowest evaluated bidder.	

ANNEXURES

	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.