KENYA REVENUE AUTHORITY

ISO 9001:2015 CERTIFIED

Terms of Reference for Digital Shipment Solution

1. EXECUTIVE SUMMARY

The Customs & Border Control Department plays a pivotal role in facilitating international trade, safeguarding society, and ensuring efficient revenue collection for the Government. However, the rapid expansion of global trade and evolving security threats have exposed the limitations of the current traditional paper-based systems, which struggle with efficiency, accuracy, and responsiveness. To meet these challenges, modernization of customs operations is essential.

The proposed solution seeks a qualified vendor to deliver a comprehensive digital shipment system that modernizes and streamlines the management of imports and exports. This solution will integrate end-to-end shipment processing, automated risk assessment, accurate and transparent valuation functionalities, GS1 standard encoding for global interoperability, advanced data analytics and automation, and real-time information sharing to enhance visibility and coordination among stakeholders. By implementing this digital shipment solution, organizations will realize significant strategic benefits, including optimized revenue collection through improved valuation and risk management, faster cargo clearance to facilitate legitimate trade, strengthened border security through advanced profiling, and enhanced operational efficiency via digital workflows that reduce errors and redundancies. Ultimately, the solution balances trade facilitation with security, contributing directly to national economic growth, competitiveness, and stability.

Through this solution, the KRA will not only modernize its Customs operations but also establish a resilient, future-ready framework for international trade and national security.

2. Background

The Kenya Revenue Authority (KRA) is tasked with collecting revenue for the Government of Kenya, with the Customs & Border Control Department playing a crucial role in facilitating international trade. This includes expediting the clearance of goods, regulating imports and exports, collecting revenue, and enforcing legal prohibitions and restrictions to protect society and the environment. However, global trade expansion and evolving security threats necessitate modernized customs operations. Traditional paper-based systems struggle with efficiency and accuracy, hence the need for modern systems and solutions built on the latest technology available.

KRA is seeking a qualified vendor to provide a comprehensive digital solution that integrates shipment processing, risk assessment, and valuation functionalities. This solution must incorporate GS1 standard encoding identifiers, leverage data analytics, automation, and real-time information to streamline customs processes, enhance revenue collection, and strengthen border security.

3. Objectives:

3.1. Intelligent Document Processing and Analysis

- Deploy advanced Optical Character Recognition (OCR) systems for automated analysis of scanned invoices, bills of lading, packing lists, and commercial documentation
- Implement comprehensive entity details extraction, identification, and profiling capabilities for traders, manufacturers, and intermediaries
- Establish automated identification and analysis of data inconsistencies across related transaction documents for imports, exports, transit, and transhipment consignments
- Deploy management and annotation systems for commercial data streams to ensure regulatory compliance and data integrity

3.2. Advanced Revenue Protection and Valuation Systems

- Implement comprehensive mis-valuation detection systems to identify over-valuation and under-valuation practices across all trade categories
- Deploy real-time price comparison engines utilizing reference databases, market intelligence, and commodity exchange data
- Establish customs valuation systems utilizing comprehensive historic data analysis, pattern recognition, and statistical benchmarking
- Integrate GS1 Digital Link technology and product authentication systems for enhanced supply chain verification and anti-counterfeiting

3.3. Predictive Analytics and Risk Intelligence

- Deploy advanced predictive analysis and comprehensive reporting systems for proactive risk management and threat identification
- Implement digital shipment vetting and automated classification systems with AI-powered risk scoring algorithms
- Establish comprehensive trade pattern algorithms for behavioral analysis, trend identification, and anomaly detection
- Deploy automated identification, examination, and analysis systems for trader profiles and high-risk transaction patterns

3.4. Comprehensive Inspection and Audit Analytics

- Implement pre-arrival analysis systems for advance risk assessment, resource allocation, and inspection planning optimization
- Deploy comprehensive post-audit analysis capabilities for performance monitoring, compliance verification, and continuous improvement
- Establish advanced cargo inspection analysis systems with automated recommendation engines for risk resolution and corrective actions

- Develop integrated analysis of cargo inspections with performance metrics, effectiveness measurement, and operational optimization

4. Scope of Work

Supply, Delivery, Installation and Commissioning of a Digital Shipment solution

4.1 Digital Shipment Processing and Automation

4.1.1 Advanced Document Processing and OCR Systems

- Optical Character Recognition (OCR) Technology:
  - Advanced OCR engines for processing scanned invoices, bills of lading, packing lists, and commercial documentation
  - Multi-language support with intelligent character recognition and document classification
  - Automated data field extraction, validation, and confidence scoring systems
- Entity Identification and Profiling:
  - Automated extraction and identification of importers, exporters, manufacturers, and intermediary entities
  - Dynamic entity profiling with historical transaction analysis and behavioral pattern recognition
  - Cross-reference capabilities with international watch lists and sanctions databases

4.1.2 Automated Clearance and Processing

- Intelligent Clearance Automation:
  - Development of automated clearance processes for low-risk shipments with AI-powered decision engines
  - Integration with logistics and transportation systems for seamless cargo flow
  - Electronic release notifications with real-time status updates and tracking capabilities
- Digital Shipment Vetting and Classification:
  - Automated shipment classification with risk-based routing and processing workflows
  - Real-time shipment tracking and tracing with end-to-end visibility
  - Provision of comprehensive shipment status updates to traders and regulatory authorities

4.2 Advanced Risk Management and Intelligence Systems

4.2.1 AI-Powered Risk Assessment Engine

- Intelligent Risk Analysis Platform:
  - Development of sophisticated risk assessment engines utilizing AI/ML algorithms for comprehensive shipment data analysis
  - Implementation of advanced risk profiling and targeting capabilities with behavioral analytics
  - Integration with intelligence databases, external risk information sources, and international threat intelligence
- Predictive Analytics and Pattern Recognition:
  - Machine learning algorithms for trade pattern analysis and behavioral anomaly detection
  - Predictive risk scoring models using historical data and real-time intelligence feeds
  - Trend analysis systems for identifying emerging threats and compliance risks

4.2.2 Anomaly Detection and Alert Systems

- Advanced Anomaly Detection:
  - Implementation of sophisticated anomaly detection algorithms to identify suspicious shipments and trading patterns
  - Automated high-risk shipment identification with intelligent alerting and escalation protocols
  - Development of risk-based inspection workflows with resource optimization and priority management
- Automated Recommendation Systems:
  - Intelligent recommendation engines for resolving identified risks and compliance issues
  - Automated action planning and resource allocation for inspection and examination processes

4.3 Comprehensive Valuation and Revenue Protection Systems

4.3.1 Advanced Valuation Assessment Platform

- Comprehensive Valuation Database and Analytics:
  - Development of extensive valuation databases with historical data, market information, and real-time pricing
  - Implementation of advanced valuation methodologies, rules engines, and statistical analysis tools
  - Automated valuation checks, calculations, and cross-reference verification systems

- Mis-valuation Detection and Price Comparison:
  - Automated over-valuation and under-valuation detection using statistical analysis and market benchmarks
  - Real-time price comparison systems with international reference databases and commodity exchanges
  - Historical data analysis engines for customs valuation patterns and anomaly detection

4.3.2 Valuation Risk Assessment and GS1 Integration

- Advanced Risk Assessment for Valuation:
  - Implementation of sophisticated risk assessment algorithms to identify valuation discrepancies and fraud patterns
  - Automated alerts and escalation procedures for potential valuation fraud and revenue protection
- GS1 Digital Link Technology Integration:
  - QR code scanning technology for instant product verification using GTIN, batch numbers, and pricing data
  - Integration with global GS1 resolver services for authentic product information and supply chain verification
  - Digital signature compliance per ISO/IEC 20248 standards for enhanced supply chain security

4.4 Comprehensive Inspection and Audit Analytics

4.4.1 Pre-arrival and Post-audit Analysis Systems

- Pre-arrival Analysis and Planning:
  - Advanced pre-arrival risk assessment and resource allocation optimization systems
  - Predictive inspection planning with cargo prioritization and workflow management
  - Integration with vessel tracking and cargo manifest analysis for advance preparation
- Post-audit Analysis and Performance Monitoring:
  - Comprehensive post-audit analysis capabilities for performance monitoring and compliance verification
  - Advanced cargo inspection analysis with effectiveness measurement and continuous improvement
  - Performance analytics and operational optimization with KPI tracking and reporting

4.5 System Infrastructure and Integration Platform

4.5.1 API Development and Data Exchange

- Comprehensive API Architecture:
  - Development of robust APIs for integration with iCMS and other Customs systems
  - Implementation of international data exchange standards and protocols
  - Integration with external platforms, port community systems, and regional customs networks
- Data Integration and Management:
  - Multi-source data collection from shipment declarations, scanner images, and historical records
  - Automated data cleansing, normalization, and centralization for efficient analysis

4.5.2 Analytics, Reporting, and Dashboard Systems

- Advanced Data Analytics Platform:
  - Implementation of comprehensive data analytics tools for generating reports on customs activities and performance
  - Development of interactive dashboards for visualizing key performance indicators and operational metrics
  - Real-time monitoring and alerting systems with customizable reporting capabilities

4.6 Regulatory Compliance and Security Framework

4.6.1 Data Privacy and Security Implementation

- Comprehensive Security Infrastructure:
  - Implementation of advanced data encryption (AES-256) and access control measures
  - Multi-factor authentication systems and role-based access management
  - Compliance with Kenya Data Protection Act and international data privacy regulations

4.6.2 Regulatory Compliance and Audit Systems

- Compliance and Audit Framework:
  - Ensuring comprehensive compliance with international customs standards and WCO regulations
  - Implementation of complete audit trails for tracking all system activities and transactions

- Compliance monitoring and reporting systems with automated regulatory updates

4.7 Training, Support, and Knowledge Transfer

4.7.1 Comprehensive Training Programs

• Training and Capacity Building:

- Development of comprehensive training programs for customs officers, traders, and system administrators
- Creation of detailed user manuals, online resources, and interactive learning modules
- Specialized training on OCR systems, risk assessment tools, and advanced analytics platforms

4.7.2 4.7.2 Technical Support and Maintenance

• Ongoing Support Infrastructure:

- Provision of 24/7 technical support and comprehensive maintenance services
- Regular system updates, performance optimization, and technology enhancement programs
- Knowledge transfer programs and local capacity building initiatives

5. Methodology

The vendor should clearly demonstrate a comprehensive understanding of the Terms of Reference (TOR) and all outlined requirements for the Supply, Delivery, Installation and Commissioning of Digital Shipments solution. In addition, they should present a well-defined delivery methodology that explains how they intend to execute the assignment.

6. Implementation team and responsibilities

The vendor should clearly demonstrate the firm's overall experience, as well as present a detailed breakdown of the proposed team structure. This should include the qualifications, roles and relevant experience of all key experts who will be assigned to the assignment.

7. Implementation schedule work plan

The vendor shall complete the assignment within a maximum duration of **18 months**. Upon delivery, the solution will be covered by a **warranty period of one year**. In addition, the vendor shall provide

maintenance and support services for a period of three years following implementation.

8. Time frame

Bidders are required to implement the solution within the stipulated **18-month period**. They must **contractually commit** to this timeline and ensure full delivery within the agreed schedule.

9. Key Deliverables

1. Software and System Deliverables:

- **Declaration Processing:**
  - Automated data extraction and verification.
- **Risk Assessment:**
  - A risk profiling and scoring engine.
  - Automated risk alerts and notifications.
  - Integration with intelligence databases and watch lists.
  - Customizable risk rules and algorithms.
- **Valuation:**
  - Automated calculation of customs duties and taxes.
  - Integration with customs valuation databases and tariff schedules.
  - Tools for verifying declared values.
  - Historical valuation data analysis and reporting.
- **Document Management:**
  - OCR capabilities for automated data extraction.
  - Version control and audit trails.

- **Shipment Tracking and Tracing:**
  - Real-time shipment tracking and status updates.
  - Integration with logistics providers' systems.
  - Alerts for shipment delays or discrepancies.
- **Reporting and Analytics Dashboard:**
  - Customizable reports on customs revenue, trade statistics, and compliance.
  - Data visualization tools for analysing trends and patterns.
  - Audit trail reports.
- **API and Integration Components:**
  - APIs for data exchange with other government agencies and trade stakeholders.
  - Integration with existing customs systems and databases.
  - Electronic Data Input (EDI) capabilities.
- **User Interface and Experience (UI/UX):**
  - User-friendly and intuitive interface for customs officers.
  - Multilingual support.
  - Role-based access control.

2. Data and Information Deliverables:

- **Centralized Customs Database:**
  - A comprehensive database of shipment, risk, and valuation data.
  - Standardized and harmonized data.
  - Data quality control and validation.
- **Risk Profiles and Intelligence Data:**

- Risk profiles of traders, commodities, and countries.
- Intelligence data on smuggling and illicit trade.
- Watch lists and alert systems.

- **Valuation Databases and Tariff Schedules:**

  - Up-to-date customs valuation databases and tariff schedules.
  - Market price information and valuation benchmarks.

- **Reports and Analytics:**

  - Customs revenue reports.
  - Trade statistics reports.
  - Compliance reports.
  - Risk assessment reports.

3. Operational and Process Deliverables:

- **Training and Documentation:**

  - Comprehensive user training materials and documentation.
  - Training programs for customs officers and traders.

- **System Maintenance and Support:**

  - Ongoing technical support and maintenance.
  - System updates and enhancements

10. Vendor evaluation

PART A: TECHNICAL SPECIFICATION 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.

Table 1: Functional Requirements

No	Feature	Requirement	Bidder's detailed Response (Pass/Fail)
1.	**Digital Shipment Processing**	Electronic submission and processing of customs declarations, manifests, and supporting documents	
		Automated data capture and validation.	
		Real-time shipment tracking and status updates.	
		Integration with logistics providers and other trade stakeholders.	
		GS1 Digital Link QR code integration for instant product verification, authentication and traceability using global standards (GTIN, batch numbers, serial numbers, expiry dates	
2.	**Advanced Risk Assessment**	Risk profiling based on various parameters (e.g., trader history, commodity type, origin, and destination).	
		Automated risk scoring and flagging of high-risk shipments.	
		Integration with intelligence databases and watch lists.	
		Ability to define and customize risk rules and algorithms.	
		GS1-powered AI risk assessment using structured product identifiers and supply chain data to enhance threat detection accuracy.	
		Anomaly detection using AI and machine learning.	
3.	**Accurate Valuation**	Automated calculation of customs duties and taxes based on valuation rules and tariff schedules.	

		Integration with customs valuation databases and market price information.	
		Support for various valuation methods (e.g., transaction value, deductive value, computed value).	
		Tools for verifying declared values and identifying potential undervaluation.	
		Historical data analysis of valuation trends.	
4.	**Data Management**	Centralized database for storing and managing shipment, risk, and valuation data.	
		Data standardization and harmonization.	
		Data quality control and validation.	
5.	**System Integration**	Integration with existing customs systems and databases.	
		Integration with other government agencies (e.g., tax authorities, trade regulators).	
		Integration with international trade platforms and systems.	
		Integration with global GS1 network infrastructure and manufacturer databases for real-time product information access.	
		API-based integration for seamless data exchange.	
6.	**Reporting and Analytics**	Customizable reports and dashboards for monitoring key performance indicators.	
		Data visualization tools for analyzing trends and patterns.	
		Audit trail functionality for tracking all transactions.	

PART B: NON-FUNCTIONAL REQUIREMENTS

Bidders are required to demonstrate how their proposed solution meets the listed requirements. Each requirement will be evaluated and scored according to the following criteria.

Table 2: Non-Functional Requirements

No	Feature	Requirement	Bidder's detailed Response (Pass/Fail)

1	**Data Management**	Data security and privacy protection.	
		Scalable and Reliable Infrastructure	
		High-performance servers and storage systems.	
		Robust network infrastructure with high bandwidth.	
		Cloud-based deployment or on-premises infrastructure, depending on requirements.	
		Disaster recovery and business continuity capabilities.	
2	**Security Infrastructure**	Strong authentication and authorization mechanisms.	
		Data encryption (at rest and in transit).	
		Intrusion detection and prevention systems.	
		Regular security audits and vulnerability assessments.	
3	**Performance Requirements**	Low-latency configuration for efficient data retrieval and analytics queries	
		Scalable infrastructure to support growing tax data volumes	
		High availability with a minimum uptime of 99.9%	
		Support for up to 5,000 concurrent users	
		Query response times of less than 2 seconds	
4	**Software and Platforms**	Robust database management systems	
		Application servers and web services.	
		Risk assessment and analytics platforms.	
		Electronic data interchange (EDI) software.	
		GS1-compliant resolver services and database systems supporting global product identification standards and real-time manufacturer data synchronization.	
		AI and Machine learning platforms.	
5	**User-Friendly Interface**	Intuitive and easy-to-use interface for customs officers and other users.	
		Multilingual support.	
		Role-based access control.	
6	**Training and Support**	Comprehensive user training and documentation.	
		Ongoing technical support and maintenance.	

7	**Key Considerations (General)**	Interoperability: The system must be able to exchange data with various stakeholders, both domestic and international.	
		Data Security: Customs data is highly sensitive, so robust security measures are essential.	
		Scalability: The system must be able to handle increasing volumes of trade and data.	
		Flexibility: The system should be adaptable to changing customs regulations and trade practices.	
		AI and Machine Learning: The integration of AI and machine learning is extremely important for modern risk assessment.	

Table 3: Minimum Security Requirements

No	Feature	Requirement	Bidder's detailed Response (Pass/Fail)
1	**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.	
2	**Access Control**	The system must implement robust access control mechanisms, including multi-factor authentication, role-based access controls, and the principle of least privilege.	
3	**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.	
4	**Incident Response**	The vendor to address security breaches or incidents promptly and minimize impact must establish an effective incident response plan.	
5	**Data Integrity**	Mechanisms must be in place to ensure the integrity of data, including checksums, digital signatures, and block chain technology where applicable.	

6	**Continuous Monitoring**	The system must have continuous monitoring capabilities to detect and respond to security threats in real-time.	
7	**Security Training**	Vendors must provide security training for system users and administrators to foster a culture of security awareness.	
8	**Secure Development**	The solution must be developed following secure coding practices, and vendors must demonstrate a commitment to security throughout the software development lifecycle.	
9	**Authentication**	No identification and authentication information must be hard-coded or scripted into the application.	
10	**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.	
11	**GS1 Digital Signature Compliance**	Implementation of GS1 Digital Signature standards for cryptographic verification of product identities and supply chain documentation.	

VENDOR EVALUATION CRITERIA

	Bidder Experience	Maximum score
No.	**Requirement Description**	

	Firm's Experience At least Five (5) years' Experience in Installation, Supply, Commissioning and Maintenance of Digital Shipment Solution. The bidder to provide a Company profile demonstrating ability to Supply, Deliver, Install and Commission, and respond to all maintenance issues. ***(3 marks)*** **Firm Experience** Above Five (5) years **(*4 marks*)** 3-5 years **(2 marks)** Bidder is required to describe and provide evidence of **3 similar projects** the bidder has undertaken within the last 5 years: a) Contract or LSO b) Completion certificate or Reference/recommendation letter from client For each satisfactory reference, the bidder will be scored per areas listed above i) Contract or Service Order **(1 Mark),** **ii)** Completion certificate or Recommendation letter from client **(1 mark)** References required should be for sites where the bidder or its partners in the tender implemented the solution.	**10**
	Project Team	

	<u>Personnel's Qualifications and Experience</u> Bidder is required to provide a responsibility matrix and profiles of delivery leads **(Project Manager, Development Lead, Solution Architecture Lead, and Infrastructure Lead).** Bidders are required to submit actual and current project team members of the core team expected to be involved in the project and clearly indicating where the teams have carried out similar implementations. Bidders must provide the following documents for the core team: a) Detailed CV b) Academic qualifications/certificates c) Years of experience d) Relevant certifications	**30**

	For each lead the scoring will be as follows per lead (At least for the following roles Project Manager, Development Lead, Solution Architecture Lead, Infrastructure Lead – 4 Leads to be evaluated) Detailed CV demonstrating lead having worked in a successful Digital Shipment Solution implementation in the proposed role **Project Manager** a) **Lead (Project Manager)** with relevant qualification i. Degree in Information and Communication Technology or other related field (2 Marks) (attach certificate) ii. Diploma in Information and Communication Technology or other related field (1 Mark) (attach certificate) b) **The Lead (Project Manager)** must have certification in Project Management (PMP/ Prince2) or any other similar/related course. (Must attach copy of certificate) – 2 marks c) Must have a minimum of five (5) years' experience in Project Management (Must provide detailed and signed CV) – Above 5 years – 2 marks – 1 to 5 years – 1 mark	**6**

	Development Lead a) Lead with relevant qualification i. Degree in Information and Communication Technology or other related field (2 Marks) (attach certificate) ii. Diploma in Information and Communication Technology or other related field (1 Mark) (attach certificate) b) The Lead must have certification in Project Management (PMP/Prince2) or any other similar/related course. (Must attach copy of certificate) – 2 marks c) Must have a minimum of five (5) years' experience as Lead developer (Must provide detailed and signed CV) i. Above 5 years – 2 marks ii. 1 to 5 years – 1 mark	**6**

	Solution Architecture Lead a) Lead with relevant qualification i. Degree in Information and Communication Technology or other related field (2 Marks) (attach certificate) ii. Diploma in Information and Communication Technology or other related field (1 Mark) (attach certificate) b) The Lead must have certification in Project Management (PMP/Prince2) or any other similar/related course. (Must attach copy of certificate) – 2 marks c) Must have a minimum of five (5) years' experience in Architecture lead (Must provide detailed and signed CV) i. Above 5 years – 2 marks ii. 1 to 5 years – 1 mark	**6**

	Infrastructure Lead a) Lead with relevant qualification i. Degree in Information and Communication Technology or other related field (2 Marks) (attach certificate) ii. Diploma in Information and Communication Technology or other related field (1 Mark) (attach certificate) b) The Lead must have certification in Project Management (PMP/Prince2) or any other similar/related course. (Must attach copy of certificate) – 2 marks c) Must have a minimum of five (5) years' experience in as Infrastructure lead(Must provide detailed and signed CV) – Above 5 years – 2 marks – 1 to 5 years – 1 mark	**6**

	Quality Assurance Lead a) Lead with relevant qualification i. Degree in Information and Communication Technology or other related field (2 Marks) (attach certificate) ii. Diploma in Information and Communication Technology or other related field (1 Mark) (attach certificate) b) The Lead must have certification in ISTQB Certification (Must attach copy of certificate) – 2 marks c) Must have a minimum of five (5) years' experience as QA Lead (Must provide detailed and signed CV) ○ Above 5 years – **2** marks ○ 1 to 5 years – 1 mark	**6**
	Total	**40**
	Cut – off	**32**

Methodology and Work Plan:

Adequacy of the proposed Methodology and Work Plan in responding to the Terms of Reference will be evaluated on how the consultant proposes to address the areas listed below:	**50 marks**
Digital Shipment Solution **i) In this section the bidder is expected to provide a detailed and comprehensive work plan and methodology(s) on how they intend to execute the items indicated below:** • Digital Shipment Processing (5 marks) • Risk Management Engine and Anomaly Detection (5 marks) • Valuation Database & Risk Assessment (4 marks) • System Infrastructure and Integration (2 marks) • Regulatory Compliance and Security (2 marks) • Training and Technical Support (2 marks) • GS1 Digital Link Implementation (5 marks)	25
ii) Development of detailed Work plan with specific and clear milestones(10 marks)	10
iii) Live System Demonstration and Proof of Concept • OCR and Document Processing Component (5 marks) • AI Risk Assessment and Analytics Component (5 marks) • GS1 Digital Link and Valuation Component (5 marks)	15
Total Scores = 50	50
Cut-Off Score	40

Price schedule/Financial Proposal

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

OVERALL EVALUATION

The bid evaluation will take into account technical factors in addition to cost factors. The weight for Technical evaluation is 80% while Financial Evaluation will be based on the Lowest Evaluated Bid.

SUMMARY OF THE EVALUATION SCORES

Criteria	**Maximum Score / Requirement**	**Cut-off Score**
Technical requirements / Specifications	**Mandatory**	**Met**
Methodology	**35**	**28**
Bidder Qualifications (Vendor)	**40**	**32**
Demo	**15**	**12**
Total Points	**90**	**72**

Notes

1. The quoted price shall be in Kenyan shillings encompassing all costs associated with the Project scope of work. Additionally, it shall cover maintenance services, transfer of knowledge, and acquisition of the source code. All these elements are to be included within the total quoted price without any additional charges.

2. The financial remuneration for the development, implementation, and maintenance of the Digital shipment solution will adhere to the following terms:

   Milestone-Based Payments: At the negotiation stage payment shall be structured around the successful completion of predefined milestones that correspond to the project's phases. Each milestone payment will be contingent upon the acceptance of deliverables as per the agreed-upon specifications and timelines.

Annex I: API Security Requirements

General Rule: The solution must implement API-first design for integration i.e. API-first design for integration is a development strategy where APIs are designed, documented and defined before any application code is written, treating the API as a core product, not an afterthought.

	ANNEX I - API Security Requirements
	Review Area
1	**Governance**
1.1	Ensure the API is properly versioned. Versioning helps in keeping track and maintainance of the API.
1.2	Ensure that the API conforms to the orgnization set style and design guidelines such formatting of headers for consistency.
1.3	Ensure that the API is included as part of the organization's APIs inventory for Discoverability and Reusability
2	**Authentication**
2.1	Ensure that every request to the API or web service is authenticated.
2.2	Ensure a strong authentication mechanism is used; Required authentication mechanisms allowed for APIs/Web services in KRA are OAuth 2.0 and JWT
2.4	Ensure implementation of anti-brute force mechanisms on authentication endpoints such as account lock-outs, use Max Retry and jail features in Login.
2.6	When JWT is used, ensure: 1. Use a random complicated key (JWT Secret) to make brute forcing the token very hard. 2. Don't extract the algorithm from the header. Force the algorithm in the backend (HS256 or RS256). 3. Make token expiration (TTL, RTTL) as short as possible. 4. Don't store sensitive data in the JWT payload, it can be decoded easily.
2.7	When OAuth 2.0, ensure: 1. Always validate redirect_uri server-side to allow only whitelisted URLs. 2. Always try to exchange for code and not tokens (don't allow response_type=token). 3. Use state parameter with a random hash to prevent CSRF on the OAuth authentication process. 4. Define the default scope, and validate scope parameters for each application.
2.8	Ensure no sensitive authentication details, such as auth tokens and passwords are sent in the URL through GET requests.
3	**Authorization**

3.1	Ensure a proper authorization mechanism is implemented that checks if the authenticated subject has access to perform the requested action.
3.2	Ensure that the issued authentication and authorization tokens have a set expiry time.
3.3	Ensure the use of random and unpredictable values as Globally Unique Identifiers (GUIDs) for records identification. Auto-incrementing IDs should never be used.
3.4	Ensure the use of proper HTTP method for each API operation: GET (read), POST (create), DELETE (to delete a record). No request should be processed if the method is not appropriate for the requested resource.
3.5	Ensure the intergrating components only access the objects they require from the integrating systems. Responses should only return the data necessary to fulfill a request
4	**Data Protection**
4.1	Ensure that the responses from the API provide only legimate requested data that is not excessive.
4.2	Ensure sensitive information such as access tokens, bearer tokens, pins, passwords etc are not being returned in request responses or stored in logs in clear text.
4.3	Error messages must ensure that sensitive information about the integrating systems is not disclosed
4.4	Ensure sensitive data parameters such as passwords, PINs, Credit card numbers etc. being passed to the APIs are hashed
4.5	Ensure minimization/masking of customer PII such as MSISDN and ID Numbers when such are returned in request responses and displayed in logs.
4.6	Ensure the communication channel is encrypted. The Endpoints should make use of HTTPS and not of HTTP
4.7	Ensure proper implementation of HTTPS; i.e current secure TLSV
5	**Resource and Rate Limiting**
5.1	Ensure implementation of a limit on how often a client can call the API within a defined timeframe. This helps mitigate DoS attacks by throttling or blocking IP addresses after making concurrent requests within a very short period of time.
5.2	Define and enforce maximum size of data on all incoming parameters and payloads such as maximum length for strings and maximum number of elements in arrays.
5.3	For APIs processing large amounts of data, ensure data is processed asynchronously. Processing large amounts of data synchronously can prevent the API from responding in a timely manner forcing clients to wait.
6	**Secure Configuration**
6.1	Ensure implementation of the **X-Content-Type-Options: nosniff** header to protect API against MIME sniffing vulnerabilities.
6.2	Ensure implementation of the **X-Frame-Options: deny** header.
6.3	Ensure implementation of the **Content-Security-Policy: default-src 'none'** header.
6.4	Ensure that fingerprinting headers such as **X-Powered-By**, **Server**, **X-AspNet-Version**, etc are not present
6.5	Force content-type for your response. If you return application/json, then your content-type response is application/json.
6.6	Return the proper status code according to the operation completed. (e.g. 200 OK, 400 Bad Request, 401 Unauthorized, 405 Method Not Allowed, etc.).
7	**Vulnerability Management**
7.1	Ensure that the API supports use of updated and vendor supported dependencies and libraries.
7.2	If the API is externally facing, ensure that it's behind a Firewall

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

Annex II: Application Security Requirements

SN.	ANNEX II - Application Security Requirements
1	**Application Architecture**
1.1	Applications hosted in a shared hosting environment should be logically isolated from other applications in the same environment
1.2	Anti-virus scanning must be performed real-time on any file transmitted to the server
1.3	All network communications between components must be authenticated, and must not explicitly trust other network devices
1.4	If an application stores highly confidential information, data must be physically separated from other applications' data stores
1.5	Applications handling highly confidential data must not be hosted in a shared hosting environment or store its data in a shared database server
1.6	If an application shares a data store with another application, the data store must be segmented logically or physically. Logical segmentation should be implemented with access control mechanisms. Physical segmentation should be accomplished with a separate instance of the data store or a separate data store server
1.7	Any administrative functions that are not meant to be accessed by users from the Internet must be located in a private DMZ, which prevents direct Internet access to the servers
1.8	Systems directly facing the Internet must not store or cache confidential data, even for a short duration. This includes file uploads and downloads, source code, etc
1.9	Internet-facing systems must be placed behind a firewall that protects against network-based denial of service attacks, blocks ports that are not required for external access, and other network attacks
1.1	Applications must not connect to a database as a privileged user, such as the SA account in SQL Server or SYSTEM account in Oracle
1.11	Applications that connect to a database, application server, or any system that utilizes application IDs must do so using an account that has been granted access to only objects and functions needed for operation of the application
1.12	All function calls between application tiers should implement digital signatures to verify authenticity of the invoking application
1.13	Applications must be designed to enforce the least privilege principle for all processes
1.14	Application server interfaces must not be accessible from the Internet. This includes Web Services, DCOM, CORBA, SOAP, EJB, RPC, and any other method of invoking remote procedure calls
1.15	All application resources must require authentication for every call to each resource, and must be kept in compliance with the recommended password policies
1.16	All servers should be kept in sync with a time synchronization mechanism
2	**Network Communication and Session Management**

2.1	Sensitive information must be transmitted via a secure channel (SSL, SSH, etc.) or encrypted prior to transmission (PGP, etc.), using KRA approved methods
2.2	All communication sessions must use secure protocols
2.3	All transactions communication sessions must enforce session expiry so that after an unacceptable period of inactivity the session must terminate to guard against session hijacking
2.4	Any vendor proprietary protocols used must be well documented (i.e. the vendor must provide comprehensive documentation on the protocols such as technical specifications or white papers). Any vendor proprietary encryption algorithms must be FIPS-140 certified
2.5	Session IDs must use strong, non -predictable algorithms
2.6	All relevant session information should be captured and stored in a secure & auditable location
2.7	Only one session should be allowed per user operating from a single computer unless a specific business case has been established for allowing multiple sessions per user
2.8	Sessions should expire after a maximum set duration, regardless of activity
2.9	Session state must be maintained on the server for web-based applications, and be associated with a single client through the use of a session ID
2.1	Session state must be tied to a specific browser session through the use of a session cookie
2.11	Sessions must not be allowed to span both secure and non-secure connections
2.12	Applications must allocate session-based resources only after successful authentication. Allocating resources prior to this can lead to denial of service attacks, session fixation attacks, and others
2.13	Synchronization of time between servers and other relevant equipment must be implemented. This is instrumental in tracking time stamps between different systems particularly where systems share/exchange data
3	**Identification and Authentication**
3.1	Each user must be authenticated with a unique user-id and password on the application
3.2	User authentication data must be stored and maintained securely in a centralized location on the system
3.3	The application must support password expiry features with a configurable frequency. Parameterize this to allow flexibility in adjusting this value as required
3.4	The password must be secure on entry, at no point must the password be in clear text
3.5	All new user accounts must have a system-generated random password when created. A secure way of communicating the initial password to the user should be utilized e.g. via KRA e-mail account
3.6	All new user accounts must be created with reference to existing authoritative databases of approved persons e.g. identifying numbers in KRA's active staff database (HR) and National PIN certificate database
3.7	Users must be prompted to change their passwords the first time they log on to the application
3.8	Newly created accounts should be set to expire if not used for a configurable period of time. Parameterize this to allow flexibility in adjusting this value as required
3.9	The application must support password lockout after a configurable number of unsuccessful attempts. Parameterize this to allow flexibility in adjusting this value as required
3.1	The application must lockout a user account after the system is idle for a configurable period of time. Parameterize this to allow flexibility in adjusting this value as required
3.11	The application must support a password change notification and a configurable number of grace logins

3.12	The application must support the ability to disable / remove / delete a user, after a number of days of inactivity, the number of days should be configurable
3.13	The application must not allow the re-use of a past password until a set number of password changes have been made. Parameterize this to allow flexibility in adjusting this value as required
3.14	The application must be flexible and enforce a minimum password length of 8 characters
3.15	The application must enforce the usage of strong alphanumeric passwords
3.16	Default / developer passwords should not reside within the application
3.17	No identification and authentication information must be hard-coded or scripted into the application
3.18	The application must provide last logon information
3.19	Backward process flows must clear all authentication fields
3.2	The application must support time-based access control
3.21	Login failure measures must not indicate which component of the username/password pair submitted was incorrect
3.22	During password changes the application must force the user to enter the new password twice
3.23	The application must support Multi Factor Authentication with at least 3 factors to choose from (OTP, TOTP, Mail)
3.24	The application should support Single Sign On at a minimum through Identity Directories for Non-Revenue systems
4	**Authorization and Access Control**
4.1	The application must support an additive access model which means by default no access is granted
4.2	Access control must be granular to facilitate adequate separation of duties, for example:
	· There should be separation of duties e.g. data entry, authorisation and final approval
	· Data entry staff should have the minimum access levels required to enter data
	· Authorisation staff should have an access level that allows them to authorise but not necessarily change the data that was entered
	· Final approval staff should have the required access level to finalise the process/transaction
4.3	Access control information should be securely stored and must be secure from unauthorized changes within and outside of the application
4.4	Reporting on all the access permissions per user must be available in the application
4.5	User must be able to explicitly terminate (logout) a session
5	**Operations**
5.1	Intrusion detection systems must be in place to detect intrusions of production systems that are Internet facing
5.2	Patch management software must be installed and regularly updated on all servers
5.3	Anti-virus software must be installed and regularly updated on all servers
5.4	A formal incidence response process plan should be in place for production systems
6	**Auditing and Monitoring**
6.1	Provision must be in place for application logs
6.2	All application logs must be in a user-friendly readable format and in English

	They should be delimited using space and allow activities to be captured per line of text Each user transaction such as printing, viewing, updates, inserts and other data manipulation should capture to the minimum the date and time, userID, the URL accessed the and source IP & remote IP. They should indicate the parameters passed where possible
6.3	All application logs must be secure from intentional or accidental modification under all circumstances by all users including administrators. Access to the logs must be restricted to authorized users only so as to ensure their integrity
6.4	It should NOT be possible for the Application Audit logs to be suppressed or modified
6.5	All logs must be viewable and printable
6.6	The application must have incident alerting capability e.g. in the event of system violations or when the audit logs are getting full
6.7	All utility or non-standard based access to the application must be captured in the logs
6.8	For all application audit logs, the log files must bear the following information:
	a) User-id
	b) Date & Time of event
	c) The source and remote IP
	d) Type of event / action performed by the user
	e) Module accessed by the user
	f) Success or failure of the event
	g) Source of the event
	h) Before and after values (where applicable, i.e. master files)
	i) Modifications to the application
	j) Account creation, lockouts, modification, or deletion
	k) Modifications of privileges and access controls
	l) Application alerts and error messages
	m) Accesses to sensitive information
	n) URL of the web page(s) accessed by a user for Internet facing applications
	o) Program used to access the system
	p) The userID at the application log should be tracked up to the database logs
6.9	The application must have a logging mechanism to log all transactions and exceptions
6.1	A violation log must exist to track any attempted unauthorized access to the application and should bear the following information:
	a) Particular action intended by the user
	b) Workstation-id or IP address of access
	c) Date & Time of event
6.11	All valid and failed login attempts must be logged with meaningful information that is actionable for investigative purposes if fraud is detected. However, passwords must not be logged
6.12	All password recovery reset attempts must be logged with meaningful information that is actionable for investigative purposes if fraud is detected
6.13	All security policy changes and attempts must be logged
6.14	All user and account management changes and attempts must be logged
6.15	Database audit trails should be present for all dynamic & static tables of interest e.g. Parameter tables, Transaction Tables etc.

6.16	Application logs should be implemented independent of database audit trails for purposes of correlation i.e. application servers should maintain their own application logs separate from database audit trails.
7	**Input – Processing – Output Controls**
7.1	Predictive input / menu based input functionality should be provided where possible, minimizing user interaction
7.2	Error messages should be standard and not provide too much application information eluding to the reason for the error allowing an attacker to deduce effective attack methods
7.3	Copy and paste must not work for data entry especially when authenticating to the application
7.4	All user input parameters must be validated by the server, and must be validated to accept only values pertinent to the values in the field in accordance with the data dictionary
7.5	Any sensitive content sent to the client machine must not be cached, unless encrypted using approved methods. The application is responsible to set the proper directive to cause the client to not cache the sensitive data
7.6	Sensitive information must not be presented to unauthenticated users
7.7	Sensitive information must not be stored in a persistent cookie, or other location on the client computer that does not have enforceable access control mechanisms.
7.8	Highly confidential data must be stored encrypted
7.9	Confidential data that is stored outside the systems that comprise the application must be encrypted by a firm approved method, such as PGP. This includes file shares, ftp servers, and e-mail
7.1	Functions should not be allowed execute on both encrypted and non-encrypted connections. If functions are required to exist on both encrypted and non-encrypted connections, then the user sessions must not be allowed to span both connections
7.11	Sensitive information must not be stored in hidden fields if the application is web-based
7.12	If data is supplied to the application from an authoritative source, the application must not allow users to modify this data
7.13	The application must not use a credential repository of a trust level less than what is required by the application's data
7.14	User credentials in one repository must not be synchronized with any other repositories unless their trust levels are equal
7.15	If an application uses more than one method or credential store for authentication, all methods and stores used must be at the same trust level
7.16	Web based interfaces should use a secure method to transmit data e.g. Using the HTTP POST method instead of the less secure GET method
8	**Cryptographic Key Management**
8.1	Cryptographic functions must be selected from an approved list. Any cryptographic functions used that are not previously approved require an exception
	Recommended algorithms (with minimum bit lengths), in order of preference, are:
	a) Hashing: SHA -512, SHA -256, RIPEMD160.
	b) Symmetric: AES256, AES192, AES128, 3 -DES (168 bits), Blowfish(minimum 128 bits), Twofish (minimum 128 bits), IDEA (128 bits),and RC4 (128 its).
	c) Public key: RSA(minimum 2048 bits) and DSA(minimum 2048 bits), ElGamal (minimum 2048 bits)
8.2	Any use of hashing must be salted. Values used for salting must be protected

8.3	Encryption keys must be protected during transit and while stored in file system
8.4	Encryption keys must not be disclosed to anyone who does not need access to them
8.5	If using public key cryptography, private keys must be protected by a pass-phrase
8.6	Pass-phrases protecting private keys or used as a share d secret with a symmetric key algorithm must be a minimum of 14 characters in length, and contain at least one upper case letter, one lower case letter, and one number
8.7	A key used to decrypt data must not be stored in the same location as data encrypted with the key
8.8	Site certificates must be current and issued by a well-known certificate authority
9	**Documentation**
9.1	A user manual should be developed as part of the application system/module/component documentation
9.2	A technical manual should be developed as part of the application system/module/component documentation
9.3	An online help facility should be present wherever possible and form part of the application system/module/component documentation
9.4	Signed user requirements/specifications document should be present as it forms the basis for the development of a new application or modification of an existing system
9.5	A Data dictionary should be developed as part of the application system/module/component documentation
9.6	A design blue print with data flow or flow chart diagrams should be present as part of the application system/module/component documentation
10	**Other Considerations**
10.1	A facility should exist to allow rolling-back of transactions/actions under special circumstances clearly documented in the user-specifications. There must be audit trail on the roll-back facility
10.2	Applications should be configurable to securely send audit data/Logs to a centralized data store that is external to the Application Server
10.3	Applications should reliably verify a user's identity using defined multi factor authentication techniques, and capable of secure communication with an external KRA E-directory service for centralized management of authorization and authentication of users to access functionality using security groups defined within the directory service
10.4	Applications should support service monitoring by logging all information that is required for effective monitoring of services based on defined service monitoring parameters
10.5	Applications should have a provision for incorporation of biometrics and related biometric solutions. The next generation of application security would be dependent on biometric identification, authorization and authentication of application users.
10.6	Security for People with Disabilities. Design of Applications should have considerations for people living with disabilities. Varied disabilities calls for design of elaborate mechanisms to enable these group of people to amicably, adequately and elaborately interact with applications. For instance, braille enhanced applications would aid the blind in interacting and using the applications in their endeavors.
10.7	The application should inco-operate certified and legitimate digital certificates, which are used to verify that a particular public key (online identity). A PKI is a technical infrastructure that comprises of a Root Certification Authority (RCA) and a Certification Authority (CA), referred to as an Electronic Certification Service Provider (E-CSP) in Kenya's legal and regulatory framework. The generation and usage of the PKIs on an application should be provisioned by the National Public Key Infrastructure for global trust and recognition.

10.8	Personal Identification data(Information) is to be kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected; and. Personal data shall not be transferred or shared outside the application unless there is proof of adequate data protection safeguards or consent from the data subject. The guidelines for this subject matter are provided by the Kenya Cyber Security Act on Personal Identifiable Information (PII).Ensure the rules of data integrity, confidentiality and availability are adequately adhered to.