KENYA REVENUE AUTHORITY

ISO 9001:2015 CERTIFIED

Terms of Reference

Image Analysis using Artificial Intelligence (AI) and Machine Learning (ML)

Tulipe Ushuru, Tujitegemee!

(1) - EXECUTIVE SUMMARY

The Kenya Revenue Authority (KRA) faces significant risks to revenue collection and national security arising from widespread tax evasion, cargo mis-declaration, and concealment of contraband. These practices undermine customs compliance and expose the country to serious security threats.

To effectively mitigate these challenges, KRA proposes the deployment of an advanced Artificial Intelligence (AI) and Machine Learning (ML)-powered solution that revolutionizes cargo inspection processes.

The system will automate and substantially enhance the accuracy of non-intrusive scanner image analysis and risk profiling. This technology-driven approach will enable consistent and reliable detection of non-compliant cargo, accurately identify false declarations to safeguard government revenue, and facilitate early detection of concealed prohibited or dangerous goods, thereby strengthening border security.

The proposed investment will deliver measurable improvements in customs compliance, ensure more predictable and protected revenue streams, and contribute to significantly safer national borders.

(2) - BACKGROUND

The Kenya Revenue Authority (KRA) faces significant challenges in addressing issues such as under-declaration, misdeclaration, and concealment of goods within cargo shipments. These challenges directly impact the Authority's ability to collect accurate revenue, as dishonest practices by importers and exporters result in significant tax evasion.

Additionally, the concealment of goods poses serious safety and security risks. Hidden contraband, such as illegal drugs, weapons, or hazardous materials, can threaten public safety and national security. The inability to detect such items effectively compromises border control efforts and exposes Kenya to potential harm.

KRA seeks to leverage on Artificial Intelligence (AI) and Machine Learning (ML) to revolutionize cargo scanner image analysis and risk assessment, enabling the revenue administration to automate, enhance the detection of suspicious items and analysis of images with greater accuracy and efficiency.

By doing so, the Authority will safeguard revenue streams, ensure compliance, and strengthen national security.

(3) - OBJECTIVES

1. To **enhance customs inspection capabilities** by integrating image interpretation with risk assessment to effectively identify high-risk cargo and prevent revenue leakage, mitigate safety and security threats.
2. To develop an **AI-driven image processing system** to detect and identify instances of under declaration, misdeclaration, and concealment in cargo shipments.
3. To develop an AI-powered image processing system capable of **automatically detecting** prohibited and restricted items.
4. To develop an AI system that will generate performance, predictive and trends analysis **reports**.
5. To implement a comprehensive solution that integrates AI-driven technologies with existing cargo and unit scanner systems.

(4) - EXPECTED BENEFITS

1. Enhanced revenue collection through consistent and accurate detection of high-risk cargo.
2. Reduced human error in the detection of prohibited and restricted items in cargo thereby mitigating safety and security threats.
3. Enhanced dynamic reporting to generate meaningful trends, patterns and insights to improve detection of fraudulent transactions.
4. Transparency, accountability and faster clearance of cargo and units through automation.
5. Easy interoperability and integration with authorities' existing ICT infrastructure.

(5) - EXPECTED DELIVERABLES

AI - Powered Image Analysis System Features

1. Features Extraction, Object Identification and Classification

The system is able to automatically pre-process the image, conduct feature engineering based on texture, shapes, orientation, patterns, pixels of the image, compare these with the known pre-trained textures, shapes, patterns, pixels of historical images evaluate and predict out comes. The system has descriptive abilities to detect objects in the image and provide accurate classification.

2. Automatic Image Comparison

Deep learning comparative capabilities to identify similarities or differences in scanner images based on density, shapes and patterns. Evaluate outcomes and detect inconsistencies based on classification.

3. Integration with Risk Analysis Engines

The available risk engines will be enhanced with AI capabilities in order to obtain real time transaction level risk ranking which will be integrated with the AI Image analysis solution to predict outcomes and detect risky transactions.

4. Human Interactive Interface

The system will provide support to the secondary analyst by availing a dynamic chatbot that evaluates predefined and random information from risk analysis and image analysis and provide text feedback. The system will also provide a summary of risk indicators identified in relation to every transaction.

5. Alerts Management

The system will have capability for alerts management including detection, alerts generation, communication & feedback for both AI-generated and human-generated alerts.

6. Knowledge Based Training Platform

The system will accumulate data, annotate, augment, and enable algorithms development, AI model training, testing, validation and deployment to accommodate user changes based on trends and risk patterns.

7. Reporting

The system will have the ability to generate dynamic reports for the business functions using AI highlighting trends, patterns, anomaly detection, and image and data parameters.

8. Data Collection and Preprocessing:

- Collect and curate a diverse dataset of images relevant to the project. These include but not limited to the KRA systems (Customs & Border Control (C&BC) systems, Domestic Tax systems, other systems including Data Warehouse, etc), Internet, Partner Government Agency (PGA) Sytems, Trading Partner Systems e.g. Customs-to-Customs Electronic Data Exchange through Trade Logistics Information Pipeline (TLIP), etc).
- Perform data preprocessing tasks such as image resizing, normalization, and augmentation to enhance the quality and diversity of the dataset.
- Annotate images with labels for supervised learning tasks.

9. **Model Development and Training:**
   - Select appropriate AI and ML algorithms for image analysis tasks e.g., convolutional neural networks, object detection models.
   - Develop and train models using the preprocessed dataset.
   - Perform hyperparameter tuning and model optimization to improve performance.

10. **System Integration and Deployment:**
   - Integrate the trained models into the existing infrastructure
   - Implement APIs and interfaces for seamless interaction with other systems and applications.
   - Guide on deployment of the system in a production environment, ensuring scalability and reliability.

11. **Documentation and Reporting:**
   - Create comprehensive documentation, including user manuals, technical specifications, and maintenance guides.
   - Generate regular reports on system performance, usage statistics, and any issues encountered.

12. **Testing and Validation:**
   - Conduct rigorous testing to evaluate the performance and accuracy of the image analysis system.
   - Validate the system against predefined metrics and benchmarks.
   - Perform user acceptance testing (UAT) to ensure the system meets stakeholder expectations.

(6) - SCOPE OF WORK

The expected scope of the work will be as follows:

1. Supply, delivery, installation and commissioning of an AI/ML solution for Image Analysis and Image Comparison (for the Image Sharing Solution). The solution shall have a fully fledged risk profiling and valuation engine to enhance image analysis.

2. Monitoring and Maintenance:
   - Implement monitoring tools to track the system's performance and detect anomalies.
   - Develop a maintenance plan for regular updates, bug fixes, and performance improvements.

- Provide ongoing support and training for users and administrators.
- Maintenance and support of both the software for the AI/ML solution for a period of three (3) years.

3. Integration with KRA systems including the Scanning Systems, Customs, PGA systems, Regional Systems, Trading Partner Systems, Third Party Systems, etc.
4. User training.
5. Capacity building for support staff.
6. Proof of Concept (A working proof of concept shall be mandatory and part of the evaluation criteria).

(7) - LEGAL 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.

#	Section	Bidder's Response
	The bidder to provide evidence of registration/incorporation. Foreign firms should comply with the Companies Act 2015 Section 975.	
	A well-established firm with a good record of accomplishment of AI Solutions and advisory services.	
	Must have very strong knowledge of national and international law /regulatory requirements, standards and practices relating to information sharing, privacy and security.	

#	Section	Bidder's Response
	The legal and professional status of the consultant in form of a certificate of registration, current licenses and any other testimonials for ease of reference.	
	The solution delivery should include manufacturer product training at an Original Equipment Manufacturer (OEM)-authorized facility by an OEM-authorized trainer. Provide the functional and technical training proposal/details for the proposed solution including training materials to be offered. This should include but not limited to user/analyst training, support, system administration/ configuration training, and use of any provided APIs etc.	
	(Note: Training delivery is required to be done based on the number of classes and not number of participants. 20 classes of 20 participants each for each level as detailed below). • Detailed functional training plan for at least 200 business users (entry-level to expert training) • Detailed technical training plan for at least 50 technical users (entry-level to expert training *NB: bidders are advised to provide Substantive explanation, which articulates clearly how they shall carry out the training*.	
	Warranty Bidder is required to provide solution warranty of at least 1 year	
	Support Maintenance Bidder is supposed to provide a 3 years post warranty support and maintenance including manufacturer, premier technical support (support 24*7*365)	
	Implementation and knowledge transfer	

#	Section	Bidder's Response
	Bidders are advised to provide a commitment letter that they will be able to transfer the knowledge and train KRA staff	
	Solution Architecture and a description of how the solution works. Bidders are required to provide details of the solution proposed including product name, brand, version, solution OEM and all the components that will form part of the solution. Additionally, bidders are required to provide detailed solution architecture and description on how the proposed solution works.	
	Currency Tendering and Payment should be made in Kenya Shillings (KSH) inclusive of all the applicable taxes.	

(8) - IMPLEMENTATION TEAM AND RESPONSIBILITIES

1. **Project Manager**
   - Provide overall project leadership, planning, scheduling, and coordination.
   - Manage scope, timelines, budget, risks, and stakeholder communication.
   - Facilitate team alignment, decision-making, and escalation of issues.
   - Ensure compliance with governance processes and project reporting requirements.
2. **Lead Business Analyst**
   - Lead requirements gathering, documentation, and validation with business stakeholders.
   - Define functional and non-functional requirements for the AI/ML image analysis solution.
   - Facilitate process mapping, user journey definition, and business rules clarification.
   - Support UAT planning and ensure delivery aligns to business needs.

3. **Lead Architect**
    - Design the target AI/ML solution architecture, including data pipelines, integration points, and deployment models.
    - Ensure architectural alignment with enterprise standards, security, and scalability requirements.
    - Guide technology selection (ML frameworks, cloud platforms, storage, compute, APIs).
    - Oversee architectural compliance and technical risk mitigation.
4. **Lead Developer**
    - Lead the development of the AI/ML models, backend components, data processing logic, and APIs.
    - Implement coding standards, version control, CI/CD, and model deployment practices.
    - Collaborate with the architect to ensure the technical design is correctly implemented.
    - Support defect resolution, technical testing, and performance optimization.
5. **Quality Assurance Lead**
    - Define the testing strategy for the AI/ML pipeline, including functional, non-functional, and model performance testing.
    - Develop test plans, test cases, and acceptance criteria for both software and ML model outputs.
    - Coordinate and execute system testing, regression testing, and UAT.
    - Verify that the solution meets accuracy, reliability, safety, and compliance standards.

(9) - IMPLEMENTATION SCHEDULE WORKPLAN

Description	Duration
Implementation Period	18 months
Warranty Period	12 months (1 year)
Maintenance and Support Period	36 months (3 years)

(10) - TECHNICAL REQUIREMENTS

Instructions to Bidders

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.

- **Stage One:** Bidder Qualifications and technical requirements. A bidder MUST provide a response to ALL the requirements and also attain an score of at least 75% to be considered successful to proceed to the next stage.
- **Stage Two**: Presentation/Demo: A bidder MUST attain a score of at least 75% be considered successful.

A. BIDDER QUALIFICATION

Bidders MUST provide a substantive response for all features irrespective of any attached technical documents. **Use of Yes, No, tick, compliant etc. will be considered non-responsive**. (Bidders to provide their responses in the table format below.)

No	Requirement Description	Maximum score
	Firm's Experience At least three (3) years' Experience in Image Analysis using AI and ML. 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 Three (3) years ***(3 marks)***	**6**

No	Requirement Description	Maximum score
	1-3 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 (1.5 Mark), ii) Completion certificate or Recommendation letter from client (1.5 mark) References required should be for sites where the bidder or its partners in the tender implemented the solution.	
	Project Team	
	<u>Personnel's Qualifications and Experience</u> Bidder is required to provide a responsibility matrix and profiles of delivery leads (Project Manager, Lead Business Analyst, Lead Architect, Lead Developer and Quality Assurance 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**

No	Requirement Description	Maximum score
	For each lead the scoring will be as follows per lead (At least for the following roles (Project Manager, Lead Business Analyst, Lead Architect, Lead Developer(s) and Quality Assurance Lead) – 5 Leads to be evaluated) Detailed CV demonstrating lead(s) having worked in a successful Image Analysis using AI and ML project implementation in the proposed role **Project Manager** a) Lead (Project Manager) with relevant qualification i. Degree in Computer Science/ Artificial Intelligence/ Data Science or other related field (2 Marks) (attach certificate) ii. Diploma in Computer Science/ Artificial Intelligence/ Data Science 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) i. Above 5 years – 2 marks ii. 1 to 5 years – 1 mark	**6**
	Business Analyst a) Lead with relevant qualification i. Degree in Computer Science/ Artificial Intelligence/ Data Science or other related field (2 Marks) (attach certificate) ii. Diploma in Computer Science/ Artificial Intelligence/ Data Science or other related field (1 Mark) (attach	**6**

No	Requirement Description	Maximum score
	certificate) b) The Lead must have certification in Certified Business Analysis Professional (CBAP) or any other similar/related course. (Must attach copy of certificate) – 2 marks c) Must have a minimum of five (5) years' experience in Business Analysis (Must provide detailed and signed CV) i. Above 5 years – 2 marks ii. 1 to 5 years – 1 mark	
	Lead Architect a) Lead with relevant qualification i. Degree in Computer Science/ Artificial Intelligence/ Data Science or other related field (2 Marks) (attach certificate) ii. Diploma Computer Science/ Artificial Intelligence/ Data Science or other related field (1 Mark) (attach certificate) b) The Lead must have relevant AI industry certifications. (Must attach copy of certificate) – 2 marks c) Must have a minimum of two (2) years' experience in AI technical skills (Must provide detailed and signed CV) i. Above 5 years – 2 marks ii. 2 to 5 years – 1 mark	**6**

No	Requirement Description	Maximum score
	Lead Developer a) Lead with relevant qualification i. Degree in Computer Science/ Artificial Intelligence/ Data Science or other related field (2 Marks) (attach certificate) ii. Diploma in Computer Science/ Artificial Intelligence/ Data Science or other related field (1 Mark) (attach certificate) b) The Lead must have certification in either: i. Python ii. R (for statistical computing & data science) iii. Java, C++, or Julia iv. JavaScript (for AI in web applications, TensorFlow.js) (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) i. 5 years and above – 2 marks ii. Below 5 years – 0 mark	**6**
	Quality Assurance Lead a) Lead with relevant qualification i. Degree in Computer Science/ Artificial Intelligence/ Data Science or other related field (2 Marks) (attach certificate) ii. Diploma in Computer Science/ Artificial Intelligence/ Data Science 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 in Project Management (Must provide detailed and signed CV)	**6**

No	Requirement Description	Maximum score
	i. 5 years and above – 2 marks ii. Below 5 years – 0 mark	
	Total	**36**
	Cut off	**27**

B. TECHNICAL REQUIREMENTS/SPECIFICATIONS
B.1 CRITICAL REQUIREMENTS

Functionality Requirements and Technical 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 and each score multiplied by the requirement weight (score * weight).

Evaluation Criteria	
Compliance	**Score**
Not Provided	0
Provided but requires customization by bidder/third party. Bidder shall bear the cost of the customization.	1
Offered by third party. **Bidder shall bear the cost of third-party products and services**	2
Provided out of the box	3

Clearly mark the appropriate box using a cross (X). If a bidder indicates the response for a particular requirement in more that one column (e.g. "Provided by third party" & "Provided out of the box") the one with the lower score will be used. Responses to requirements need to be substantiated/explained/articulated demonstrate how solution meets the requirement.
Use of Yes, No or compliant, including the use of ticks without substantive narrative explanations in these tables is considered non-responsive.

Bidder SHOULD cross-reference technical response to corresponding data sheets or product technical documentation for product features and

capabilities. **Where a bidder indicates a 3rd party, the bidder should provide a list of components that the 3rd party will implement. Product version (KRA requires the latest stable enterprise version as at the time of Tender submission**.)

No	Feature	Weight	Not Provided	Provided but requires customization by bidder/third party. Bidder shall bear the cost of the customization.	Offered by third party. Bidder shall bear the cost of third-party products and services	Provided out of the box	Explain/Substantiate NB: Data Sheet is mandatory
1	**High level User Requirements**						
	Features Extraction, Object Identification and Classification The system should be able to automatically pre-process the image, conduct feature engineering based on texture, shapes, orientation, patterns, pixels of the image, compare these with the known pre-trained textures, shapes, patterns, pixels of historical images evaluate and predict out comes. The system has descriptive abilities to detect objects in the image and provide accurate classification.	3					
	Automatic Image Comparison The system should have deep learning comparative capabilities to identify similarities or differences in scanner images based on density, shapes and patterns. Evaluate outcomes and detect inconsistencies based on classification.	3					
		3					

	Integration with Risk Analysis Engines The available risk engines will be enhanced with AI capabilities in order to obtain real time transaction level risk ranking which will be integrated with the AI Image analysis solution to predict outcomes and detect risky transactions.						
	Human Interactive Interface The system should provide support to the secondary analyst by availing a dynamic chatbot that evaluates predefined and random information from risk analysis and image analysis and provide text feedback. The system will also provide a summary of risk indicators identified in relation to every transaction.	**3**					
	Alerts Management The system should have capability for alerts management including detection, alerts generation, communication & feedback for both AI-generated and human-generated alerts.	**3**					
	Knowledge Based Training Platform The system should accumulate data, annotate, augment, enable algorithms development, AI model training, testing, validation and deployment to accommodate user changes based on trends and risk patterns	**3**					
	Reporting The system should have the ability to generate dynamic reports for the business functions using AI highlighting trends, patterns, anomaly detection, image and data parameters.	**3**					

2	**Business Requirements/Capabilities**						
	Detect and flag Mis-declaration (weights, quantity, Country of Origin)	**3**					
	Detect and flag Mis-classification	**3**					
	Detect and flag Concealment	**3**					
	Detect and flag counterfeit and prohibited items	**3**					
	Analysis of x-ray scanner image	**3**					
	Classification of goods upon automated analysis of x-ray scanner image	**3**					
	Analysis of scanned or uploaded documents such as invoices through Optical character recognition	**3**					
	Mis-valuation (Over/Undervaluation)	**3**					
	Price comparison of declared value with reference prices	**3**					
	Customs Valuation using historic data	**3**					
	Entity Details Extraction, Identification and Profiling	**3**					
	Digital Shipment Vetting and Classification	**3**					
	Predictive analysis and reporting	**3**					
	pre-arrival analysis	**3**					
	post audit analysis	**3**					
	Automated Identification, examination and analysis of trader and risk transactions	**3**					
	Recommended action to resolve identified risks	**3**					
	Trade pattern algorithm	**3**					
	Trend analysis	**3**					
	Analysis of Cargo Inspections	**3**					

	Identification of inconsistencies of data in related transaction documents for import, exports, transit and transhipment consignments	**3**					
	Management and annotation of stream of commercial data for compliance with regulatory requirements	**3**					
	Automated reconciliation of manifested/declared weight vs. the weighbridge (actual) weight	**3**					
	Automated reconciliation of weight of transit goods at the point of entry vis-à-vis the weight at the exit point	**3**					
	Automated Stock reconciliation from the point of landing to know -the movement of stocks from port to other customs stations -categorization of cargo as to imports, transits, empties, transhipments, export, re-exports etc. -balances at any given time and point per customs station (entered or unentered per the above categories) -number of vessels expected (14 days list)	**3**					
	Automated container/cargo tallying/tracing	**3**					
3	**Feature: General Requirements**						
	Dashboard Reports. The system should allow an officer to generate, view and print customizable report (s).	**3**					
	System should have a user friendly interface	**3**					
	System should provide an audit trail for all the transactions	**3**					
	System should allow for Natural language processing on declaration	**3**					

	System should have self-supervised learning models	**3**					
	System should have valuation standard that complies with customs valuation methods	**3**					
	System should regularly refreshed price database from multiple sources including government and large-scale logistics	**3**					
	System should be capable of fraud detection	**3**					

B.2 SECURITY 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 and each score multiplied by the requirement weight (score * weight).

Evaluation Criteria	
Compliance	**Score**
Not Provided	0
Provided but requires customization by bidder/third party. Bidder shall bear the cost of the customization.	1
Offered by third party. **Bidder shall bear the cost of third-party products and services**	2
Provided out of the box	3

Clearly mark the appropriate box using a cross (X). If a bidder indicates the response for a particular requirement in more that one column (e.g. “Provided by third party” & “Provided out of the box”) the one with the lower score will be used. Responses to requirements need to be substantiated/explained/articulated demonstrate how solution meets the requirement.

Use of Yes, No or compliant, including the use of ticks without substantive narrative explanations in these tables is considered non-responsive.

Bidder SHOULD cross-reference technical response to corresponding data sheets or product technical documentation for product features and capabilities. **Where a bidder indicates a 3rd party, the bidder should provide a list of components that the 3rd party will implement. Product version (KRA requires the latest stable enterprise version as at the time of Tender submission**.)

No	Feature	Security Requirement	Weight	Not Provided	Provided but requires customization by bidder/third party. Bidder shall bear the cost of the customization	Offered by third party. Bidder shall bear the cost of third-party products and services	Provided out of the box	Explain/Substantiate NB: Data Sheet is mandatory
High Level Security Requirements								
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.	3					
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					
3	**Auditing and Logging**	Comprehensive audit trails must be maintained for all system activities, enabling traceability and	3					

		accountability. Ensure the logs are in a format that is consumable by Security information and event management (SIEM) system.						
4	**Incident Response**	An effective incident response plan must be established by the vendor to address security breaches or incidents promptly and minimize impact.	3					
5	**Data Integrity**	Mechanisms must be in place to ensure the integrity of data, including checksums, digital signatures, and blockchain technology where applicable.	3					
6	**Continuous Monitoring**	The system must have continuous monitoring capabilities to detect and respond to security threats in real-time.	3					
7	**Security Training**	Vendors must provide security training for system users and administrators to foster a culture of security awareness.	3					
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.	3					
9	**Authentication**	No identification and authentication information must be hard-coded or scripted into the application.	3					

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 test cases.	3					

B.3 NON-FUNCTIONALITY 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 and each score multiplied by the requirement weight (score * weight).

Evaluation Criteria	
Compliance	**Score**
Not Provided	0
Provided but requires customization by bidder/third party. Bidder shall bear the cost of the customization.	1
Offered by third party. **Bidder shall bear the cost of third-party products and services**	2
Provided out of the box	3

Clearly mark the appropriate box using a cross (X). If a bidder indicates the response for a particular requirement in more that one column (e.g. "Provided by third party" & "Provided out of the box") the one with the lower score will be used. Responses to requirements need to be substantiated/explained/articulated demonstrate how solution meets the requirement. Use of Yes, No or compliant, including the use of ticks without substantive narrative explanations in these tables is considered non-responsive. Bidder SHOULD cross-reference technical response to corresponding data sheets or product technical documentation for product features and capabilities. **Where a bidder indicates a 3rd party, the**

bidder should provide a list of components that the 3rd party will implement.
Product version (KRA requires the latest stable enterprise version as at the time of Tender submission.)

No	Feature: Technical Requirements	Weight	Not Provided	Provided but requires customization by bidder/third party. Bidder shall bear the cost of the customization	Offered by third party. Bidder shall bear the cost of third-party products and services	Provided out of the box	Explain/Substantiate NB: Data Sheet is mandatory
1.	**Data Integration Capabilities:** a) Ability to ingest and process (curate, label and annotate stream of commerce data) data from multiple sources (e.g., import/export declarations, shipping manifests, x-ray cargo scanner, cargo monitoring, invoice data). b) Support for various data formats (structured, semi-structured, unstructured). c) Full data sharing capabilities and open architecture that allows installation in multiple location	3					
2.	**Advanced Analytics and Algorithms:** a) Implementation of robust machine learning algorithms for: i. Predictive analytics, ii. Fraud detection, such as: • Analysis of various documentations used in the cargo clearance processes for inconsistencies • Analysis of cargo inspections iii. Hs Classification.	3					

No	Feature: Technical Requirements	Weight	Not Provided	Provided but requires customization by bidder/third party. Bidder shall bear the cost of the customization	Offered by third party. Bidder shall bear the cost of third-party products and services	Provided out of the box	Explain/Substantiate NB: Data Sheet is mandatory
	b) Use of AI techniques for analysing text-based data and computer vision for image analysis.						
3.	**Scalability and Performance:** a) Solutions should be scalable to handle increasing volumes of data and transactions. b) High-performance computing capabilities to ensure real-time or near-real-time processing.	3					
4.	**Data Security and Privacy:** a) Compliance with data protection regulations and standards. b) Implementation of strong encryption and access control measures to safeguard sensitive information.	3					
5.	**Interoperability:** a) Seamless integration with existing customs IT systems and other government agencies' databases. b) Use of standard APIs and protocols for communication and data exchange.	3					
6.	**User Interface and Reporting:** a) Intuitive and user-friendly dashboards and interfaces for customs officers. b) Advanced reporting tools to generate insights and analytics for decision-making	3					

No	Feature: Technical Requirements	Weight	Not Provided	Provided but requires customization by bidder/third party. Bidder shall bear the cost of the customization	Offered by third party. Bidder shall bear the cost of third-party products and services	Provided out of the box	Explain/Substantiate NB: Data Sheet is mandatory
	c) Dashboard with management reports						
7.	**Sustainability** a) To ensure full transparency and long-term sustainability of our software solutions, we require that the successful bidder during the procurement phase shall surrender the complete and uncompiled source code to us upon delivery, rather than placing it in escrow. This requirement is critical to guarantee our ability to modify, enhance, and maintain the software independently, ensuring that we are not dependent on the vendor for future updates or troubleshooting. By obtaining direct access to the source code, we can safeguard our operations against potential vendor insolvency, contractual disputes, or any other circumstances that might impede our ability to access or utilize the software effectively. b) Minimum maintenance cost	2					
8.	Platform independent a) Solution should be accessed through mobile platform b) Solution should not be restricted to specific operating systems	3					
9.	Workflow a) Solution should have the capability to manage processes in a workflow	2					

No	Feature: Technical Requirements	Weight	Not Provided	Provided but requires customization by bidder/third party. Bidder shall bear the cost of the customization	Offered by third party. Bidder shall bear the cost of third-party products and services	Provided out of the box	Explain/Substantiate NB: Data Sheet is mandatory
	b) b) Solution should give visibility to structured workflow and queue management						
10.	**Data Processing Speed:** The efficiency and speed at which the AI/ML solution can process and analyse large volumes of data.	3					
11.	**Data Quality Management:** a) The capability of the system to handle inconsistencies, missing data, and ensure data integrity across various sources. b) Data should be compliant with WCO and WTO standards	3					

C. PRESENTATION/DEMO (POC)

Bidders who are successful in stage one will be invited for a live presentation/demo that will form additional assessment of the solution capabilities and vendor experience. The live demo will include real time analysis of a select set of scanner images from the Kenyan scanners. The different available methodologies of sharing the images with the bidder shall be defined in the bidder's response. The most appropriate method shall be selected by KRA during the evaluation process. Notwithstanding the stated methodologies, the final Demo Scenarios shall be decided by KRA and shared through email to the bidders who qualify after stage 3 of the technical evaluation.

Demo Evaluation Criteria

	COMPONENT	REQUIREMENT	EXPECTED OUTPUT	MARKS	BIDDER'S RESPONSE
1.	**Introduction** Overview of the solution's purpose and goals.	• Outline the scenarios covered by the solution. Demonstrate AI techniques used (NLP, computer vision, machine learning).	Demonstrate an understanding of AI/ML techniques	2	
2.	**AI/ ML construction** and algorithm maintenance	• Demonstrate how the system can label different kinds of data (text, images, scanner images etc.), show how a user can provide feedback to improve the AI and use real-time data from online trading platforms to continuously update and maintain the AI.	Show integrated annotation, user feedback loop and export of outputs for algorithm re-training	5	
3.	**Data Handling and Quality** Structured & Unstructured Data:	***Sources:*** Data sources (customs manifest, IDF, Declarations, scanned invoices/documents, x-ray scanner images etc.)	**Data Quality Algorithm:** Demonstrate the algorithm used for data cleaning and enrichment. Show before-and-after states of data cleaning for both text and image data. Demonstrate robustness of collecting data using OCR from scanned documents and	2	

	COMPONENT	REQUIREMENT	EXPECTED OUTPUT	MARKS	BIDDER'S RESPONSE
			handwritten documents.		
4.	**Analysis, Risk ranking & Predictive analytics** for Importer/ Exporter/ Declarant/ cargo type/ Analysis	***Linking Activities:*** *Data Aggregation*: Collect and aggregate data from multiple sources. *Link Analysis*: Demonstrate how the AI links entities and types of goods to identify patterns of smuggling.	• Case study showing how suspicious activities are traced back to specific entities and type of goods. • Risk ranking of importers/ exporters/declarants'/ type of goods and demonstrate the targeting capabilities	3	
5.	**Mis-declaration Detection** For potential tax evasion or smuggling.	***Algorithms for Mis-declaration:*** a) *Text Analysis:* NLP techniques to detect inconsistencies in quantity, weight, origin, and description.	Highlight discrepancies in a sample declaration.	2	
		b) *Image Analysis*: Computer vision to verify document integrity.	Show detection of altered documents.	1	
		c) Automated X-ray image analysis	• Show detection of an item not declared/ mis-declared by marking the area with	5	

	COMPONENT	REQUIREMENT	EXPECTED OUTPUT	MARKS	BIDDER'S RESPONSE
			multiple visual aids.		
			• Demonstrate atlease 5 multiple algorithms for identifying mis-declaration, fraud in a scanned container/ cargo – (Each algorithm will be score one mark)	5	
		d) *Text Analysis:* NLP techniques to detect inconsistencies in quantity, weight, origin, and description.	• Highlight discrepancies in a sample declaration.	1	
		e) *Image Analysis*: Computer vision to verify document (invoice, certificates etc) integrity.	• Show detection of altered documents.	1	
6.	**Automated Data Analysis for Fraud Detection**	Demonstrate analysis for each document type: Manifest, BL, IDF, Invoice, Declaration, Certificates, tracking seal, container number, truck registration (text and image): and assess data for inconsistency which may indicate fraud or mistakes consignment	Data Mismatch/Inconsistency: Algorithms to detect fraud or errors. • Present a scenario where inconsistencies are flagged.	5	
7.	**Valuation Assessment**	AI Techniques: Describe the methods used for	Show a valuation assessment case	5	

	COMPONENT	REQUIREMENT	EXPECTED OUTPUT	MARKS	BIDDER'S RESPONSE
		undervaluation/overvaluation detection.	with AI predictions vs. actual values using standard valuation methods.		
8.	**Smuggling and Contraband Detection**	Demonstrate Analysis & Evidence: Illicit Goods: Detect smuggling of goods/humans/illicit/ illegal goods/ contrabands in cargo scanner images	Case study with detected concealments and supporting evidence.	5	
			Demonstrate at lease 5 multiple algorithms for identifying smuggling and contrabands in a scanned container/ cargo – (Each algorithm will be score one mark)	5	
9.	**Mis-classification Detection**	Using text	HS Classification: AI model for correct HS code classification using text.	3	
		Using X-ray Scanner Image	HS Classification: analysis of scanner images and automated recommendation for HS classification.	5	
			Comparison of manual vs. AI classification	5	

	COMPONENT	REQUIREMENT	EXPECTED OUTPUT	MARKS	BIDDER'S RESPONSE
			results of an x-ray cargo image analysis.		
			Tampering Detection: Analyse scanner images for signs of tampering and demonstrate detection of altered images.	5	
			Demonstrate marking of x-ray images for immutability	5	
10.	**Automated Comparison of Scanner Images**	Image Consistency: Entry vs. Exit Analysis: Compare images from different ports/release stations.	Scenario demonstrating automated detection of mismatches in x-ray image details at entry and exit point.	5	
			Scenario demonstrating automated detection of mismatches in container number details at entry and exit point.	5	
			Scenario demonstrating automated detection of mismatches in truck registration	5	

	COMPONENT	REQUIREMENT	EXPECTED OUTPUT	MARKS	BIDDER'S RESPONSE
			details (including stuffing and density analysis at entry and exit point.		
11.	**Truck Scanner Analysis**	Smuggling Link: Cab/Chassis Analysis: Identify patterns linking trucks to smuggling activities. Identify smuggling in the scanner image	Show a case where truck analysis led to smuggling detection.	2	
12.	**Cargo Monitoring and Tracking**	Location Analysis: Dumping Locations: Use tracking data to identify suspicious dumping locations	Demonstrate tracking data analysis and incidence scene location identification.	2	
		Automated RECTS Alert Analysis and intervention	Ability to Receive, Categorize, interpret and escalate cargo tracking alerts	2	
		Weights Analysis: Through integration with Kenya National Highways Authority (KENHA) and Regional Cargo Tracking System (RECTS)	Compare weight at initial release with the weigh at exit/flag out inconsistencies	2	
		Automated Transit Cargo reconciliation, issuance of	Mirror entry and exit data and flag	2	

	COMPONENT	REQUIREMENT	EXPECTED OUTPUT	MARKS	BIDDER'S RESPONSE
		Certificate of Export (CoE) and bonds cancellation	out inconsistencies		
13.	**Queue And Shipment Management**	Customizable Filters: Inspection Management: Demonstrate queue and shipment management system.	Show how inspections are prioritized, and decisions are captured transparently.	2	
14.	**Interactive Dashboards**	Visualization and Reporting: • Trend Analysis: Interactive dashboards showing trends over time. • Predictive Analysis: Predict future smuggling activities or inconsistencies. • Secure Reports: Generate immutable, tamper-proof reports. • Shipment management with full risk areas visualization • Trader management with customizable filters, investigation capability features	Walkthrough of dashboard features and a sample report	3	
Total Marks				**100**	
Cut off				**75**	

Note:

The vendor must achieve 75%, which translates to a numerical cut-off of 75 points (100 x 0.75).

KENYA REVENUE AUTHORITY

ISO 9001:2015 CERTIFIED

SUMMARY OF THE EVALUATION CRITERIA AND THE CUT-OFF SCORES.

Technical evaluation of bidder responses will be carried out in Two (2) stages:

- **Stage One:** Bidder Qualifications and technical requirements. A bidder MUST provide a response to ALL the requirements and also attain an score of at least 75% (60 out of 80) to be considered successful to proceed to the next stage.
- **Stage Two**: Presentation/Demo: A bidder MUST attain a score of at least 75% (75 out of 100) be considered successful.

#	Section	Cut-off Score	Maximum Score
Stage 1	a. Bidder Qualifications b. Technical Requirements (C.1, C.2 and C.3) *(The mark scored by a bidder out of 579 shall be prorated to a mark out of 80)*	60 (75%)	80
Stage 2	**Presentation/Demo**		
	Presentation/Demo *(The mark scored by a bidder out of 100 shall be prorated to a mark out of 20)*	15 (75%)	20
	TOTAL TECHNICAL EVALUATION SCORE	**85**	**100**

(11) - PRICE SCHEDULE

All quoted amounts shall be in Kenyan shillings

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

KENYA REVENUE AUTHORITY

ISO 9001:2015 CERTIFIED

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

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

4.1	Ensure that the responses from the API provide only legimate requested data that is not excessive.
4.2	Ensure sensitive information such as access tokens, bearer tokens, pins, passwords etc are not being returned in request responses or stored in logs in clear text.
4.3	Error messages must ensure that sensitive information about the integrating systems is not disclosed
4.4	Ensure sensitive data parameters such as passwords, PINs, Credit card numbers etc. being passed to the APIs are hashed
4.5	Ensure minimization/masking of customer PII such as MSISDN and ID Numbers when such are returned in request responses and displayed in logs.
4.6	Ensure the communication channel is encrypted. The Endpoints should make use of HTTPS and not of HTTP
4.7	Ensure proper implementation of HTTPS; i.e current secure TLSV
5	**Resource and Rate Limiting**
5.1	Ensure implementation of a limit on how often a client can call the API within a defined timeframe. This helps mitigate DoS attacks by throttling or blocking IP addresses after making concurrent requests within a very short period of time.
5.2	Define and enforce maximum size of data on all incoming parameters and payloads such as maximum length for strings and maximum number of elements in arrays.
5.3	For APIs processing large amounts of data, ensure data is processed asynchronously. Processing large amounts of data synchronously can prevent the API from responding in a timely manner forcing clients to wait.
6	**Secure Configuration**
6.1	Ensure implementation of the **X-Content-Type-Options: nosniff** header to protect API against MIME sniffing vulnerabilities.
6.2	Ensure implementation of the **X-Frame-Options: deny** header.
6.3	Ensure implementation of the **Content-Security-Policy: default-src 'none'** header.
6.4	Ensure that fingerprinting headers such as **X-Powered-By**, **Server**, **X-AspNet-Version**, etc are not present
6.5	Force content-type for your response. If you return application/json, then your content-type response is application/json.
6.6	Return the proper status code according to the operation completed. (e.g. 200 OK, 400 Bad Request, 401 Unauthorized, 405 Method Not Allowed, etc.).
7	**Vulnerability Management**
7.1	Ensure that the API supports use of updated and vendor supported dependencies and libraries.
7.2	If the API is externally facing, ensure that it's behind a Firewall
7.3	Ensure that unused dependencies, unnecessary features, components, files, and documentation are deleted in production APIs
8	**Data/Input Validation**
8.1	Perform data validation using a single, trustworthy and actively maintained library.
8.2	Validate, filter and sanitize all client-provided data, or other data coming from integrated systems.
8.3	Special characters should be escaped using the specific syntax for the target interpreter.
8.4	Prefer a safe API that provides a parameterized interface.
8.5	Always limit the number of returned records to prevent mass disclosure in case of injection.

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

	ANNEX II - Application Security Requirements
1	**Application Architecture**
1.1	Applications hosted in a shared hosting environment should be logically isolated from other applications in the same environment
1.2	Anti-virus scanning must be performed real-time on any file transmitted to the server
1.3	All network communications between components must be authenticated, and must not explicitly trust other network devices

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

2.11	Sessions must not be allowed to span both secure and non-secure connections
2.12	Applications must allocate session-based resources only after successful authentication. Allocating resources prior to this can lead to denial of service attacks, session fixation attacks, and others
2.13	Synchronization of time between servers and other relevant equipment must be implemented. This is instrumental in tracking time stamps between different systems particularly where systems share/exchange data
3	**Identification and Authentication**
3.1	Each user must be authenticated with a unique user-id and password on the application
3.2	User authentication data must be stored and maintained securely in a centralized location on the system
3.3	The application must support password expiry features with a configurable frequency. Parameterize this to allow flexibility in adjusting this value as required
3.4	The password must be secure on entry, at no point must the password be in clear text
3.5	All new user accounts must have a system-generated random password when created. A secure way of communicating the initial password to the user should be utilized e.g. via KRA e-mail account
3.6	All new user accounts must be created with reference to existing authoritative databases of approved persons e.g. identifying numbers in KRA's active staff database (HR) and National PIN certificate database
3.7	Users must be prompted to change their passwords the first time they log on to the application
3.8	Newly created accounts should be set to expire if not used for a configurable period of time. Parameterize this to allow flexibility in adjusting this value as required
3.9	The application must support password lockout after a configurable number of unsuccessful attempts. Parameterize this to allow flexibility in adjusting this value as required
3.1	The application must lockout a user account after the system is idle for a configurable period of time. Parameterize this to allow flexibility in adjusting this value as required
3.11	The application must support a password change notification and a configurable number of grace logins
3.12	The application must support the ability to disable / remove / delete a user, after a number of days of inactivity, the number of days should be configurable
3.13	The application must not allow the re-use of a past password until a set number of password changes have been made. Parameterize this to allow flexibility in adjusting this value as required
3.14	The application must be flexible and enforce a minimum password length of 8 characters
3.15	The application must enforce the usage of strong alphanumeric passwords
3.16	Default / developer passwords should not reside within the application
3.17	No identification and authentication information must be hard-coded or scripted into the application
3.18	The application must provide last logon information
3.19	Backward process flows must clear all authentication fields
3.2	The application must support time-based access control
3.21	Login failure measures must not indicate which component of the username/password pair submitted was incorrect
3.22	During password changes the application must force the user to enter the new password twice
3.23	The application must support Multi Factor Authentication with at least 3 factors to choose from (OTP, TOTP, Mail)

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

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

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

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