KENYA REVENUE AUTHORITY

ISO 9001:2015 CERTIFIED

Technical Specification for Procurement of Governance Risk & Compliance (GRC) Solution with Embedded Business Continuity Management and Enterprise Risk Management Solution.

KENYA REVENUE AUTHORITY

ISO 9001:2015 CERTIFIED

Technical Specification for Procurement of Governance Risk & Compliance (GRC) Solution with Embedded Business Continuity Management and Enterprise Risk Management Solution.

1.1 Executive Summary

The Authority implemented an on-premise Business Continuity Management Solution (BCMS), Recovery Pro Planner RPX Business Continuity Management Software (BCMS) product.

Mitratech, the software manufacturer, acquired the Recovery Planner RPX BCMS software and has advised customers using RPX to expedite commencement of the process of migration a new on cloud platform.

The Authority is therefore seeking to procure a Governance Risk & Compliance (GRC) solution incorporating Business Continuity Management and Enterprise Risk Management Solution.

1.2 Purpose

The purpose of this document is to provide a comprehensive specification for procuring, deploying, or upgrading the Business Continuity Management Solution and Enterprise Risk Management Solution to systematically prepare for, respond to, and recover from disruptions, minimizing downtime, financial loss, and reputational damage by centralizing plans, automating alerts, managing incidents, ensuring communication, and providing real-time insights, essentially turning chaotic plans into actionable, resilient operations.

1.3 Scope

The solution will serve over **12,000 KRA staff** across headquarters, regional offices, and border stations, and will provide an integrated platform for managing service recovering following a disaster.

1.4 Objectives

Minimizes Downtime & Losses: Automates responses and workflows, allowing teams to act faster and restore operations quicker, preventing significant revenue loss.

Centralizes & Organizes Plans: Moves plans from documents to a system, integrating data and providing live reporting, making them accessible and scalable.

Enhances Communication: Facilitates rapid alerts and information sharing with employees, customers, and stakeholders during a crisis, building trust.

Automates Tasks & Alerts: Triggers actions, assigns responsibilities, and sends mass notifications automatically, reducing manual effort.

Provides Real-Time Insights: Offers dashboards and data visualization for monitoring performance, identifying risks, and making informed decisions.

Builds Employee Confidence: Ensures staff know their roles during a crisis, improving their ability to handle both major disruptions and everyday issues.

Ensures Compliance & Resilience: Helps meet industry standards (like ISO 22301) and builds overall organizational resilience against various threats (cyber, natural, operational).

Technical Response Checklist for Business Continuity Management Solution

The following Checklist is provided to help the vendor organize and consistently present its technical bid. **For each of the technical requirements, the bidder must describe how its technical bid responds to the requirements.**

In addition, the vendor must provide cross references to the relevant supporting information, if any, included in the bid. The cross reference should identify the relevant document(s) and page number(s). The cross reference should be indicated in the column "DETAILED DESCRIPTION".

The Technical Response Checklist does not supersede the rest of the technical requirements (or any other part of the bidding documents). If a requirement is not mentioned in the Checklist that does not relieve the vendor from the responsibility of including supporting evidence of compliance with that other requirement in its technical bid. One- or two-word responses (e.g. "Yes," "No,", "Will comply," etc.) are not enough to confirm technical responsiveness with Technical Requirements.

Vendors should use the following options to indicate the "DEGREE OF COMPLIANCE" their solution provides for each of items listed in this section:

- **FS** – (Fully Supported) the application fully supports the requirement without any modifications.
- **PS** – (Partially Supported) the application supports the requirement with use of a workaround.
- **CR** – (Customization required) the application will be customized to meet the requirement(s).
- **NS** – (Not Supported) the system is not capable of supporting the requirement and cannot be modified to accommodate the requirement.

Where customizations are required, clearly and comprehensively indicate the plan, design and/or approach to be undertaken to achieve the requirements.

A clause-by-clause commentary on the Technical Specifications demonstrating substantial response of the goods and service to those specifications, or a statement of deviations and exceptions to the provisions of the Technical Specifications is required

For each SPECIFICATION, vendors are requested to provide a clear and concise explanation in the DETAILED DESCRIPTION section or provide a cross-reference to where that explanation or supporting information can be found in other parts of the technical proposal.

Please fill in the COMPLIANCE column as appropriate to indicate one of the responses listed above for each item and add as many comments, diagrams, maps and/or screenshots in the DETAILED DESCRIPTION column.

Blanks on the COMPLIANCE and DETAILED DESCRIPTION columns will be assumed that the functionality is Not Available.

1.0 System Functional Requirements

#	Item	Minimum Requirement	Degree of Compliance FS/PS/CR/NS	Vendor Response
	Software Product Requirement			
	Compliance with Domain Area International Standards	Tl1e system must deliver BCM functions in conformance to ISO 22301:2012		
	Work Operations Environment Module:			
	The user should be able to;			
	Record recovery resources	The System Should include a resource file to document recovery resources.		
	Record personnel/staff details including the following:	System should be able to accommodate or allow addition of required personnel details as per Human Resource requirements		
	Record locations/sites of the organization	The system accommodates Locations and Sites		
	Record the organizational structure 'departments, sub-departments Record Files/documents	The System should support KRA organization units such as Department, Division, Section, unit, sub-units etc.		

	Record Files/documents	The System should have a repository to synch or store documents and files uploaded into the system Bidder to state what is the expected storage to be provided.		
	Record customized recovery resource records	The system should allow for customizable fields that can be reportable and searchable.		
	Record customized personnel/staff records	The system should provide capability to create custom files for personnel details that can be reportable and searchable.		
	Record locations/site records	The system should provide capability to create custom locations/sites that can be reportable and searchable		
	Customization of the organizational structure (departments, sub-departments records	The system should provide capability to create custom Departments that can be reportable and searchable		
	Business Impact Analysis Module			
	Record Business Impact Analysis (BIA)	The system should provide BIA that allows for the management of functions (or processes). performed, incorporating all the relevant information. The system should provide a worksheet area which allows for the depiction of what will be recovered, when it will be recovered, and details about the people and resources necessary for the recovery. The system should allow for update of all of this information directly within each page, or through an incorporated BIA wizard. The wizard provides a guide through the BIA process which can be utilized by personnel of any background/experience such as a department manager		
	Record customized BIA parameters	The System should allow for Custom fields be used within the BIA		
	Record BIA results	The system should provide for a BIA worksheet area which allows for the depiction of what will be recovered, when it will be recovered, and details about the people and resources necessary for the recovery. All of this information should be updated directly within each page, or through		

		an incorporated BIA wizard. The wizard should provide a guide through the BIA process which can be utilized by personnel of any background/experience such as a department manager.		
	Record BIA resource dependencies	The system should be capable of capturing Resource upstream and downstream dependencies within the BIA		
	Risk Management Module			
	Record Risk Assessment (RA)	The system should provide Risk Assessment functionality that allows for determination of threats and includes functionality to quantify the effects and mitigation steps. for each. It should provide Survey functionality that is built in to allow for questions to be sent to specific recipients. The Risk survey should be open to enable non registered system users to respond. The system should present the survey questions in an email format and answers captured made available centrally in the system.		
	Record customized RA parameters	The System should allow for creation of Custom fields within the Risk Assessment.		
	Record customized risk computation formula	The system should allow for customization of the risk formula is customizable used for risk evaluation		
	Record customized BIA parameters	The System should provide capability to customize BIA parameters		
	Generate customizable RA templates	The System should provide Risk Assessment templates can be reused and customized whenever required.		
	Support collaboration of risk assessors from within the risk assessment process	The System should have capability to email Risk Assessment questionnaires to assessors for completion without a need to a registered system user.		
	Business Continuity Plan Development and access Module			
	Upload/download excel/word-processed documents into/from the BCM software	The system should provide capability for uploading or downloading Word/Excel Documents to generation customizable plans		
	Editing of a business continuity plan document within the BCM Software	The System should enable full editing capabilities within the business continuity Plan document.		

	Assembly/de-assembly of system components necessary to create/modify a business continuity Piano	The system should provide capability for assigning/unassigning necessary resources for recovery required to update business continuity plans. Further, the content of the downloaded business continuity plan can be customized.		
	Record incident type-specific/scenario contingency plans within a business continuity plan	The system should allow for documentation of Scenarios within plans and teams can be associated to each scenario.		
	Support for standardization of plans	The System should allow for the development of plan templates. The content within these templates should be linkable to actual plans so that the update in one place would be mirrored everywhere that content has been linked. This provides standardization of plans across the organization. Our flexible structure allows for plans & templates to address locations, departments, and resources. A plan typically contains informational areas, specific scenarios which are addressed, and teams which address specific circumstances.		
	Creation and management of activity (test, maintenance etc) schedules and workflows	The system should have a default schedule can be applied for plan updates, reviews, and tests. At the plan level specific schedules can be applied. When the schedule becomes due an alert is created, an optional email can be sent, and the plan's status would change, escalation is supported if no action was taken. The details of the update, review, and separate test schedules can be automatically included within a plan appendix. Reports are available to isolate gaps in any of these schedules. Gap analysis is also available to return threats which have been assessed and other items which require plans, for which no plans have been associated. Summary reports are available within the Reports area of the system a wide range of prebuilt reports are available and these include summary reports and dashboard views of the data. Filters used on reports can be saved so that views can be easily recalled.		

		Program administration is configurable within the system. This encompasses areas such as terminology, navigation, email verbiage, security, and other global settings from the System Configuration area. There are features within the system that support program administration such as plan update, review, and test schedules. Alerts and optional emails c□11 be distributed to ensure awareness of due dates and timeframes. An escalation option can be used to send notices if timeframes are not met. Workflows can be designed consisting of one or many people and/or levels. The system engages those involved through optional emails and a system alert. Workflows can be applied to an entire plan or to any of the pieces which comprise the plan changed since the last review.		
	Tracking and reporting on plan revisions	Markup and revision information is displayed to highlight the original text, modified text (with markup\, and a final version. Functionality is included which can display all changes to the plan over time, who performed the changes, and the specifics of any change. Collaboration is also supported through plan update review, and test schedules. For plan reviews the system highlights areas of the Plan which have changed since the last review.		
	Addition of plan dependencies	The System allows for the definition of inter-dependencies between resources (assets) and functions (processes). These can be used to track the inter-dependencies between hardware, software, and the business functions they support. Mapping is available graphically to show dependencies across organizational structures. Resources can be defined to plans and their dependencies are automatically attached.		

	Attachment of files to a business continuity plan	The system should allow for attachment of Files to a business continuity plan		
	Conversion of a BCM software-based business continuity plan to a PC-based document	The system should allow plans to be exported into word, pdf, rtf documents. In addition, a zipped bundle can be downloaded containing attached files olona with plan documents.		
	Dynamic generation of a business continuity plan as needed, with support for customization of plan contents	The System should allow Business Continuity plans to generated on demand with selection options for user to customize content of the plans.		
	Distribution of business continuity plans	The system should allow for distribution of Business Continuity plans to anyone as desired.		
	Access to business continuity plans during an incident	The system should allow for association of business plans as part of incident documentation.		
	Support for plan testing/exercising	As part of Incident management, the system should allow for the activation of teams, the coordination of tasks, the notification of recipients, and oversight over multiple incidents or exercises. The System should provide capability for tracking of incidents in terms of incidents resolution progress, how complete they are, and when they are expected to be resolved. Exceptions which occur, outside of the planned details should be highlighted to assist in the post mortem review of incidents or exercises. Teams can be planned for ahead of time or created within the context of an incident which is underway. Each plan should contain multiple scenarios which may occur and multiple teams can be assigned to each scenario. This should therefore allow for incident management at the plan, scenario, and at a specific team level. Teams also support precedence with tasks which can be dependent on tasks within other teams. Automation is in place to assist with the activation of		

		tasks, the distribution of specific tasks to individual team members, and the notification of groups of recipients. Process development is supported by tasks/responsibilities on teams, and complimented with Goon/ charts that show precedence. Teams identify roles and notification lists can be attached to a plan already or created ad hoc at time of incident, Graphics and diagrams con be supported as attachments to plans, teams and tasks, or within the incident itself.		
	Notifications/Alerts to personnel Module			
	Generate and automate sending of notifications to staff	The system should provide capability to generate and send notifications to staff in real time or via scheduling.		
	Support for a variety of communication devices/channels	The system should have capability to send messages via e-mail and e-mail-to-SMS Texting.		
	Record acknowledgement/tracking of notification receipt	The system should have capability to maintain a record and enable reporting of acknowledgement and tracking of notification receipt.		
	To automatically generate and send plan maintenance schedule reminders	The system should support program administration such as plan update, review, and test schedules. Alerts and optional emails should be supported to ensure distribution and awareness of due dates and timeframes. An escalation option should be used to send notices if timeframes are not met. Workflows can be designed consisting of one or many people and/or levels. The system engages those involved through optional emails and a system alert. Workflows can be applied to an entire plan or to any of the pieces which comprise the plan chanced since the last review		
	Record Service Provider/vendor contract notifications	The system should have capability to document and track Service provider/vendor contract notifications.		
	Record plan maintenance and testing/exercising	As part of Incident management, the system should allow for the activation of teams, the coordination of tasks, the notification of recipients, and oversight over multiple incidents or exercises.		

		The system should provide capability to assist with the activation of tasks, the distribution of specific tasks to individual team members, and the notification of groups of recipients.		
	Incident Management Module			
	Visual incident communications & reporting facility	The system should have dashboards and other reports for the incident management process.		
	Real time incident tracking, logging and management	The system should have capability to track, log and manage incidents in real time		
	Business continuity plan activation	As part of incident management, the system should provide capability for the user to activate one or more plans.		
	Record Incident audit trail	The System should provide an un-editable incident log used to track important information during an incident for audit purposes.		
	Assignment of/changes to team members/teams in an ongoing incident	The system should allow for changes in membership of Teams and tasks during an incident.		
	Creation of ad-hoc teams at the time of/during an incident	The system should provide capability to create Teams on the fly as needed during an incident.		
	Collaboration and Workflows support Module			
	Record sending of email to users	The system should provide capability for presenting Reminders and messages upon to the user log-in.		
	Record and create To-Do lists	The system should provide capability for creating To-Do Lists		
	Record and color code revisions	The system should have a mechanism for Revisions to differentiate original and revised text.		
	Record and create Message Boards/virtual notice boards	The system should provide facility for Message boards for sharing information between users.		
	Record and create workflows	The system should provide Workflows capability including approvals of plan revisions can be set-up and throughout the system.		
	Record and display Gantt chart of a team's recovery tasks	System should provide for automatic generated Gantt charts for team task schedules.		
	Reporting and Analysis function Module			

	Record comprehensive list of standard reports	The system should provide extensive built in reporting capability is built into RPX with a capability to create customized reports. Some highly utilized reports are: Gap Analysis, Resource Interdependency, Department Details, Contract Reports, Objects Updated, Login, etc.		
	Record customized standard reports	The system should provide capability to define custom reports using simple pull-down menus and requires no programming skills. The report should be downloadable in Excel and accessible programmatically via our Web Service API.		
	Record What-if analysis	The system should provide a virtual command center from which • plans and notifications can be managed. • Functionality to create teams, manage existing ones, • allow for activation of plans, • monitoring of the progress, and • provides methods in which tasks can be flagged for improvement. • Notifications are centrally managed to assist with direct, two-way, communications between administrators, teams. and across multiple plans. A scenario analysis feature, which provides "What If" modeling		
	Record and generate Customizable system-wide dashboard	The system should provide capability to customize Dashboards to be displayed on the screen and through reports.		
	Management of personnel, supply chain and BCPs Module			
	Flexible (centralized or distributed) management of personnel, vendor/supply chain and business continuity plans	The system should be able to support flexible management of personnel, vendor/supply chain and business continuity.		
	Compliance, Audit and Benchmarking module			

	Record Audit and compliance with BCM policies	The system should support key BCM frameworks, such as DRII, BS25999, ISO22301 and ISO27002 required to document Business Continuity Program activity as per industry standards and regulations		
	Record compliance with regulatory requirements and BCM standard	RPX supports key BCM frameworks, such as DRII, BS25999, ISO22301 and ISO27002. The RPX Compliance area allows you document your Business Continuity Program activity to industry standards and regulations for the construction of comprehensive audits. A library of preformatted Compliance templates for common industry standards/regulations, such as BS25999, ISO22301, DRII, NFPA 1600, NIMS, FDIC, and FFIEC is included. The system allows for new standard templates to be added by the client and provides hot links to other global standards web sites for convenient reference.		
	Usability/Training Requirements			
	The system must be structured in such a way as to be understood by a novice user within a short period	The system should focus on ease of use, and addressing all components of the BCM lifecycle, compliance and best practices concerns while remaining customer centric and responsive by providing; • intuitive interface allowing for use of the variety of easily accessible options, such as drop down menus, etc. • common look and feel across modules, • Documentation such as help pages and context sensitive help		
	Volume & Storage Requirements			
	The system must address optimal storage capability as necessary and implement relevant compression strategy. System must support	The system should be capable of supporting an employee base of approximately 10,000 employees while accommodating hundreds of plans, manuals, diagrams user guides etc.		

	compression to allow large amounts of data transfers over any network medium for efficiency and economizing	The bidder should disclose applicable constraints and/costs applicable		
	Compatibility Requirements			
	The system should be a N-Tier Web based system and provide seamless integration with KRA's existing Mail Server system for automated reminders as well as other systems	The system should support 3 Tier architecture that is scalable when required i.e. 3 tier system with Web Server, App Server, and Database Server tiers.		
	The system modules should have the capability of being enhanced or modified with minimal impact to other interfacing modules	The system should be customizable to reflect corporate branding and information requirements		
	Reliability Requirements			
	The system should be able to recover data and should be able to roll back	The system should be able to support high availability configurations that ensures that backup volumes can be replicated across multiple sites		
	Error logging - the system will have comprehensive error handling routines. The error description should be logged to aid system developers in tracing and solving the error	The system should implement a variety of error codes and logs if clients come across errors while using the system to assist in troubleshooting		
	Availability Requirements			
	The system shall be capable of running 24 x 7 continuously with minimal downtime	The bidder should provide system should guaranteed 24/7 availability		
	The average response times for interactive transactions should be less than 2 seconds	The System should have a maximum of 2 seconds response time		
	Legal Requirements			

	Warranty and support provision (including online support, knowledge-bases, upgrades and releases) must be provided	The bidder should specify warranty and support provisions included with the purchase		

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

1.1 Vendor Evaluation

#	Description	Score
1	**Firms Experience** The bidder shall state the number of years of experience in Business Continuity Management (BCM) software implementation. At least 3 years but less than 5 years – 4 Marks At least 2 years but less than 3 years – 2 Marks Less than 2 years – 0 Marks	4
2	**BCM Planning and Training Experience** The bidder shall state the number of years of experience in **BCM planning and training**. • At least 3 years but less than 5 years – 4 Marks • At least 2 years but less than 3 years – 2 Marks • Less than 2 years – 0 Marks	4
3	**BCM Consultants** **a) BCM Consultants Qualifications** The bidder shall propose at least two (2) BCM planning consultants holding recognized BCM qualifications. (CVs and copies of certificates must be attached.) • BCM Professional Certification – 1 Mark per consultant • CV for BCM Consultant – 2 Marks per consultant **b) Academic Qualifications of Proposed Technical Personnel** The bidder shall propose three (3) technical personnel/staff with the following minimum qualifications: • University Degree – 2 Marks per staff • Diploma – 1 Mark per staff **c) Experience of Senior Consultant / Team Leader** State the number of years of **BCM planning experience** possessed by the proposed Senior Consultant/Team Leader. • At least 3 years but less than 5 years – 4 Marks • At least 2 years but less than 3 years – 2 Marks • Less than 2 years – 0 Marks	16
4	**Project Management** The bidder shall briefly describe the project management expertise available within the proposed team and the approach to be adopted. **a. Project Management Certification** (3 Marks) **b. Project Management Experience:** At least 3 years but less than 5 years – 4 Marks At least 2 years but less than 3 years – 2 Marks Less than 2 years – 0 Marks	10

#	Description	Score
	c. Project Team Structure Provide a chart outlining the recommended BCM project team organization – 3 Marks	
5	**Reference Sites** The bidder shall provide details of **at least two (2) reference organizations** where the proposed BCM software has been successfully implemented and is operational. The company should have a proven track record in this domain and preferably have executed projects of similar scale for large organizations or government agencies. • Provide two (2) LSOs or Contracts for similar assignment undertaken successfully (3 marks each) • Provide at least two (2) corresponding reference letters confirming that the bidder successfully carried out the project (7.5 marks each) Reference letter should have (full contacts; postal address, telephone and email)	21
6	**Manufacturer Partnership** Provide evidence of Partnership level from the Manufacturer. This is to ensure the bidder is an authorized implementation partner for the proposed solution	8
7	**Support and Local Presence:** The vendor should be able to provide support framework available for the product for KRA stating Service Levels to be provided. • Local presence Support Escalation (5 Marks) • OEM Support Escalation (5 Marks) The Service Level Requirements would be discussed and mutually agreed	10
	Maximum Score	73
	Cut Off Scores	**55**

2 Technical Requirement for the Enterprise Risk Management Solution

2.1 Background

The reforms being undertaken in the Authority under its Revenue Administration Reforms and Modernization Programme as part of the wider public service reforms have identified the need for more effective corporate governance framework in the public sector. Key amongst this is the adoption of Enterprise Risk Management (ERM), to provide a basis for management to effectively deal with the uncertainties and the associated risks.

KRA has an ongoing programme of implementation of ERM based on ISO 31000 International Standard -Risk Management Principles and Guidelines. The Authority intends to engage a firm to supply and install an appropriate state-of-the art Enterprise Risk Management (ERM) software platform and provide other related services necessary for a successful ERM implementation.

Specifically, the software is intended to automate the following Enterprise Risk Management processes for greater efficiency;

1. Risk and Control Self-Assessment (RCSA) procedures and workflows which include the following;

    a) Identification and recording of risks
    b) Quantitative Risk Assessments based on Likelihood and Consequence
    c) Capturing of both inherent and residual risks
    d) Identification of existing and proposed controls related to each risk
    e) Evaluation of control effectiveness
    f) Built in RCSA scheduling

ii. Incident reporting that will allow staff and Business Units within the Authority to capture and report on incidents, breaches, losses, complaints and control failures, including anonymous reporting of incidents. The system must allow for analysis of the incidents to determine the root cause, controls that failed if any and have ability to reference back to the RCSA.

iii. Tracking and reporting on key risk and control indicators (KRIs). These will act as early warning signals by providing the capability to indicate existence of predefined risk factors that will allow the Authority to take proactive action.

iv. Tracking of risk reduction activities including person responsible, timeframes for resolution and status of proposed actions

v. Mapping and tracking of compliance to legal and regulatory requirements

vi. Generation of dashboards, heat maps and scorecards to support decision making.

1.1 Objectives

The objectives of the automation assignment will include but not limited to:

g) Supply, delivery, installation and commissioning of ERM software
h) Undertake capacity building on the ERM software through training and knowledge transfer.
i) Undertake capacity building on Enterprise Risk Management.
j) Carry out operational risk assessment for the various business processes of KRA

1.2 Scope of the Assignment

The successful firm will be required to familiarize themselves with the Authority's strategic plan including the vision, mission, core mandate, goals, objectives and departmental work plans and undertake the following:

a) Supply, delivery, installation and commissioning of Enterprise Risk Management software.

Supply and installation of the hardware platform is not in the scope of this assignment but bidders are required to provide the recommended hardware and system software specification for the successful implementation of their proposed software at KRA.

- Customize the ERM software to automate the Authority's Enterprise Risk Management process as outlined in the Authority's Risk Management Policy and Framework.
- Provide administrator and end-user training on the ERM software.
- Develop and document an ERM system user's manual
- Work with the Authority throughout the full cycle of ERM software implementation.
- Undertake a post ERM software implementation review.

1.3 Deliverables

The minimum expected deliverables of the assignment are as follows:

- An Enterprise Risk Management System that is hosted and operated on a state-of-art ICT platform which includes modules for the ERM framework tools, namely;
  - Risk and Control Self-Assessment (RCSA) module
  - Key Risk Indicators (KRIs) module
  - Compliance attestation module (for key controls and legal & regulatory compliance monitoring)
  - Action tracking module for monitoring progress in implementation of control improvement actions
  - Incidence recording and management module with capabilities for post incidence analysis
- ERM process deliverables, including:
  - Automated Risk Registers (with identified and assessed risks and KRIs, Identified key controls, Compliance attestation questions and identified improvement actions) for a minimum of 20 business units/ processes in the Authority, to be derived from RCSAs conducted using the software
  - Automated Incidence registers for a minimum of 20 business units/ processes
  - Automated Risk heat maps and dashboards for a minimum of 20 business units/ processes
  - Automated Key Risk Indicators (KRIs) dashboards for a minimum of 20 business units/ processes

- Automated Compliance Monitoring Framework with key controls and legal/regulatory requirements to be monitored for a minimum of 20 business units/ processes
- Automated Improvement Action Tracking dashboards indicating desired control improvements for a minimum of 20 business units/ processes.
- Review the ERM policies and give recommendations for improvement as necessary.

➢ Software end-user and system administrator training

- Undertake skills assessment and determine the skills gap
- Training curriculum and materials to be based on skills gaps analysis by the vendor/trainer
- Training sessions designed to address the identified skills gaps (KRA will provide training venues/facilities)
  - System administrator training to be provided for 10 system administrators from ICT and the Corporate Risk Management Department
  - System end users training and Operational Risk Management training to be provided to 100 staff
- Training report including skills assessment and training evaluation

➢ ERM system user's manual

➢ Post-ERMS implementation review report.

➢ ERM Software Support and Maintenance for two (2) years, including, software upgrades

1.4 Scope of Usage of the software

The ERM software will be used throughout the Authority for risk management in both the business and support services departments. The software is therefore envisaged to support management of the business risks and operational risks. The key users of the system will therefore be the Risk Management Officers of the various departments/ divisions and regions of the Authority and the Risk Champions appointed at the various sections/ stations of the revenue and support departments. The Authority's Management will also be a key user and consumer of the management reports generated from the system either a user with access rights or recipients of the reports.
It is anticipated that the software will have an incremental usage as more business units and processes undergo risk and control self-assessment (RCSA). The respondents are therefore requested to provide costs based on incremental usage as follows;

i. Cost for 200 users
ii. Cost for 500 users
iii. Cost for 1000 users
iv. Cost for 1,500 users

1.5 Objectives of automation of the ERM process

1. Provide a system that supports the ERM framework operation to ensure adequate management of risks
11. Facilitate effective reporting on risk management to ensure risk-based decision making in the Authority both at the strategic and operational levels.
iii. Provide a medium of monitoring risks through integration with KRA business and support service systems.

1.6 Technical Requirements

2.1.1 Acronyms

1. Authority - Refers to Kenya Revenue Authority
2. RCSA (Risk and Control Self-Assessment) - Refers to the process of identifying, recording and assessing risk exposures and the effectiveness of related controls in mitigating those risks.
3. KRI-Key Risk Indicators
4. Cause and events libraries- Collection of risk causes and events collated into a single repository.
5. ERM-Enterprise Risk Management
6. Full cycle of implementation refers to; supply, delivery, installation, configuration, testing, quality assurance, issue resolution, training, holding RCSA Workshops, commissioning, system warranty and annual maintenance on ERM Software.

The following Checklist is provided to help the vendor organize and consistently present its technical bid. **For each of the technical requirements, the bidder must describe how its technical bid responds to the requirements.**

In addition, the vendor must provide cross references to the relevant supporting information, if any, included in the bid. The cross reference should identify the relevant document(s) and page number(s). The cross reference should be indicated in the column "DETAILED DESCRIPTION".

The Technical Response Checklist does not supersede the rest of the technical requirements (or any other part of the bidding documents). If a requirement is not mentioned in the Checklist that does not relieve the vendor from the responsibility of

including supporting evidence of compliance with that other requirement in its technical bid. One- or two-word responses (e.g. "Yes," "No,", "Will comply," etc.) are not enough to confirm technical responsiveness with Technical Requirements.

Vendors should use the following options to indicate the "DEGREE OF COMPLIANCE" their solution provides for each of items listed in this section:

- **FS** – (Fully Supported) the application fully supports the requirement without any modifications.
- **PS** – (Partially Supported) the application supports the requirement with use of a workaround.
- **CR** – (Customization required) the application will be customized to meet the requirement(s).
- **NS** – (Not Supported) the system is not capable of supporting the requirement and cannot be modified to accommodate the requirement.

Where customizations are required, clearly and comprehensively indicate the plan, design and/or approach to be undertaken to achieve the requirements.

A clause-by-clause commentary on the Technical Specifications demonstrating substantial response of the goods and service to those specifications, or a statement of deviations and exceptions to the provisions of the Technical Specifications is required

For each SPECIFICATION, vendors are requested to provide a clear and concise explanation in the DETAILED DESCRIPTION section or provide a cross-reference to where that explanation or supporting information can be found in other parts of the technical proposal.

Please fill in the COMPLIANCE column as appropriate to indicate one of the responses listed above for each item and add as many comments, diagrams, maps and/or screenshots in the DETAILED DESCRIPTION column.

Blanks on the COMPLIANCE and DETAILED DESCRIPTION columns will be assumed that the functionality is Not Available.

2.1.2 System Functional Requirements

#	Sub functions	Minimum requirements	Degree of Compliance FS/PS/CR/NS	Vendors Response	Pass/Fail
1	System Functional Requirements				
1.1	Risk and Control Self-Assessment (RCSA) Module				
1.1.1	Scheduling of RCSAs	The system must be able to			
		1. Allow scheduling of all business processes to carry out RCSAs			
		2. Assign specific periods for RCSA for individual business units			
		3. Notify users when RCSA are due by sending emails via lotus email for 1st and 2nd reminders prior to due dates of the RCSA			
1.1.2	Linkage of Corporate and Business Unit Objectives to risks	The system must be able to			
		1. Record corporate objectives			
		2. Record the individual objectives of each business unit for up to 100 business units with scalability.			
		3. Link the objectives of the business units to the corporate objectives			
		4. Record critical success factors for achievement of the			
		business unit objectives			
1.1.3	Risk identification and cause, event effect analysis (Bow tie analysis)	The system must be able to			
		1. Record identified inherent risks that exist in each business unit			
		2. Record the causes and effects of the risks			
		3. Amalgamate all identified causes and effects to create a library of causes and effects			
		4. Enable identification of risk causes and effects through drill down to the libraries from the identified risks			
1.1.4	Risk Assessment	The system must be able to			
		1. Record the likelihood and consequence of occurrence of the inherent risk			
		2. Record the likelihood and consequence of occurrence of the residual risk			
		3. Record the ranking of the inherent and residual risks based on the			

#	Sub functions	Minimum requirements	Degree of Compliance FS/PS/CR/NS	Vendors Response	Pass/Fail
		product of the likelihood and consequence			
		4. Classify the risks into High, Medium and Low risks based on the risk rankings with corresponding colour skims (High-Red, Medium-Amber and Low-Green)			
		5. Filter risks above the set desired risk ranking (High and Medium risks)			
		6. Record improvement in controls for risks filtered as High and Medium.			
1.1.5	Evaluation of controls	The system must be able to			
		1. Recording of controls related to each risk -must allow recording of more than one control for each risk			
		2. Compute the control effectiveness as a percentage difference between the inherent and residual risk ranking			
		3. Recording of the desired control effectiveness thresholds			
		4. Filter controls that are below the set desired control effectiveness thresholds			
		5. Record action to be taken on controls filtered as below the desired control effectiveness threshold			
1.2	**Compliance Monitoring Module**				
1.2.1	Control Compliance	The system must be able to			
		1. Filter controls with effectiveness above predetermined thresholds (key controls)			
		2. Record key control ownership			
		3. Record frequency of application for the key control			
		4. Record evidence of key control performance (performance attestation)			
		5. Record evidence of review of the key control for accuracy and completeness			
		6. Generate reports on ownership, frequency and performance of key controls			

#	Sub functions	Minimum requirements	Degree of Compliance FS/PS/CR/NS	Vendors Response	Pass/Fail
		7. Generate reports on key controls without details of ownership,frequency and performance			
		8. Escalate controls without ownership, frequency and evidence of performance to specified users			
1.2.2	Legal and regulatory compliance	The system must be able to			
		1. Record key legislation and regulatory requirements that KRA need to adhere to			
		2. Record responsible officers to attest to/confirm compliance to identified key legislation and regulatory requirements			
		3. Record evidence of compliance to identified key legislation and regulatory requirements			
		4. Record evidence of review of attestation to compliance to identified key legislation and regulatory requirements			
		5. Escalate to predetermined users key legislation and regulatory requirements that have not been attested to at a given point in time and/or over a given period			
		6. Generate reports on key legislation and regulatory requirements that do not have attestation on performance			
1.3	**Key Risk Indicators Module**				
1.3.1	Collection of KRI data	The system must be able to			
		1. Record key risk indicators (KRis)			
		2. Input KRI data by assigned users			
		3. Upload key risk indicator data from KRA business systems (Customs Simba System, Domestic Taxes ITMS and i-Tax and KRA ERP system)			
1.3.2	Analysis of KRIs	The system must be able to			
		1. Record of parameters to allow classification/scaling of KRIs into High-Red, Medium-Amber and Low-Green			

#	Sub functions	Minimum requirements	Degree of Compliance FS/PS/CR/NS	Vendors Response	Pass/Fail
		2. Compare the KRI data to scaling parameters			
1.3.3	Tracking of KRIs	The system must be able to			
		1. Flag out predetermined KRI exceptions (e.g KRis in Red and Amber)			
		2. Send emails via Lotus mail to users for the exceptions			
		3. Record action taken for KRis flagged as red and amber			
		4. Provide reports on KRis trends			
1.4	**Incidence recording and management module**				
1.4.1	Recording of incidences (incidence registers)	The system must be able to record incident details as follows:			
		1. Business area to which the incident relates			
		2. Description of the incident			
		3. Whether the risk is sensitive and should have restricted viewing access			
		4. Cause and Event type category of the incidence			
		5. Whether the incident relates to a larger group of incidents and if so, which group			
		6. The dates the incident started, ended, was identified and reported.			
		7. The nature and size of each incident			
		8. The key control(s) that failed to permit the incident to occur or controls that did not exist and are to be added to the RCSA to mitigate the likelihood of the risk incidence occurring again.			
		9. Suggested improvement to prevent the incident from recurring and to minimise its consequence should it occur, together with a due by date and person responsible			
1.4.2	Tracking of incidences	The system must be able to			
		1. Assign unique reference numbers for each incidence recorded			
		2. Facilitate assignment of action to deal with incidents			

#	Sub functions	Minimum requirements	Degree of Compliance FS/PS/CR/NS	Vendors Response	Pass/Fail
		3. Send notification/ alerts through lotus mail to defined users of recorded incidences and incidences not acted on			
		4. Escalate recorded incidences based on defined parameters			
		5. Facilitate attachment of evidence of incidence in file formats (e.g., PDF, Excel, HTML, XML, CSV, etc.)			
		6. Provide document indexing and search capabilities			
		7. Provide document versioning and archiving			
		8. Provide sufficient document security for attached evidence			
		9. Provide multiple access from various points			
		10. Provide access controls to limit incident recorder to view their incidences alone			
		11. Provide anonymous recording of incidences			
		12. Generate Status reports on incidents			
1.5	**Action tracking module**				
1.5.1	Recording of improvement actions	The system must be able to			
		1. Record suggested control improvements for controls assessed as not effective enough			
		2. Record owners of the control improvements			
		3. Record the due dates for the control improvement			
		4. Record the importance of the agreed improvement in terms of High, Medium and Low			
		5. Record defined actions for High, Medium and Low improvement actions			
		6. Record agreed action plan			
		7. Record employee responsible for implementing the plan			
		8. Record the due by date of the action plan			
1.5.2	Tracking of improvement actions	The system must be able to			

#	Sub functions	Minimum requirements	Degree of Compliance FS/PS/CR/NS	Vendors Response	Pass/Fail
		1. Notify control improvement owners of due dates for control improvement actions			
		2. Escalate outstanding control improvement actions to specified user through Lotus notes email			
		3. Generate reports on overdue control improvement actions at business unit level, department level and corporate level.			
1.6	**Reporting module**				
1.6.1	Risk and Control Self Assessments (RCSA) reports	The system must be able to			
		1. Summary of all RCSAs completed in the month			
		2. Results of RCSAs completed highlighting the top risks in the business unit as well as all high (red) and medium (yellow) risks on a net residual risk basis.			
		3. Have drill down/up mechanism to facilitate viewing of underlying risks, causes and effects for business unit, region, department and corporate risks			
1.6.2	Key Control Compliance	The system must be able to			
		1. Generate a summary of the number of key controls being attested to across the Authority by business unit showing the: □ Total number of key controls □ Number that have and have not been attested to in the month □ Number that have been attested to but with a negative response together with an explanation for the negative response			
		2. Generate dashboard reports for Key Controls that have not attested to or have not been reviewed			
1.6.3	Legislative and compliance	The system must be able to			
		1. Generate a summary of the number of key legislation and regulations being attested to across the Authority by business unit showing the:			

#	Sub functions	Minimum requirements	Degree of Compliance FS/PS/CR/NS	Vendors Response	Pass/Fail
		□ Total number of key legislation and regulations			
		□ Number that have and have not been attested to in the			
		month			
		□ Number that have been attested to but with a negative			
		response together with an explanation for the negative response			
		2. Generate dashboard reports for Key legislations and regulations that have not been attested to or have not been reviewed			
1.6.4	Key Risk Indicators	The system must be able to			
		1. Generate a summary of KRis for each business unit and across the Authority showing all high (red) and medium (yellow) rated KRis together with management comment for follow up action.			
		2. Generate dash board reports for KRis which include KRis in red, amber and green by business units, process and corporate levels, with drill down capability to the basic unit such as business process			
1.6.5	Incidence recording and management	The system must be able to generate a summary of risk incidents by business unit with details of all events that have a consequence in excess of set appetite levels.			
1.6.6	Action Point Tracking	The system must be able to			
		1. Generate a summary of outstanding and overdue action points by business unit.			
		2. Generate dashboard reports for completed improvement actions, actions in progress and overdue improvement actions by department with drill down capability to the basic unit such as business unit or process			
1.6.7	Other reports	The system must be able to			
		1. Generate risk registers for each business units which contain the following fields; Objectives, CSFs, Risk events, Controls, risk assessment and ranking (colour			

#	Sub functions	Minimum requirements	Degree of Compliance FS/PS/CR/NS	Vendors Response	Pass/Fail
		schemed), risk owner, improvement action, KRis, Key controls.			
		2. Generate reports in various formats including word, excel, PDF, power point, graphics e.t.c			
	Maximum Score				
	Cut Off Score				

2.1.3 Other functional requirements

#	Description	Degree of Compliance FS/PS/CR/NS	Vendors Response	Pass/Fail
1.7.1	The vendor must be able to do a practical demonstration of how the software fulfils the requirements 1.1 to 1.6 above at a venue to be determined by the purchaser, prior to award of the tender. The purchaser reserves the right to make site visits to the client referees to confirm the working of the software.			
1.7 .2	The software must be able to support at least 100 concurrent users			
1.7 .3	The software should have 'replica' ability for remote site usability			
1.7.4	The software must have an ad-hoc query builder facility to enable deeper analysis			
1.7.5	The software must have the ability to import/upload/export/download data in PDF, Excel, HTML, XML, CSV formats.			
1.8	**Software Support and Maturity Requirements**			
1.8	**ERM Software Maturity and Support**			
1.8.1	The ERM software must have been in the market and use in various installation(s) for the last three (3) years			
1.8.2	The proportion of the software manufacturer's current technical staff dedicated to the development and support of the proposed ERM software			
1.8.3	Evidence that the bidder is officially authorized by the manufacturer to sell and support the proposed ERM software			
1.8.4	State the number of years the bidder has been providing technical support of the proposed ERM software.			
1.8.5	Brief statement of approach to training of key users and administrators on the ERM Software			

#	Description	Degree of Compliance FS/PS/CR/NS	Vendors Response	Pass/Fail
1.8.6	state the ERM software licensing approach (e.g per user, per module…) and the duration of the licences			
1.8.7	IThe bidder should commit to install the software products in KRA premises. NB: Software as a service will not be acceptable.			
1.8.8	State the intellectual property rights ownership and service level agreements that will apply to the software. I.e. Bidder is required to confirm that client has the right to customise the software.			

2.1.4 System Non-Functional Requirements

#	Category	Minimum Requirement	Degree of Compliance FS/PS/CR/NS	Vendors Response	Pass/Fail
3.1	**Quality Management**	The system must deliver ERM functions in conformance to ISO 9001:2015 and ISO 31000:2009 requirements			
		The system must be web based and must operate in a multi-office organization format, i.e. system must be accessible to all KRA stations countrywide			
3.2	**Usability and Training Requirements**	The system must be structured in such a way as to be understood by a novice user within a short period			
		The system should provide predictive input/ menu based input functionality where possible to minimize user interaction			
		The system should have common look and feel across modules, e.g. common placements of buttons, boxes, choices and even messages so that users are not confused. This will shorten the user learning curve			
		The solution must have adequate documentation that describes at minimum, the design, functionality and use of the system			
3.3	**Volume & Storage Requirements**	The system must address optimal storage capability as necessary and implement relevant compression strategy. System must support compression to allow large amounts of data transfers over any network medium for efficiency and economizing			

#	Category	Minimum Requirement	Degree of Compliance FS/PS/CR/NS	Vendors Response	Pass/Fail
		The system must be able to allow for expanding the disk space			
3.4	**Compatibility Requirements**	The system should be a N-Tier Web based system and provide seamless integration with KRA's existing Mail Server system for automated reminders as well as other systems			
		The system modules must have the capability of being enhanced or modified with minimal impact to other interfacing modules			
		The system must be able to integrate seamlessly with existing KRA business and support systems (Customs Services Simba System, Domestic Taxes ITMS and i-Tax and KRA ERP) and Java applications (swing client, Web clients and EJBs).			
3.5	**Reliability Requirements**	The system must be able to recover data and must be able to rollback			
		Error logging - the system will have comprehensive error handling routines. The error description should be logged to aid system developers in tracing and solving the error			
3.6	**Availability Requirements**	The system shall be capable of running 24 x 7 continuously with minimal downtime			
		The average response times for interactive transactions should be less than 2 seconds			
3.7	**Warranty and Support Requirements**	Warranty and support provision (including online support, knowledge-bases, upgrades and releases) must be provided for at least 1 year and the rate for subsequent annual maintenance (after 1 year) must be specified.			

Vendor Evaluation

1.0	ERM Software Implementation Capability	Max Score
1.1	State the number of years of the ERM software implementation experience that bidder possess. • 3 to 5 years.....2 marks • 2 to below 3 years.....1 marks • Below 2 years.....0 mark	2
1.2	State the number of years the ERM software has been in the market and use in various organizations; • Above 6 years.....5 marks • 2 to below 6 years.....3 marks • Below 2 years..... .....0 mark	2
1.3	**Reference Sites** Provide a list and contacts of at least 3 reference organizations where the proposed solution has been implemented and is in use. The company should have a proven track record in this domain and preferably have executed projects of similar scale for large organizations or government agencies. • Provide three (3) LSOs or Contracts (from the three reference organizations above) for similar assignment undertaken successfully (2 marks for each) • Provide at least three (3) corresponding reference letters confirming that the bidder successfully carried out the project (5 marks each) Reference letter should have (full contacts; postal address, telephone and email)	21
1.4	**ERM Consultants** At least Three (3) No. of the proposed ERM consultants hold recognized Certification on the solution (attach CVs and evidence of qualifications) Product Certification on the Solution (2 Mark for each Consultant) CV for ERM Consultant (1 Mark) The proposed three (3) Technical personnel/ staff to have a minimum of University Degree/Diploma. • University Degree (2 marks) • Diploma (1 marks) • Certificate (0.5 marks) State the number of years of Enterprise Risk Management experience the proposed senior consultant/team leader possesses. • Above 3 years.....4 marks • 2 to below 3 years.....2 marks • Below 2 years.....0 mark	19

1.5	Demonstrate how you intend to meet KRA defined deliverables including associated activities for ERM Software implementation which the bidder is of the view would make this project a success • Defined Project Delivery Methodology (2 Marks) • Defined Project Plan (2 Marks) • Proposed Vendor Project Delivery Team (2 Marks) • Defined Deliverables and clear milestones (4 Marks)	10
1.6	Bidder to state the following as applicable to the solution being proposed • The software licensing approach (4marks) • Software licensing model of the product (4 Marks) • Proposed Service Level Targets to form basis of negotiation (4 Marks)	12
	Maximum Score	**66**
	Cut Off Score	**53**

Solution Demo/ Presentation/Pitch

Bidders who meet the cut off score will be invited for demo/ pitch. The bidders will be guided on the Key areas of focus.

Post Qualification/ Due Diligence

Due diligence/ Reference checks will be conducted as provided in the RFP Document.

FINANCIAL REQUIREMENT

Note: Bidders are required to provide a detailed breakdown of how they arrived at the total cost.