



Kenya National Highways Authority

Quality Highways, Better Connections

HORN OF AFRICA GATEWAY DEVELOPMENT PROJECT (HoAGDP)

PROJECT ID NO. P161305

**TERMS OF REFERENCE FOR CONSULTANCY SERVICES FOR THE
REVIEW OF KENYA NATIONAL HIGHWAYS AUTHORITY'S (KeNHA)
ENVIRONMENT AND SOCIAL SAFEGUARDS MANAGEMENT SYSTEMS,
AND DEVELOPMENT OF DIGITIZATION AND AUTOMATION
REQUIREMENTS**

TENDER NO.: KeNHA/3006/2026

SEPTEMBER 2026

**DIRECTOR HIGHWAY DESIGN & SURVEY
KENYA NATIONAL HIGHWAYS AUTHORITY
P. O. BOX 49712 - 00100
NAIROBI.**

**DIRECTOR GENERAL
KENYA NATIONAL HIGHWAYS
AUTHORITY P.O. BOX 49712 - 00100
NAIROBI.**

TERMS OF REFERENCE FOR CONSULTANCY SERVICES FOR THE REVIEW OF KENYA NATIONAL HIGHWAYS AUTHORITY'S (KENHA) ENVIRONMENT AND SOCIAL SAFEGUARDS MANAGEMENT SYSTEMS, AND DEVELOPMENT OF DIGITIZATION AND AUTOMATION REQUIREMENTS

1. The Client and Name of the assignment

The Government of the Republic of Kenya (hereinafter called “Borrower”) the Ministry of Roads and Transport) has received financing from the International Development Association (IDA) (the “Bank”) in the form of a “credit” (hereinafter called “credit”) toward the cost of the Horn of Africa Gateway Development Project. The Kenya National Highways Authority (KeNHA) is a State Corporation established under the Kenya Roads Act, 2007 with the mandate to manage, develop, rehabilitate, and maintain national trunk roads in Kenya. KeNHA intends to apply a portion of the proceeds of this credit to eligible payments under the contract for the above consultancy services.

In implementing infrastructure projects, KeNHA is required to comply with:

- National environmental and social safeguards legislation and regulations;
- Occupational health and safety requirements;
- Land acquisition and resettlement requirements;
- International financing institutions’ environmental and social safeguards frameworks;
- Stakeholder engagement and grievance management obligations; and
- Climate resilience and sustainability requirements.

KeNHA’s Safeguards Department is responsible for coordinating environmental and social safeguards compliance across the project lifecycle, including planning, design, procurement, construction, operation, and maintenance phases.

Over the years, the scale and complexity of safeguards requirements have increased significantly due to:

- Expansion of the road infrastructure portfolio;
- Multiple financing partners with varying safeguards requirements;
- Increasing public scrutiny and stakeholder engagement expectations;
- Expanded compliance and reporting obligations; and
- Need for timely and reliable safeguards information management.

Currently, several safeguards processes are implemented through manual or semi-manual systems involving spreadsheets, paper-based workflows, fragmented databases, email correspondence, and decentralized reporting mechanisms. These approaches present challenges related to:

- Process inefficiencies;
- Delayed approvals and reporting;
- Data inconsistency and duplication;
- Limited traceability and accountability;

- Weak integration across departments and projects;
- Inadequate analytics and dashboard reporting; and
- Difficulties in real-time monitoring and compliance tracking.

KeNHA therefore intends to engage a qualified consulting firm to undertake a comprehensive review of the operations of the Safeguards Department and develop requirements and recommendations for automation and digitization of safeguards procedures and systems.

This assignment is expected to support institutional strengthening, improved safeguards compliance, enhanced operational efficiency, and establishment of an integrated safeguards management information system.

2. Objective of the Assignment

2.1 Overall Objective

The overall objective of the assignment is to undertake a comprehensive institutional, operational, and systems review of KeNHA's Safeguards Department and develop functional and technical requirements for automation and digitization of safeguards operations.

2.2 Specific Objectives

The specific objectives of the assignment are to:

(i) Review Existing Safeguards Operations

- Assess and document current safeguards operational structures, procedures, workflows, tools, reporting systems, and institutional arrangements.

(ii) Identify Operational and Systems Gaps

- Identify procedural, institutional, technological, operational, and capacity gaps affecting effective safeguards management.

(iii) Assess Automation Opportunities

- Identify safeguards processes and functions suitable for automation and digitization.

(iv) Develop IT and Systems Requirements

- Prepare detailed business, functional, technical, infrastructure, cybersecurity, integration, and implementation requirements for a safeguards automation system. The proposed Environmental, Social, Health and Safety Management System (ESHSMS) should ensure environmental, social, health and safety

commitments and mitigation measures are implemented and re-evaluated throughout the Projects life cycle, meets the national regulations, and applicable Good International Industry Best Practices (GIIBP). Ultimately, the ESHSMS should enable KeNHA to be ISO 14001, ISO 45001 and ISO 26000 compliant.

3. Scope of the Assignment

The Consultant shall carry out all activities necessary to achieve the objectives of the assignment, including but not limited to the tasks outlined below.

Task 1: Inception Phase

3.1.1 Kick-Off Meetings

Identification and mapping of key stakeholders involved in road designs and construction. Document the roles of the key stakeholders in relation to road design and construction.

Conduct inception and consultative meetings with:

- KeNHA senior management;
- Safeguards Department staff;
- ICT Directorate;
- Procurement Directorate
- Finance Directorate
- Legal Directorate
- Engineering Design and Maintenance Departments
- PPP Directorate
- Project implementation teams (Technical Departments); and
- Other relevant stakeholders e.g. Development Partners, National Environment Management Authority (NEMA), National Land Commission (NLC), Directorate of Occupational Safety and Health Services (DOSHS), etc.

3.1.2 Review all relevant documentation including:

- Organizational structure and mandates;
- Existing safeguards manuals and SOPs;
- ESIA, RAP, and compliance management procedures;
- Internal reporting templates and systems;
- ICT policies and architecture documents;
- Existing databases and information systems;
- World Bank and other donor safeguards requirements;
- Relevant Kenyan legislation and regulations.

Task 2: Review and Mapping of Existing Safeguards Operations

The Consultant shall undertake a comprehensive institutional and operational assessment of safeguards functions to establish a clear understanding of the current (“As-Is”) state of safeguards management systems, structures, workflows, and decision-making arrangements.

The exercise shall provide the foundational basis for identifying gaps, inefficiencies, automation opportunities, and future-state redesign.

3.2.1 Institutional Assessment

The Consultant shall assess the institutional framework governing safeguards management, including organizational arrangements, human resources, governance structures, and internal coordination mechanisms.

(a) Organizational Structure

The Consultant shall:

- Review the formal organizational structure of the Safeguards Department and related units;
- Assess alignment between structure and functional mandates;
- Identify structural overlaps, gaps, or misalignment with operational needs;
- Evaluate adequacy of regional and project-level safeguards presence;
- Assess integration between safeguards, engineering, planning, procurement, and implementation units;
- Review escalation structures and authority hierarchies.

(b) Staffing Levels and Competencies

The Consultant shall:

- Assess staffing adequacy relative to project portfolio and workload;
- Evaluate distribution of staff across headquarters, regional offices, and projects;
- Review reliance on consultants and external support;
- Assess skill mix across environmental and social safeguards disciplines;
- Evaluate ICT, data, and digital literacy levels relevant to automation readiness;
- Identify staffing shortages, overcapacity, and skill imbalances.

(c) Roles and Responsibilities

The Consultant shall:

- Review job descriptions and functional mandates;
- Assess clarity and completeness of assigned responsibilities;

- Identify overlapping roles or unclear accountability lines;
- Evaluate segregation of duties and risk management controls;
- Assess role clarity between headquarters, regional offices, and project teams;
- Review contractor and supervision consultant roles in safeguards implementation.

(d) Reporting Lines

The Consultant shall:

- Map formal reporting structures within safeguards operations;
- Assess vertical and horizontal reporting relationships;
- Identify delays or inefficiencies caused by reporting hierarchies;
- Evaluate alignment between technical and administrative reporting lines;
- Assess clarity of escalation pathways for urgent safeguards issues.

(e) Coordination Mechanisms

The Consultant shall assess coordination between safeguards and other institutional actors.

This shall include:

- Coordination between safeguards and engineering/design teams;
- Coordination with procurement and contract management units;
- Coordination with contractors and supervision consultants;
- Coordination with regulatory agencies and financiers;
- Internal coordination across environmental and social units;
- Regional-office-to-headquarters coordination mechanisms.

Key issues to assess:

- Effectiveness of coordination committees;
- Frequency and quality of coordination meetings;
- Information sharing mechanisms;
- Use of digital collaboration tools;
- Fragmentation of communication channels.

(f) Decision-Making Processes

The Consultant shall assess how safeguards-related decisions are made, approved, escalated, and documented.

Key aspects include:

- Decision authority levels and delegation frameworks;
- Approval processes for ESIA, RAP, and compliance decisions;

- Timeliness and transparency of decision-making;
- Evidence base used for decision-making;
- Bottlenecks in approval chains;
- Degree of centralization versus decentralization;
- Documentation and traceability of decisions.

3.2.2 Business Process Mapping

The Consultant shall undertake comprehensive end-to-end mapping of all safeguards-related business processes to establish detailed “As-Is” workflows, including inputs, outputs, actors, systems, and decision points.

The mapping shall follow internationally recognized Business Process Management (BPM) standards (e.g., BPMN notation where applicable).

(a) Environmental and Social Impact Assessment (ESIA)

The Consultant shall map:

- Project screening and categorization processes;
- ESIA commissioning and TOR development;
- Consultant procurement and management;
- ESIA study execution workflows;
- Review and approval processes;
- Public consultation and disclosure steps;
- Integration of ESIA findings into project design;
- Regulatory submission and approval tracking.

(b) Environmental Audits and Monitoring

The Consultant shall map:

- Environmental audit planning and scheduling;
- Field inspection workflows;
- Data collection and validation processes;
- Non-compliance identification and reporting;
- Corrective action tracking and closure;
- Reporting and escalation procedures.

(c) Resettlement Action Plans (RAPs)

The Consultant shall map:

- Land acquisition initiation and valuation processes;
- Census and socio-economic surveys;
- Compensation approval workflows;
- Payment processing and verification;
- Livelihood restoration tracking;
- Grievance handling related to resettlement;
- RAP implementation monitoring and reporting.

(d) Livelihood Restoration Programs

The Consultant shall map:

- Beneficiary identification and eligibility verification;
- Program design and approval;
- Implementation tracking;
- Monitoring of livelihood outcomes;
- Reporting and evaluation mechanisms.

(e) Stakeholder Engagement

The Consultant shall map:

- Stakeholder identification and mapping;
- Consultation planning and execution;
- Meeting documentation and feedback capture;
- Disclosure and communication processes;
- Follow-up and feedback integration mechanisms.

(f) Grievance Redress Mechanisms (GRM)

The Consultant shall map:

- Grievance intake channels (manual, email, field reports, etc.);
- Registration and classification processes;
- Assignment and investigation workflows;
- Resolution and escalation procedures;
- Closure and feedback mechanisms;
- Reporting and analytics processes.

(g) Occupational Health and Safety (OHS)

The Consultant shall map:

- Safety planning and risk assessment;
- Incident prevention measures;
- Safety inspections and audits;
- Incident reporting and investigation workflows;
- Corrective action tracking;
- Compliance reporting.

(h) Community Health and Safety

The Consultant shall map:

- Community risk assessments;
- Engagement with local communities;
- Incident reporting and response;
- Emergency preparedness and response workflows;
- Monitoring of community impacts.

(i) Incident Reporting and Management

The Consultant shall map:

- Incident detection and reporting channels;
- Classification and severity assessment;
- Escalation workflows;
- Investigation processes;
- Corrective and preventive actions (CAPA);
- Closure and reporting mechanisms.

(j) Contractor Safeguards Supervision

The Consultant shall map:

- Contractor reporting requirements;
- Supervision consultant review processes;
- Field verification workflows;
- Compliance assessment procedures;
- Performance evaluation and enforcement mechanisms.

(k) Monitoring and Evaluation (M&E)

The Consultant shall map:

- Indicator definition and tracking;
- Data collection schedules;
- Consolidation and validation processes;

- Reporting cycles;
- Feedback loops into decision-making.

(l) Regulatory Approvals

The Consultant shall map:

- Submission of safeguards documentation to regulators;
- Review and feedback cycles;
- Approval timelines and dependencies;
- Tracking of compliance conditions;
- Permit renewal and monitoring workflows.

(m) Compliance Reporting

The Consultant shall map:

- Internal compliance reporting structures;
- Donor reporting requirements;
- Regulatory reporting obligations;
- Data aggregation and validation processes;
- Report approval and submission workflows.

(n) Data Collection and Records Management

The Consultant shall map:

- Field data collection processes;
- Paper-based and digital data entry workflows;
- Data validation and verification processes;
- Storage and retrieval systems;
- Archiving and retention procedures;
- Document version control mechanisms.

3.3.3 Information Systems Assessment

Review:

- Existing ICT tools and platforms; The Consultant shall identify and assess all ICT tools, software applications, and digital platforms currently used by the Safeguards Department and related departments in managing safeguards activities.
- Databases and spreadsheets; The Consultant shall review all databases, spreadsheets, and repositories currently used for safeguards data collection, storage, analysis, and reporting.

- Data flows and storage mechanisms; The Consultant shall assess how safeguards data and information flow across departments, projects, systems, and stakeholders.
- Reporting systems; The Consultant shall assess existing safeguards reporting systems and reporting workflows.
- GIS and spatial data usage; The Consultant shall assess the use of Geographic Information Systems (GIS), spatial data, and geo-enabled tools in safeguards management.
- Mobile data collection tools; The Consultant shall assess the use of mobile technologies and field-based digital data collection tools for safeguards monitoring and reporting.
- Integration between systems; The Consultant shall assess interoperability and integration between safeguards-related systems and other enterprise systems within KeNHA.
- User access and security controls. The Consultant shall assess information security, user access management, and cybersecurity controls applicable to safeguards systems and data.

3.3.4 Performance Assessment

Assess:

- Efficiency of workflows; The Consultant shall assess the efficiency and effectiveness of safeguards operational workflows across the project lifecycle.
- Turnaround times; The Consultant shall assess the timeliness and responsiveness of safeguards operational processes.
- Reporting accuracy; The Consultant shall assess the accuracy, completeness, consistency, and reliability of safeguards reporting systems and outputs.
- Compliance tracking; The Consultant shall assess mechanisms used to track compliance with safeguards obligations, commitments, permits, corrective actions, and donor requirements.
- Data quality; The Consultant shall assess the quality, consistency, completeness, integrity, and reliability of safeguards data.
- Internal controls; The Consultant shall assess the adequacy and effectiveness of internal controls governing safeguards operations and information management.
- Audit trails; The Consultant shall assess the availability and effectiveness of audit trails and traceability mechanisms within safeguards systems and workflows.
- User satisfaction; The Consultant shall assess user experience, usability, adoption levels, and stakeholder satisfaction with current safeguards systems and operational processes.
- Operational bottlenecks. The Consultant shall identify operational, procedural, institutional, and technological bottlenecks affecting safeguards performance.

Task 3: Gap Analysis

The Consultant shall undertake a detailed gap assessment, in relation to KeNHA's safeguards department and the Authority as a whole. The analysis will cover:

3.4.1 Operational Gaps

Identify:

- Workflow inefficiencies; The Consultant shall assess inefficiencies within existing safeguards operational workflows and business processes.
- Duplication of functions; The Consultant shall assess duplication of activities, responsibilities, systems, records, and reporting functions within safeguards operations.
- Delays in approvals; The Consultant shall assess delays affecting safeguards approvals, reviews, decision-making, and escalation processes.
- Weak coordination mechanisms; The Consultant shall assess coordination arrangements between departments, regional offices, project teams, contractors, consultants, regulators, and other stakeholders involved in safeguards management.
- Compliance risks; The Consultant shall assess operational and systems-related risks that may result in non-compliance with safeguards requirements, legal obligations, donor requirements, and institutional policies.
- Documentation weaknesses. The Consultant shall assess weaknesses in safeguards documentation management, records handling, document accessibility, and information retention practices.

3.4.2 Institutional and Capacity Gaps

Assess:

- Safeguards department human resource adequacy; The Consultant shall assess the adequacy of human resources within the Safeguards Department in relation to the Department's mandate, workload, operational responsibilities, and future automation requirements.
- Technical competencies; The Consultant shall assess the technical competencies, professional qualifications, and skills of staff involved in safeguards operations.
- Training needs; The Consultant shall assess current and future training and capacity building needs required to strengthen safeguards operations and support proposed automation initiatives.
- Change readiness; The Consultant shall assess the organizational readiness of the Safeguards Department and related stakeholders to adopt new technologies, systems, workflows, and institutional changes associated with automation and digital transformation.

- Governance arrangements. The Consultant shall assess governance structures, oversight mechanisms, accountability frameworks, and decision-making arrangements supporting safeguards operations and systems management.

3.4.3 Technology and Systems Gaps

The Consultant shall undertake a comprehensive assessment of technology, information systems, digital infrastructure, and data management gaps affecting the efficiency, reliability, integration, security, and scalability of safeguards operations within Kenya National Highways Authority.

The assessment shall identify weaknesses, limitations, risks, and opportunities associated with existing ICT systems and digital processes, and provide recommendations to support automation, integration, and modernization of safeguards management systems.

The assessment shall specifically cover the following areas:

- Data management; The Consultant shall assess the adequacy, effectiveness, governance, and reliability of safeguards data management practices and systems.
- Systems interoperability; The Consultant shall assess the interoperability and integration capabilities of existing safeguards systems and related enterprise systems.
- Automation; The Consultant shall assess the extent of automation within safeguards operations and identify opportunities for workflow digitization and process automation.
- Reporting capabilities; The Consultant shall assess the adequacy, effectiveness, and flexibility of existing safeguards reporting systems and reporting capabilities.
- Cybersecurity; The Consultant shall assess cybersecurity risks, controls, governance arrangements, and information security practices associated with safeguards systems and data.
- Remote access; The Consultant shall assess the capability of existing systems to support secure and efficient remote access for safeguards operations and field activities.
- Backup and disaster recovery; The Consultant shall assess existing backup arrangements, disaster recovery capabilities, and business continuity mechanisms for safeguards systems and data.
- Data analytics and dashboarding. The Consultant shall assess existing data analytics, visualization, and dashboarding capabilities supporting safeguards monitoring and decision-making.

3.4.4 Benchmarking

The Consultant shall undertake a desk-based structured benchmarking assessment of safeguards operations within Kenya National Highways Authority against international standards, peer institutions, multilateral development bank requirements, and emerging digital safeguards management practices.

The purpose of the benchmarking exercise is to identify performance gaps, institutional weaknesses, and modernization opportunities, and to inform the design of an improved, automated, and globally aligned safeguards management system.

The benchmarking shall specifically cover the following dimensions:

- International best practice; The Consultant shall assess KeNHA safeguards systems and practices against globally recognized environmental and social safeguards management standards and institutional best practices for infrastructure agencies.
- Comparable road agencies; The Consultant shall benchmark KeNHA's safeguards operations against similar national road authorities and highway agencies in comparable jurisdictions, particularly in emerging and developing economies.
- World Bank environmental and social management expectations; The Consultant shall assess KeNHA safeguards systems against the requirements of multilateral development institutions, with particular emphasis on the Environmental and Social Framework (ESF) of the World Bank Group.
- Digital safeguards management standards. The Consultant shall assess KeNHA's safeguards systems against emerging global standards in digital transformation, e-governance, and digital environmental and social management systems.

Task 4 Automation Needs Assessment and Business Process Re-engineering

The Consultant shall undertake a structured automation readiness assessment and business process re-engineering (BPR) exercise to define a future digital safeguards management environment. This shall be based on findings from the current-state assessment, gap analysis, and benchmarking.

The objective is to identify inefficiencies, redesign workflows, and define a streamlined, automated, and integrated safeguards management system.

4.1.1 Identification of Automation Opportunities

The Consultant shall systematically assess all safeguards processes and identify opportunities for digitization, workflow automation, and system integration.

(a) Workflow Approvals

- Assess manual approval chains across safeguards processes;
- Identify approval bottlenecks and redundancies;
- Define opportunities for electronic workflow routing, digital signatures, and automated escalation;
- Recommend role-based approval hierarchies and delegation mechanisms.
-

(b) Compliance Tracking

- Evaluate current manual compliance tracking mechanisms;
- Identify gaps in monitoring environmental and social commitments;
- Define automated compliance registers linked to project activities;
- Recommend alert-based compliance monitoring systems.

(c) Safeguards Monitoring

- Assess field monitoring processes and reporting structures;
- Identify opportunities for real-time digital monitoring systems;
- Recommend integration of mobile data capture and geo-tagging;
- Define automated compliance dashboards for monitoring activities.

(d) ESIA and RAP Tracking

- Assess tracking of ESIA approvals, RAP implementation, and mitigation measures;
- Identify fragmentation in documentation and reporting;
- Recommend integrated ESIA/RAP lifecycle tracking modules;
- Define automated milestone tracking and progress monitoring tools.

(e) Grievance Management

- Review current grievance redress mechanisms (GRM);
- Identify inefficiencies in complaint logging, tracking, and resolution;
- Recommend fully digitized grievance case management systems;
- Define escalation workflows and automated response timelines.

(f) Contractor Reporting

- Assess contractor safeguards reporting formats and frequency;
- Identify duplication and manual consolidation issues;
- Recommend digital contractor portals for real-time reporting;
- Define standardized reporting templates and validation rules.

(g) Incident Management

- Evaluate incident reporting and response workflows;
- Identify delays in escalation and closure of incidents;
- Recommend automated incident reporting systems with alerts;
- Define classification and severity-based escalation logic.

(h) Mobile Inspections

- Assess current field inspection practices;
- Identify gaps in data capture, verification, and timeliness;
- Recommend mobile applications for offline/online inspections;
- Define geo-tagging, photo capture, and real-time sync capabilities.

(i) GIS-Enabled Monitoring

- Assess use of spatial data in safeguards management;
- Identify lack of integration between GIS and operational systems;
- Recommend GIS-enabled dashboards and spatial analytics;
- Define integration of geospatial layers with project data.

(j) Dashboard Reporting

- Review current reporting dashboards and MIS tools;
- Identify limitations in real-time reporting and analytics;
- Recommend interactive dashboards for executive decision-making;
- Define KPIs and visualization frameworks.

(k) Document Management

- Assess current document storage and retrieval systems;
- Identify reliance on paper-based and decentralized storage;
- Recommend enterprise document management systems (EDMS);
- Define metadata standards, version control, and access rules.

(l) Stakeholder Engagement Tracking

- Evaluate stakeholder engagement processes and documentation;
- Identify lack of structured tracking of consultations and feedback;
- Recommend digital stakeholder engagement platforms;
- Define engagement logs, feedback tracking, and reporting tools.

4.1.2 Business Process Re-engineering (BPR)

The Consultant shall undertake a comprehensive redesign of safeguards business processes to eliminate inefficiencies and align operations with digital workflows.

(a) Redesign of Workflows

- Map all current end-to-end safeguards processes;
- Identify non-value-adding steps and redundancies;
- Design simplified, standardized, and integrated workflows;

- Align workflows with automation and system capabilities.

(b) Process Simplification

- Reduce excessive approval layers;
- Eliminate duplication of data entry and reporting;
- Streamline interdepartmental coordination processes;
- Standardize documentation and reporting templates.

(c) Elimination of Redundancies

- Identify overlapping roles and duplicated responsibilities;
- Consolidate parallel reporting systems;
- Harmonize data collection and validation processes;
- Remove manual reconciliation requirements where possible.

(d) Optimized Digital Workflows

- Design fully digital, end-to-end workflows for key safeguards functions;
- Define system-driven approvals, notifications, and escalations;
- Ensure traceability and auditability in all workflows;
- Align workflows with proposed automation architecture.

4.1.3 Future-State Operating Model

The Consultant shall define a future-state operating model for safeguards management reflecting a fully digitized and integrated environment.

(a) Target Operating Model (TOM)

- Define future organizational structure for safeguards management;
- Define roles, responsibilities, and accountability in a digital environment;
- Establish interaction between safeguards, ICT, and project teams;
- Define centralized versus decentralized functions.

(b) Governance Arrangements

- Define governance structure for the digital safeguards system;
- Establish system ownership and administration roles;
- Define data governance and decision-making authority;
- Recommend oversight committees and reporting structures.

(c) Staffing Implications

- Assess impact of automation on staffing requirements;
- Identify roles to be enhanced, reskilled, or redefined;
- Recommend staffing adjustments under automated systems;
- Define capacity needs for system administration and analytics.

(d) Future-State Process Maps

- Develop detailed “to-be” process maps for all key safeguards functions;
- Illustrate automated workflows and decision points;
- Define system interactions and data flows;
- Ensure alignment with functional and technical system design.

4.2 Development of Functional and Technical Requirements

The Consultant shall develop a comprehensive Functional Requirements Specification (FRS) and Technical Requirements Specification (TRS) for the proposed Safeguards Management Information System (SMIS).

4.2.1 Functional Requirements

(a) User Requirements

- Define user categories and roles (e.g., safeguards officers, engineers, contractors, management);
- Specify user needs for each role;
- Define access levels and permissions.

(b) Workflow Requirements

- Define end-to-end digital workflows for safeguards processes;
- Specify approval hierarchies and routing rules;
- Define escalation mechanisms and notifications.

(c) Case Management Requirements

- Define structured case handling for grievances, incidents, and non-compliance;
- Include case creation, assignment, tracking, and closure;
- Define SLA tracking and alerts.

(d) Reporting and Analytics Requirements

- Define standard and ad-hoc reporting capabilities;
- Specify automated report generation;
- Define KPI tracking and performance reporting.

(e) Dashboard Requirements

- Define executive dashboards and operational dashboards;
- Specify real-time visualization of safeguards performance indicators;
- Define drill-down and filtering capabilities.

(f) GIS Integration Requirements

- Define spatial mapping and visualization requirements;
- Specify integration with geospatial databases;
- Define mapping of projects, incidents, and environmental assets.

(g) Mobile Functionality

- Define offline and online mobile data capture requirements;
- Specify field inspection tools;
- Define geo-tagging, photo capture, and synchronization features.

(h) Notification and Escalation Mechanisms

- Define automated alerts for deadlines, incidents, and compliance breaches;
- Specify escalation workflows;
- Define SMS/email/app notifications.

(i) Audit Trails

- Define system logging requirements;
- Ensure traceability of user actions and approvals;
- Define tamper-proof audit records.

(j) Records Management

- Define electronic document storage and retrieval;
- Specify version control and indexing;
- Define retention and archival policies.

4.2.2 Technical Requirements

(a) System Architecture

- Define high-level and detailed system architecture;
- Specify modular and scalable design principles;
- Define integration architecture.

(b) Hosting Environment

- Recommend hosting options (cloud, on-premise, hybrid);
- Define infrastructure requirements for hosting;
- Ensure compliance with government ICT standards.

(c) Cloud/On-Premise Considerations

- Evaluate trade-offs between deployment models;
- Recommend optimal deployment strategy;
- Assess security and cost implications.

(d) Database Requirements

- Define database architecture and structure;
- Specify relational and spatial database needs;
- Define data storage standards.

(e) APIs and Interoperability

- Define API requirements for system integration;
- Specify interoperability with enterprise systems;
- Define data exchange formats and protocols.

(f) Scalability Requirements

- Define system scalability for multi-project expansion;
- Specify user load and performance thresholds;
- Ensure future-proof architecture.

(g) Performance Standards

- Define system response times;
- Specify uptime requirements;
- Define system reliability standards.

(h) Backup and Disaster Recovery

- Define backup frequency and retention policies;
- Specify disaster recovery architecture;
- Define recovery time and recovery point objectives (RTO/RPO).

(i) Cybersecurity Controls

- Define security architecture and controls;

- Specify encryption standards;
- Define intrusion detection and monitoring requirements.

(j) Authentication and Role-Based Access

- Define user authentication mechanisms;
- Specify role-based access control (RBAC);
- Define multi-factor authentication requirements.

(k) Data Protection Requirements

- Ensure compliance with data protection laws;
- Define privacy safeguards;
- Specify data anonymization where required.

4.2.3 Infrastructure Requirements

(a) Hardware Requirements

- Define servers, storage devices, and backup hardware;
- Specify end-user devices and field equipment requirements.

(b) Network Requirements

- Define network bandwidth and connectivity requirements;
- Specify VPN and secure access infrastructure.

(c) Connectivity Requirements

- Define requirements for field and remote connectivity;
- Include offline data synchronization capabilities.

(d) Server and Storage Requirements

- Define storage capacity and redundancy requirements;
- Specify cloud storage configurations if applicable.

(e) User Devices and Field Equipment

- Define tablets, smartphones, GPS devices for field operations;
- Specify rugged devices for field inspections.

4.2.4 Implementation Options Analysis

The Consultant shall evaluate alternative system implementation approaches.

(a) Custom-Built Solutions

- Tailor-made system development;
- Full customization to KeNHA needs.

(b) Commercial Off-the-Shelf (COTS) Solutions

- Existing enterprise systems adapted to safeguards needs;
- Vendor-supported platforms.

(c) Open-Source Platforms

- Customization of open-source frameworks;
- Cost-effective and flexible solutions.

(d) Hybrid Solutions

- Combination of COTS and custom modules;
- Integration of multiple platforms.

Comparative Analysis Criteria

The Consultant shall evaluate each option based on:

- Total cost of ownership (TCO);
- Implementation risks;
- Scalability and flexibility;
- Sustainability and maintainability;
- Vendor dependence;
- Integration capability;
- User adoption and usability.

4.3 Implementation Roadmap and Change Management Strategy

4.3.1 Implementation Roadmap

(a) Phased Implementation Plan

- Define short-, medium-, and long-term implementation phases;
- Prioritize critical safeguards modules for early rollout.

(b) Prioritization Matrix

- Rank automation components based on impact and feasibility;
- Define quick wins versus long-term investments.

(c) Timelines

- Develop detailed implementation schedule;
- Align timelines with procurement and rollout phases.

(d) Resource Requirements

- Define technical, financial, and human resource needs;
- Include vendor and internal capacity requirements.

(e) Procurement Considerations

- Define procurement packaging strategy;
- Recommend procurement methods under donor guidelines.

4.3.2 Change Management Strategy

(a) Stakeholder Engagement

- Identify internal and external stakeholders;
- Define engagement and consultation mechanisms.

(b) Communication Strategy

- Develop structured communication plan;
- Promote awareness and buy-in across the organization.

(c) Capacity Building

- Define training programs for users and administrators;
- Include ICT and safeguards capacity development.

(d) User Adoption Strategy

- Define strategies to ensure system uptake;
- Include incentives and user support mechanisms.

(e) Institutional Strengthening

- Recommend organizational adjustments for digital transformation;
- Strengthen governance and ICT support structures.

4.3.3 Cost Estimates

The Consultant shall prepare indicative cost estimates covering:

(a) System Development or Acquisition

- Software development or licensing costs;
- Customization and configuration costs.

(b) Infrastructure Costs

- Servers, storage, network infrastructure;
- Cloud hosting fees (if applicable).

(c) Licensing Costs

- Software licenses and subscriptions;
- Third-party integration tools.

(d) Training Costs

- User training and capacity building programs;
- Change management workshops.

(e) Support and Maintenance Costs

- Annual maintenance and support contracts;
- System upgrades and enhancements.

Deliverables and Reporting Schedule

Loop No.	Deliverable	Description	Indicative Timeline from commencement
1	Inception Report	Understanding of the assignment; Methodology; Work plan and schedule; Stakeholder engagement strategy; Data collection tools; Risk management approach; Quality assurance plan.	2 weeks
2	Current State Assessment Report	Operational review and process mapping	6 weeks
3	Gap Analysis Report	Institutional, operational, and systems gaps	8 weeks
4	Business Process Re-engineering Report	Optimized future-state workflows	10 weeks
5	Automation Needs Assessment Report	Automation opportunities and requirements	12 weeks
6	Draft Functional & Technical Requirements Specification	Comprehensive IT/system requirements	14 weeks
7	Draft Final Report	Consolidated report and roadmap	18 weeks
8	Draft Bidding Document - ESHMS	Bidding document for deployment of the digital system	18 weeks
9	Draft Environmental, Social, Health and Safety Management System Handbook/Manual	To include procedures for all safeguards processes based on international best practice	18 weeks
10	Final Report	Final approved deliverable	22 weeks
11	Final Bidding Document - ESHMS	Bidding document for deployment of the digital system	22 weeks
12	Draft Environmental, Social, Health and Safety Management System Handbook/Manual	To include procedures for all safeguards processes based on international best practice	22 weeks

3 Assignment Duration and Schedule

The duration of the assignment is 22 weeks with commencement expected to be two (2) weeks from the date of signing of the contract. In addition, the Consultant is expected to submit detailed program of works for the assignment and any assumptions made regarding the level of effort indicated in the ToRs. It is expected that the key members of the Consultant team shall not change throughout the duration of the contract. Any staff changes will require KeNHA's approval.

3.1 Procedure for Review of Reports and Other Deliverables

The procedure for submission and reviewing reports will be as follows:

- i. All reports shall be submitted in hard copy with an electronic copy in English in pdf and MSWord. The consultant shall submit 2 No. hardcopies and 3 No. soft copies for every report. The recipients of reports will be the World Bank, Project Management Office in the Ministry of Roads and Transport and KeNHA.
- ii. The standard review period for KeNHA and World Bank is 10 working days.
- iii. Draft reports, Final reports and documents should be submitted in editable MS Word and PDF versions. Final version of the reports should be submitted one week after receiving feedback on draft version.

4 Reporting Obligations

Director, Highway Design and Survey(HDS) has an overall mandate to oversee and coordinate various aspects related to environment, health, and social management in the Authority. The Director, HDS will be represented by the Deputy Director, Environmental and Social Safeguards (ESS) under which this assignment will be housed. The Deputy Director, ESS will be the Principal Contact for the assignment and will manage the contract execution.

KeNHA will share with the World Bank and Project Management Office in the Ministry of Roads and Transport updates on the consultancy progress and activities.

5 Consultant Qualification and Experience

Firm Experience

The consulting firm shall demonstrate:

- At least 10 years' experience in institutional reviews and systems assessments;
- Experience in environmental and social safeguards management systems;
- Experience in business process re-engineering;
- Experience in ICT systems analysis and digital transformation;
- Experience with public sector institutions;
- Experience with World Bank or other donor-funded projects.

Key Experts Qualification Requirements

a) Team Leader / Institutional Development Specialist

The Team Leader shall provide overall leadership and coordination of the assignment and serve as the primary liaison with KeNHA.

Academic Qualifications

- Advanced degree in any of the following: Public Administration, Business Administration, Organizational Development, Transportation Engineering, Infrastructure Management, Project Management, or related field.
- Additional qualifications in institutional reform, governance, or strategic management will be an added advantage.

Experience Requirements

- Minimum 15 years of relevant professional experience;
- Demonstrated experience leading institutional review and organizational transformation assignments;
- Experience in public sector institutional strengthening;
- Experience in donor-funded infrastructure projects;
- Proven experience managing multidisciplinary consulting teams;
- Experience in East Africa or similar developing-country contexts is desirable.

b) Environmental Safeguards Specialist

Lead assessment of environmental safeguards systems, compliance processes, environmental monitoring, and environmental reporting workflows.

Academic Qualifications:

Master's degree in: Environmental Science, Environmental Engineering, Environmental Management, Natural Resources Management, or related field.

Experience Requirements

- Minimum 10 years of relevant experience;
- Experience in environmental safeguards for infrastructure projects;
- Experience with ESIA processes and environmental compliance systems;
- Familiarity with:
 - Kenyan environmental legislation,
 - World Bank Environmental and Social Framework (ESF),
 - IFC Performance Standards,
 - or equivalent donor safeguards frameworks.
- Experience in environmental management information systems is an added advantage.

Specific Expertise

- ESIA processes;
- Environmental monitoring;
- Compliance systems;
- Environmental reporting;
- Environmental data management.

c) Social Safeguards / Resettlement Specialist

Lead review of social safeguards operations including RAPs, stakeholder engagement, grievance management, community health and safety, and social compliance monitoring.

Academic Qualifications

- Master's degree in: Sociology, Social Development, Development Studies, Land Economics, or related field.

Experience Requirements

- Minimum 10 years relevant experience;
- Demonstrated experience in:
 - RAP preparation and implementation,
 - stakeholder engagement,
 - grievance redress mechanisms,
 - social risk management.
- Experience in infrastructure projects financed by development partners;
- Familiarity with World Bank ESF ESS5 and ESS10 requirements.

Specific Expertise

- Resettlement management;
- Social safeguards compliance;
- Community engagement;
- Vulnerability assessments;
- Social monitoring systems.

d) GBV and Gender Expert

The gender and GBV protection expert shall have a minimum of a relevant bachelor's degree in social sciences (Gender studies, Sociology, Social work and Anthropology) with at least ten (10) years practical post qualification experience. He/She must have extensive experience in gender mainstreaming, instituting GBV referral pathways, and executing investigations, provision of psychosocial support to GBV survivors and case management. Previous experience on similar capacity will be an added advantage.

e) ICT Systems Architect / Enterprise Architect

Lead the development of technical architecture, systems integration requirements, infrastructure requirements, and overall automation framework.

Academic Qualifications

Master's degree in: Computer Science, Information Systems, Software Engineering, ICT, Enterprise Architecture, or related field.

Experience Requirements

- Minimum 10 years relevant experience;
- Experience designing enterprise information systems;
- Experience in systems architecture and interoperability;
- Experience in public sector ICT systems;
- Experience in cloud and hybrid architectures;
- Familiarity with government ICT standards and cybersecurity frameworks.

Specific Expertise

- Enterprise architecture;
- Systems integration;
- Database architecture;
- API integration;
- Infrastructure planning.

f) Business Process Re-engineering Specialist

Lead business process mapping, workflow analysis, process optimization, and redesign of safeguards operational procedures.

Academic Qualifications

- Master's degree in: Business Process Management, Industrial Engineering, Operations Management, Information Systems, Business Administration, or related field.

Experience Requirements

- Minimum 10 years relevant experience;
- Demonstrated experience in:
 - process mapping,
 - workflow optimization,
 - institutional process redesign,
 - automation readiness assessments.
- Experience in public sector digital transformation assignments;
- Familiarity with BPMN or equivalent process modelling standards.

Specific Expertise

- Workflow analysis;
- Operational efficiency;
- Change process design;
- Digital workflow optimization.

g) Database and Data Governance Specialist

Lead assessment of data structures, records management, reporting architecture, data governance, and analytics requirements.

Academic Qualifications

Bachelors Degree in: Computer Science, Information Management, Data Science, Information Systems, or related field.

Experience Requirements

- Minimum 8 years relevant experience;
- Experience in database design and management;
- Experience in data governance frameworks;

- Experience with reporting and dashboard systems;
- Familiarity with GIS-enabled databases is an advantage.

Specific Expertise

- Data architecture;
- Data quality management;
- Reporting systems;
- Records management;
- Data governance.

h) Cybersecurity / Data Governance Specialist

Assess cybersecurity, data protection, system access controls, and information security requirements.

Academic Qualifications

Bachelors Degree in: Cybersecurity, Information Security, Computer Science, ICT, or related field.

Experience Requirements

- Minimum 8 years relevant experience;
- Experience in cybersecurity assessments;
- Familiarity with:
 - ISO 27001,
 - data protection regulations,
 - cybersecurity governance frameworks.
- Experience securing enterprise systems.

Specific Expertise

- Information security;
- Risk assessment;
- Identity and access management;
- Data protection compliance.

i) GIS and Spatial Data Specialist

Assess GIS integration opportunities for safeguards monitoring, spatial compliance tracking, and field inspections.

Academic Qualifications

Bachelors Degree in: GIS, Geomatics, Surveying, Geography, Spatial Sciences, or related field.

Experience Requirements

- Minimum 7 years relevant experience;
- Experience in GIS systems for infrastructure or environmental monitoring;
- Experience integrating GIS with enterprise systems.

Specific Expertise

- Spatial data systems;
- GIS dashboards;
- Mobile mapping;
- Geo-enabled compliance systems.

j) Change Management Specialist and Capacity Building Specialist

Lead institutional change management, stakeholder engagement, training needs assessment, and user adoption planning.

Academic Qualifications

Bachelors Degree in: Organizational Psychology, Human Resource Development, Organizational Development, Business Administration, or related field.

Experience Requirements

- Minimum 8 years relevant experience;
- Experience in digital transformation change management;
- Experience designing training and capacity building programs;
- Experience in public sector reforms.

Specific Expertise

- Change management;
- Stakeholder engagement;
- Training strategies;
- User adoption planning.

k) Procurement and ICT Acquisition Specialist

Support preparation of implementation and procurement recommendations for automation systems.

Academic Qualifications

Bachelors Degree in: Procurement, Supply Chain Management, ICT Procurement, Business Administration, or related field. Infrastructure or ICT procurement is preferred.

Experience Requirements

- Minimum 8 years relevant experience;
- Experience in ICT procurement under World Bank or donor-funded projects;
- Familiarity with procurement of enterprise systems.

Specific Expertise

- ICT procurement;
- Technical evaluation support for ICT procurement
- Procurement planning.

Key Experts Input

No.	Expert	Input (Months)
1	Team Leader / Institutional Development Specialist	4.0
2	Environmental Safeguards Specialist	2.5
3	Social Safeguards / Resettlement Specialist	2.5
4	GBV and Gender Expert	1.0
5	Business Process Re-engineering Specialist	3.0
6	ICT Systems Architect / Enterprise Architect	3.0
7	Systems Analyst / Functional Requirements Specialist	2.5
8	Cybersecurity & Information Security Specialist	1.0
9	Database & Data Governance Specialist	1.5
10	GIS & Spatial Data Specialist	1.0
11	Change Management & Capacity Building Specialist	1.5
12	Procurement / ICT Acquisition Specialist	0.5
	Total	24

Applicable Guidelines

The assignment shall be implemented in accordance with:

- Applicable laws of Kenya;
- KeNHA policies and procedures;
- Relevant donor procurement and safeguards guidelines;
- International good practice in digital governance and safeguards management.

6 Support to be provided by KeNHA

The Client shall provide timely and adequate administrative, technical, and logistical support to enable the Consultant to execute the assignment effectively, efficiently, and within the agreed timelines.

The Client's support shall include, but not be limited to, the following:

i. Access to Information and Documentation

The Client shall provide the Consultant with full access to all relevant documentation and data necessary for execution of the assignment, including:

- Existing safeguards policies, manuals, and procedures;
- Environmental and Social Impact Assessments (ESIAs);
- Environmental and Social Management Plans (ESMPs);
- Resettlement Action Plans (RAPs) and Livelihood Restoration Plans;
- Grievance Redress Mechanism (GRM) records and reports;
- Environmental audit and monitoring reports;
- Occupational Health and Safety (OHS) reports;
- Contractor and supervision consultant safeguards reports;
- Compliance and regulatory submission records;
- Donor-funded project safeguards documentation;
- Existing ICT system documentation (where available), including:
 - system architecture diagrams;
 - user manuals;
 - database structures;
 - reporting templates;
- Any relevant internal audit reports or performance reviews.

The Client shall ensure that documentation is provided in a timely manner and in usable formats (electronic preferred where available).

ii. Access to Systems and Databases

The Client shall facilitate controlled access for the Consultant to relevant systems and platforms, where applicable, including:

- Safeguards-related databases and spreadsheets;
- Project management systems;
- GIS platforms and spatial data repositories;
- Document management systems;
- Reporting and dashboard tools;
- Any interim or legacy systems used for safeguards management.

Where direct system access is not possible, the Client shall provide:

- System screenshots or extracts;
- Sample datasets;
- Exported reports and data dumps;
- Read-only access or controlled viewing sessions.

iii. Facilitation of Stakeholder Engagement

The Client shall support the Consultant in engaging relevant stakeholders, including:

- Safeguards Department staff at headquarters and regional offices;
- Project implementation teams;
- Engineering, planning, procurement, and finance departments;

- Field supervision consultants and contractors;
- Regulatory agencies (e.g., environmental and land authorities);
- Development partner representatives (where applicable).

The Client shall:

- Facilitate introduction letters and official communication;
- Support scheduling of interviews, workshops, and validation sessions;
- Ensure availability of key personnel for consultations;
- Support organization of stakeholder workshops and validation meetings.

iv. Appointment of Focal Persons

The Client shall designate:

- A Project Focal Point within the Safeguards Department;
- A Technical Focal Point from the ICT department;
- A Procurement/Contract Management liaison officer (if required);
- Additional focal persons at regional offices where necessary.

The focal persons shall:

- Coordinate Consultant access to information and stakeholders;
- Facilitate approvals and administrative processes;
- Support review and validation of deliverables;
- Serve as primary communication channels with the Consultant.

v. Logistical and Administrative Support

The Client shall provide reasonable logistical support to facilitate fieldwork and stakeholder engagement, including:

- Office space for Consultant meetings when required;
- Access to meeting rooms for workshops and presentations;
- Facilitation of field visits to project sites (consultants should cost for the visits in their financial proposals);
- Security clearances for restricted project areas (if applicable);
- Coordination support for travel to regional offices and field locations.

Where applicable, the Client may also support:

- Official letters for field access;
- Coordination with contractors for site visits;
- Local administrative support for workshops.

vi. Review and Feedback on Deliverables

The Client shall:

- Review Consultant deliverables within agreed timelines;
- Provide consolidated and timely feedback;
- Organize technical review sessions and validation workshops;

- Facilitate internal approvals of key outputs;
- Ensure participation of relevant technical experts in reviews.

The Client shall ensure that delays in review processes are minimized to avoid impacting the overall project timeline.

vii. Participation in Workshops and Validation Sessions

The Client shall ensure participation of relevant staff in:

- Inception workshop;
- Stakeholder consultation meetings;
- Process mapping and validation workshops;
- ICT and systems requirements validation sessions;
- Draft and final report review meetings.

The Client shall also support dissemination of findings within the institution.

viii. Data Quality and Availability Assurance

The Client shall:

- Ensure that data provided is accurate, complete, and up to date;
- Clarify any inconsistencies in datasets or reports;
- Identify and facilitate access to authoritative data sources;
- Support reconciliation of conflicting information where required.

ix. Timely Decision-Making and Approvals

The Client shall:

- Provide timely approvals of deliverables and key decisions;
- Facilitate escalation of decisions where required;
- Ensure that internal approval bottlenecks do not delay implementation;
- Support prompt resolution of clarifications raised by the Consultant.

x. Safeguards for Confidentiality and Data Use

The Consultant shall be granted access to sensitive information subject to:

- Applicable confidentiality agreements;
- Data protection and privacy requirements;
- Institutional information security policies.

The Client shall define any restrictions on data sharing or publication at project commencement.

Note: *All documentation supplied will remain property of KeNHA and shall solely be used for purposes of the assignment and all copies shall be returned to KeNHA upon completion of the assignment together with an inventory tracking sheet.*

7 Confidentiality statement

All data and information received during the assignment, from respondents, KeNHA and the World Bank are to be treated confidentially and are only to be used in connection with the execution of these Terms of Reference. All intellectual property rights arising from the

execution of these Terms of Reference are assigned to KeNHA. The content of written materials obtained or prepared in this assignment will not be disclosed to any third parties without the expressed advance written authorization of KeNHA and/or the World Bank.

8 Code of Ethics

In performing this assignment, the consultant shall comply, at all times and in all circumstances, with the World Bank Code of Ethics which may be found at the following web address:

<http://documents1.worldbank.org/curated/en/147281468337279671/pdf/WBG-Code-of-Ethics.pdf>

The Client reserves the right to suspend or terminate the assignment where material breaches of the above Code of Ethics are found to have occurred.