



International
Labour
Organization

► **Developing an Electronic Case Management System for the Ministry of Labour of Kenya**

Request for Proposals (individual Consultant)

November 2023

► Contents

	Page
► Contents	3
► Background and Objective	4
► Scope of Work	5
System requirements	5
Technical requirements	5
Security requirements	8
Other requirements	9
ECMS Modules	9
Common Modules (accessible from the Labour and OSH Department)	10
Labour Department Specific Modules	12
OSH Department Specific Modules	12
Written Documentation	12
Change management	14
Communication and Training Plan	14
Adjustment & Maintenance Strategy	14
Testing	14
Programming and Unit Testing	14
System Testing	15
Pilot deployment	16
Phase 1	16
Phase 2	16
Bug fixes	16
Final Deployment	17
Post deployment service/warranty/maintenance	17
► Deliverables	18
► Required Qualifications	21
► Request for Proposals	22
Technical proposal	22
Financial proposal	Error! Bookmark not defined.

► Background and Objective

The ILO is implementing the USDOL funded development cooperation project, All Hands in Kenya: Advancing Labour Standards through Cooperative Action. The project aims to strengthen labour inspection to promote compliance with labour law, international labour standards and acceptable conditions of work. To support this objective, the Labour Department and the Occupational Safety and Health Department within the Ministry of Labour (MoL) of Kenya will be equipped with an online Electronic Case Management System (ECMS) to manage labour inspection actions.

The Project recently completed the process of mapping the procedural workflows, drawing a static wireframe, and developing the Software Requirement Specifications (SRS) for the proposed system. These documents form the foundation of the ECMS and should be studied and referenced in the preparation of a response to this request for proposals.

► Scope of Work

System requirements

Technical requirements

Interface language

The web application/user interface labels will be in English.

Concurrent users

The application should be designed to handle 200 concurrent planned system users (400 total) in 52 county offices throughout Kenya and 1000 concurrent public users.

Web based

The proposed ECMS must be a web-based application. The application should be accessible from a standard personal computer (PC), tablet, and/or cell phone device depending on the type of user and functions being used. The user interface should be homogenous on each platform (web and mobile). The application should be designed to work with a range of browsers (e.g. Chrome, Firefox, Safari) and operating systems (e.g. Windows, Mac, Linux) to ensure maximum accessibility.

User Interface (UI), User Experience (UX)

The user interface appearance and behavior should be coherent and compatible with W3C accessibility guidelines. The ECMS application will be built with the user experience in mind, with ease of use, low learning curve and sufficient performance as core principles. The application should be able to facilitate efficient navigation and minimize the time required to complete tasks.

The application should provide online help and context-sensitive online help facilities, with meaningful error messages that users can appropriately act upon. The user interface should follow a single or a limited number of user interface rules, consistently with the operating system environment in which the ECMS operates. The application should also provide easy-to-use and intuitive end user and administrator functions, as assessed by a panel of typical users. Furthermore, the user interface should be compatible with specialist software used by users with disabilities and provide the ability for users to move, resize and modify display windows, select sound and volume of audio alerts, and save modifications in a user profile. The application should offer persistent, user-definable defaults for data entry where desirable.

Single Sign On

The application should work with a “Single Sign On” approach. This means that a user needs to login only once to navigate through the entire ECMS application to access the functionality associated with their user profile. Depending upon the user rights and access control, functional modules are displayed and specific data at the appropriate administrative level is provided. To ensure security, the system must have a session timeout set with auto logout after a fixed time, whereby the user will have to login again.

Reporting and Analytics

The ECMS should provide built-in reporting and analytics capabilities that allow users to generate ad-hoc reports and analyze data. The system should support a variety of data visualization tools and should be able to export data in various formats, including PDF, Excel, and CSV.

Document Management

The ECMS must have document management capabilities that can capture and declare electronic records, including those from existing electronic documents or newly created ones. It should be able to acquire metadata directly from the record-generating application and allow additional metadata completion by the user. The system must also manage electronic documents within the same file plan and access control mechanisms as electronic records. Additionally, it should allow editing of electronic documents that have not been declared as records, while preventing editing of those that have been declared as records. The ECMS should manage versions of electronic documents as separate entities while maintaining the link between them. It should interface with related packages such as image processing and scanning systems and workflow systems while retaining control of existing electronic records.

Cloud environment during the duration of the service contract

The service provider will provide the cloud environment from application development until the end of the maintenance period. At handover, the cloud environment will be migrated to the cloud or physical server to be determined.

Cloud environment/data hosting post the service contract

Data hosting will be provided on the premises using the Government Common Core Network (GCCN). This is to be determined and may differ per office.

Hardware, operating systems, and network environments

The hardware environment should support both client-server platforms and workstation environments. The operating system environment should be compatible with the ECMS, such as Microsoft Server 2019 or Unix versions like Ubuntu Server. The user interface industry standards should be supported, including Microsoft Windows and X-Windows. The ECMS should also have an intranet browser interface using HTML5 standards.

Supporting Software

A database management system license and implementation are necessary for integration with the ECMS, including the SQL language version. The ECMS should be able to interface with various user applications like word processors, spreadsheets, e-mail systems, and other applications for the capture of electronic records. The system should also produce various output formats for individual or bulk exports, including PRO-required formats for permanent preservation and electronic publishing formats such as CSV, PDF, HTML 5.0, and XML. Search and retrieval and information exchange standards, including Z39.50, should be supported by the ECMS. TWAIN and/or Isis scanner interfaces and Group IV facsimile compression should also be integrated into the system. The ECMS should support the TIFF v6 image format, and if the system allows for color images, JPEG, PNG, GIF, or other user-selectable formats should also be supported.

Scalability and Performance

The ECMS should be designed to handle the current workload and should be scalable to accommodate future growth. The system should have sufficient processing power, storage, and network bandwidth to provide fast response times and minimize downtime. Estimated system data requirements are as follows:

Year One:

Installation, System Data and User Data: 2 TB

Year Three:

Total system Data and User Data: 3 TB

Year Five:

Total system Data and User Data: 6 TB

Departments should consider the extent to which the ECMS provides short response times (in line with user expectations), and is capable of serving the range of sizes of user population for which it is intended, including:

- Adequate response times for commonly performed functions under standard conditions, including 75% of the total 1000 anticipated user population logged on and active, 100% of the anticipated total volume of documents managed by the system, and consistent performance over at least ten transaction attempts.
- Simple searches should be performed within 3 seconds and complex searches within 10 seconds.
- The first page of a record accessed within the previous three months should be retrieved and displayed within 4 seconds, while the first page of a record not accessed within the previous three months should be retrieved and displayed within 20 seconds.
- A single implementation of the system should have an electronic record store of at least 17 Terabytes or and serve at least 200 users simultaneously.
- The system implementation should be expandable in a controlled manner, up to at least 800 users, while providing effective continuity of service.
- The system should support the above without imposing undue systems/account management overheads and without any features that would preclude use in small or large organizations, with equally variable numbers of differently-sized organizational units.

Maintenance

The ECMS system should allow for organizational changes, support user movement, re-configure system parameters, provide backup and recovery facilities, monitor storage space, and ensure ongoing development and support.

- It should allow for bulk changes to record organization, folder structure, and indexing information, while ensuring metadata and audit trail data are accurately handled. This allows for organizational changes such as dividing an organizational unit into two, combining two units into one, moving/re-naming an organizational unit, or dividing a whole organization into multiple units. The system should also support the fluid movement of users between organizational units, individually or in bulk.
- It should allow for retrieval, display, and re-configuration of system parameters and implementation choices, such as indexing elements, user roles, and functions.
- It should provide backup facilities and rebuild capabilities using backup and audit trails.
- It should also offer recovery and rollback facilities in case of system failure or update errors, with notification to administrators of the results.
- It should monitor available storage space and alert administrators when necessary.
- Ongoing development and support are crucial to ensure the system can be upgraded to keep up with changes in systems and application software.

Integration with Other Systems

The ECMS should be designed to integrate seamlessly with other existing systems, such as document management systems, accounting systems, etc. If the new or modified system needs to communicate with another government site or an external organization (like a payment carrier), certain specifications for the interface need to be written. These specifications depend on whether the interface is sending data from the new system to the other site/organization or receiving data from them. If the interface is sending data, the specifications should be detailed enough for the other organization to develop the necessary file processing. If the interface is receiving data, the specifications should provide sufficient information for the other organization to effectively use the interface file in their application. The interface specifications should include the following:

- An overview of the data required for each specified file, including a description of the data.
- The frequency of data submission (e.g., monthly, annually), the effective dates of the submissions, and the due dates (e.g., 5th working day of the month).
- A record layout for each transmitted file.
- A list of data elements, including the format for each data element.

- Physical file characteristics, such as the data set name, record length, and record format.

Alternatively, if the files are transferred via FTP (File Transfer Protocol), the specifications should include:

- The file name to be transmitted.
- The target system for the FTP transmission.

Additionally, the specifications should outline the procedure for notifying the receiving site when the file has been submitted. It's important to note that at this stage of the development process, any general issues regarding the interface should have already been resolved.

Regulatory compliance

The ECMS should be designed to comply with all relevant regulatory requirements, such as data protection laws, privacy laws, and institution-specific regulations. The system should have built-in controls and features that help users comply with these regulations.

Security requirements

Access Control and Domain Rights

The ECMS should establish access controls including controls to identify, authenticate and permit access only to authorized individuals and controls to prevent users from providing information to unauthorized individuals who may seek to obtain this information by fraudulent means. Access control protocols for users will be based on the following functions:

- ECMS shall require a login and password designed to meet minimum security requirements (e.g. X number of letters, numbers, etc.) to access a web-based case management system algorithm.
- A two-factor authentication - this is where a system may, for example, require users to provide a verification code or answer a security question, along with their username and password to log in.
- In addition, the software shall include Single Sign On (SSO) capability - this is an authentication process that allows organizations to manage login credentials for multiple applications in a singular location using an Identity Provider (IDP).
- The ECMS must support control of access to electronic records and electronic folders.
- The ECMS must support a minimum protective marking scheme, which allocates security categories to records, folders and users as a means of controlling access; and should support a more extensive protective marking scheme.
- The ECMS must support control of access to electronic records and electronic folders by business or organisational grouping, lists of named users, or individual owner.
- The ECMS must support the allocation of users to one or more user roles, which determine allowable user access to system functions and facilities available in the ECMS.

Encryption

The ECMS should provide encryption of electronic information, including while it is in transit or in storage on networks or systems to which unauthorized individuals may have access. The ECMS must be able to retain the information that an electronic signature has been verified as authentic, as a metadata element bound to the electronic record with which the signature is associated.

- The ECMS must be able to retain and preserve as metadata, details about the process of verification for a digital signature, including the Certification Authority with which the signature has been validated and any checks made against a certification revocation list or similar status verification agency.
- Where an electronic record has been sent or received in encrypted form by a software application which interfaces with the ECMS, the ECMS must be capable of restricting access to that record to users listed as

holding the relevant decryption key, in addition to any other access control marking allocated to that record.

- Where an electronic record has been transmitted in encrypted form by a software application which interfaces with the ECMS, the ECMS must be able to keep as metadata with that record the fact of encrypted transmission, the type of algorithm, and the level of encryption used.

Network Security

System should use SSL encryption based on https protocol. Public-key encryption methods are used as part of SSL encryption and are expected to be part of the ECMS.

Intrusion Detection Systems, Backup and Continuity Plans

Monitoring systems and procedures should be suggested by the service provider to detect actual and attempted attacks on or intrusions into ECMS. Measures should be in place to protect against destruction, loss, or damage of beneficiary information due to potential environmental hazards, such as fire and water damage or technological failure. The system should have built in data archiving facility to perform automatic data backup provision and archive all historical data based on the scheduled time/date.

Data Protection and Privacy

International best practices to maintain the data protection and privacy in the ECMS is strongly proposed. Specific reference is made to Kenya data protection guidelines where applicable. Any sensitive issues or concerns should be raised as soon as they are identified.

Audit Trail

The system must maintain a record of all activities and changes to management information. This will include trail of all actions executed, which identifies the user and associated details, the data being changed, and the time of the action. The audit trail must be retrievable and exportable in various formats, including PDF, Excel, and CSV.

Other requirements

Data Migration

Data migration from existing legacy Microsoft Excel or Access will only be facilitated by the service provider if provided in a uniform and homogenized manner. Errors in data migration due to unclean or non-uniform data is not the responsibility of the service provider.

Cloud computing services

The service provider will provide cloud computing services throughout the duration of the contract, including during the warranty period. Upon completion of the warranty period, cloud computing services or physical servers to ensure functionality of the system, will be the responsibility of the Ministry of Labour.

ECMS Modules

The ECMS should include the following modules as detailed in the workflow, wireframe, and SRS. These modules should be interconnected and integrated with each other to support implementation as proposed in the SRS.

There are three groups of modules. The Common Modules are accessible by both the Labour and OSH Department. The Labour Department Modules are only accessible by the Labour Department. The OSH Department Modules are only accessible by the OSH Department.

Common Modules (accessible from the Labour and OSH Department)

Complaints Module

Receive and review labour law and OSH related complaints. A complainant can lodge a complaint with the labour/OSH inspector by filling in the form. The system should create an entry on the Complaint Register with a reference number, generate a PDF document of the form, and notify the complainant. The system should allow for automated or manual allocation of the complaint to an officer. The officer determines the complaint's validity and whether to link it to the inspection process or end the process. The system flags various actions as per timelines laid out and changes the complaint's colour to indicate the stages of the process.

OSH Recording Module (accidents, diseases, dangerous occurrences)

Receive and review reports of accidents, illnesses, and diseases from workers and employers, and analyse statistics for public policy making. The module should make available the DOSH 1 form sections Part 1 to the public to enable them to make accident notifications, Part 2 to doctors to enable them to make doctor's reports, and all sections to only inspectors to enable them to make investigation reports. The system should create an entry on the Complaint Register with a reference number, generate a PDF document of the form, and notify the complainant. The system should allow for uploading of evidence and reports by all parties, including the public, doctors, and inspectors, and should present an option for inspectors to take a subsequent inspection action. All complaints should be entered into a register with each complaint being tracked as per agreed timelines. Additionally, on completion of investigation and when a claim is found, the system shall present form DOSH for filling the claim details. During the filling of the claim form, the system shall automatically calculate the total claim as per the agreed parameters.

Reporting/Notifications Module

This module should be able to capture various types of reports such as death, dismissal, redundancies, strikes/lockouts, and distress calls. For death reports, the system should capture the cause and location of death and trigger an inspection by OSH or Labour for benefits. For dismissal reports, employers should upload evidence of the dismissal process and indicate the amount of wages due. For redundancy reports, employers should fill a notice one month prior, indicate the criteria and provide details on numbers, gender, occupation, sector, and region county. For strikes/lockouts reports, employers/employees should indicate the sector, notice period, region, and reasons. Finally, for distress calls, the system should capture details such as name, ID/passport number, employer/employment agency details, and the nature of distress and report to NEA or Labour Attaché.

Inspection Assignment Module

The Inspection Assignment Module should have the capability to assign inspection actions to inspectors, which may include statutory visits based on inspections, complaints or accident reports from Module 1 and 2, and other relevant criteria. It should be able to enable automated assignment based on agreed parameters, such as unit/speciality (OSH or labour law), workload, geography, or other criteria. This feature can save time and ensure that the most appropriate inspector is assigned to the task. Moreover, the module should allow managers to manually assign, cancel or pause inspection actions as needed, providing them with greater control over the inspection process.

Customizable Digital Inspection Checklist Module

The Customizable Digital Inspection Checklist Module should be designed to enhance the inspection process by allowing inspectors to view and check off topics in real time using a cell phone or tablet. The module must be easily customizable with an administrator login to keep up with the latest changes in laws and practices. Additionally, the module should provide inspectors with the ability to pull up content relevant to a specific issue, enabling them to quickly address any potential problems that arise during the inspection process. With these features, the Digital Inspection Checklist Module can streamline the inspection process, saving time and ensuring thoroughness in inspections.

Reports Module

The reports module should be able to visualize key inspection metrics, such as inspection actions undertaken by sector, location, and enterprise type, violations detected by sector and issue, remediation rates by sector and issue, and other to be determined metrics. Inspectors should be able to access this module, which automatically draws from the input fields of the Complaints Module, OSH Accident Reporting Module, and Case Management Module. The module also generates preconfigured reports, such as a report based on Part IV of the ILO Labour Inspection Recommendation R081, pulling from a static set of input fields. In addition, inspectors should be able to generate unique reports pulling from user-selected input fields, providing customized insights into inspection data.

Case Management Module

The case management module is responsible for tracking and managing inspection actions and complaint investigations. It should include the following functionalities:

- Allow the officer to generate a contravention notice or letter of improvement. Once all the minimum fields are entered, a PDF should be generated. The system should automatically sign the notice and send it to the contravening party via email (if available) with a link for them to acknowledge receipt and commit to correct the issues raised.
- Allow the contravening party to upload evidence of dealing with the corrective action(s) and the officer to upload evidence of dealing or not dealing with corrective actions.
- Allow the officer to enter a decision on whether compliance has been met or not. If yes, the system should generate a compliance certificate; otherwise, the case is linked to the appeal or prosecution process.
- The system should generate a notice of prosecution and a charge sheet from templates and forward the file to the Office of the Director of Public Prosecution (ODPP).
- Be linked to the ODPP system, if ODPP allows, to enable registration of the case and have a diary for entering court proceedings and dates.
- Track and trace inspection actions (at a minimum labour and OSH inspections and accident/complaint investigations).
- Include all the steps in each inspection action, from initiation to conclusion.
- Record start and end dates and required timeframes for each step. Replicate required input fields for standard forms used in some steps.
- Allow digital reviews and authorizations for different user roles at required decision points.
- Record transfers of actions to other authorities.

User Dashboard

The User Dashboard should provide a real-time status of current and pending actions, including alerts for upcoming deadlines. Inspectors should be able to use the dashboard to manage and review their workload and outputs. Managers should also be able to monitor the performance of inspectors under their supervision or the inspection system. The dashboard should provide a centralized location for users to access information and track progress.

Economic Units Database

The master list of economic units should be searchable for the inspectors to research previous inspection actions and findings. It should also be searchable and sortable for the selection of economic units for an inspection plan. The master list is preferably integrated with the most comprehensive registry of economic units in the country, and each economic unit should be linked to a unique identifier like the Tax Identification Number (TIN). The list should be automatically updated with manual entries from users to ensure accuracy and timeliness of information. Having a well-maintained and up-to-date master list of economic units would aid in efficient and effective inspection planning and implementation.

Data Analysis Module

The Data Analysis Module should enable the review and analysis of data from the Reports Module and Economic Units Database to target non-compliant economic units for inspection. Inspectors should be able to classify enterprises based on their infringement history and other indicators of non-compliance. The module should be integrated or aligned with other relevant internal or external systems to provide useful data for targeting. The data set should be built to enable predictive analytics in the future, enhancing the efficiency and effectiveness of the inspection process.

Labour Department Specific Modules

Attestation Module

This module should allow employers to download forms and provide details such as the number of workers, country of destination, and occupation/sector. Once the form is completed, employers can book a date for attestation. After the attestation, the system should provide feedback and remarks.

OSH Department Specific Modules

Approval of Consultants/Institutions Module

The Approval of Consultants/Institutions Module should be able to facilitate the approval process for consultants and institutions. The module should enable the completion of forms, attachment of credentials/certifications, payment of fees, submission to DOSH, and interview by DOSH. It should also allow for the upload of reports and the generation of certificates. The module should be accessible to the public and inspectors.

Approved Work (OSH Audits, Fire Audits, Examination of Plants, Training) Module

This module should be able to manage approved work activities, such as OSH audits, fire audits, examination of plants, and training. The module should require notification to the officer 14 days prior to the activity, with the submission of the report within 30 days after the activity. The report should be available to the employer after review, with actions taken by officers/employer on recommendation.

Architectural Plans Approval/Construction Sites Module

This module should be able to manage the approval process for architectural plans and construction sites. The module should enable the submission of plans, computation of charges, payment of charges, and approval of licences. The module should also allow for collaboration between the public, inspectors, and the system.

Registration of Workplaces and Renewal of Registration Module

The Registration of Workplaces and Renewal of Registration Module should enable the registration and renewal of workplaces. The module should include two tabs for Workplace and BCR registration and renewals, each containing forms for registration and renewal. Once a registration form is filled, the system should present the self-assessment form for the respective application. All applications should be entered into a register and presented on the dashboard. The system should allow for automatic or manual assignment of applications to various inspectors based on their duty station. Inspectors should be able to review the filled forms and decide whether to approve the application or not. Once an application is approved, the system should generate the certificate automatically and send it to the applicant in PDF format. If the application is not approved, the system should send reasons for rejection to the applicant.

Written Documentation

The service provider will develop and handover full system documentation. These documents must be current at the time of the handoff and cover the final version of the system implemented.

Required technical documents include:

1. Design documents that outline the design and architecture of the electronic case management system, including its various modules, features, and functionality. These documents may include flowcharts, diagrams, and other technical specifications that describe how the system works.
2. System database schema that refers to the underlying structure of the electronic case management system's database, which stores all the data associated with the system. This schema defines the various tables, fields, and relationships within the database and serves as a blueprint for the development and maintenance of the system's data storage. The Systems Manual is for use by those responsible for on-going maintenance of the system.
3. Application interface requirements that contain the specifications and guidelines for the graphical user interface (GUI) of the electronic case management system. This includes the layout, appearance, and functionality of the various screens, forms, and menus within the system, as well as any other user-facing components.
4. Technical support/Operations Manual. The Operations Manual contains information required for the production control group to run batch portions of the system, if any. The Operations Manual must be reviewed by the manager of the production control group. (The production control group is the group within the administrative computing department that is responsible for running batch portions of production systems.) This would include:
 - Overview of the system architecture: Provide a high-level overview of the system's hardware and software components.
 - Installation and setup instructions: Provide step-by-step instructions for installing and setting up the system.
 - System configuration: Provide information on how to configure the system, including setting up user accounts, roles, and permissions.
 - Troubleshooting: Provide guidance on how to troubleshoot common issues that may arise with the system, including error messages and connectivity problems.
 - Maintenance and updates: Provide information on how to maintain and update the system, including regular backups and system updates.
 - Security considerations: Provide guidance on how to secure the system and protect against data breaches.
5. User Documentation: The User Documentation contains instructions for the functional office(s) on how to use the system, and may be combined, if appropriate, with the functional office's internal procedures manuals. The User documentation is completed by the functional office(s) or the administrative computing department, or some combination of staff from these departments, and may consist of online help or a hardcopy manual, or a combination of the two. This includes:
 - Overview of the system: Provide an introduction to the system, including its purpose and key features.
 - User account setup and login instructions: Provide step-by-step instructions on how to set up a user account and login to the system.
 - User interface: Provide an overview of the system's user interface, including navigation, menus, and icons.
 - Modules and features: Provide detailed instructions on how to use each of the system's modules and features, including the Complaints Module, OSH Recording Module, Inspection Assignment Module, Digital Inspection Checklist Module, Reports Module, Case Management Module, User Dashboard, Economic Units Database, and Data Analysis Module.
 - Frequently asked questions: Provide answers to common questions that users may have about the system.
 - Glossary of terms: Provide definitions for technical terms and jargon used in the system.

Change management

The adoption of new technology requires effort and planning across change management tasks, capacity development and training to ensure a successful outcome. With any new software solution, staff may resist change to their current practice and process, citing the complexities of learning new technology and the perception of an additional workload. An Institutional Readiness Plan should be developed from the early conception phase. To ensure successful implementation, a well-planned change management strategy is essential, which should include the following key components:

Communication and Training Plan

A robust training plan is crucial to ensure that all users are equipped with the knowledge and skills required to use the system effectively. This plan should include a needs assessment to identify the training requirements, the development of training materials and modules, the delivery of training, and the assessment of training effectiveness.

Training of IT administrators: The service provider will develop a comprehensive training plan for the IT administrators that will inherit the maintenance and improvement of the system. The service provider will develop training materials (PowerPoint and handouts) and conduct hands on training of no less than 24 hours using the actual or dummy environment of the application. The training will include sessions on how the system is setup and configured to manage current and future functionality and existing design and development assets available for the application, including the operational handover and support information.

Training of end users: The service provider will develop a comprehensive training plan for end users (inspectors, managers, administrative professionals). The service provider will develop training materials (PowerPoint and handouts) and conduct hands on training of no less than 24 hours using the actual or dummy environment of the application. The training provided must include a combination of classroom and on-the-job training. The training will include sessions on the features of the system and the functions that each role will use in their day-to-day work. The training schedule must correspond to the system implementation and rollout schedule. The service provider must also take into consideration that not all staff from a given location can be released for training at the same time. Therefore, classroom training must be organized in such a way to ensure sufficient coverage in each location prior to go-live.

A clear and comprehensive communication plan is necessary to inform all users about the benefits of the system, its implementation timeline, and the changes in workflows and procedures that may result from its adoption. This plan should outline the key messages, communication channels, and frequency of communication.

Adjustment & Maintenance Strategy

A plan for adjustment and maintenance is necessary to ensure the system's ongoing functionality and relevance. A monitoring strategy should be put in place to track the implementation progress, identify any issues or challenges that arise, and measure the impact of the system on labour inspection activities. This strategy should include regular reviews, audits, and evaluations, as well as the use of performance indicators to measure the system's effectiveness. This plan should include regular updates to the system, the incorporation of user feedback, and the identification of opportunities for improvement. It should also include procedures for troubleshooting and resolving technical issues that may arise.

Testing

Programming and Unit Testing

Purpose

The programming and unit testing phase aims to complete the design and programming for each database and program in the system. The application developer is responsible for testing each portion of the system as it is developed. The developer shall involve the functional office in testing portions of the system as they are completed

(e.g., testing a screen as the processing for that screen is completed), whereas for other projects, functional office involvement in testing may be primarily during the System Testing phase.

Programming

The design of databases and programs is based on the Design document, either the Detail Design or General Design (where the Detail and General Design phases were combined). The programming must follow the standards and guidelines set by the Ministry for the programming language being used.

Unit Testing

The application developer should determine the required testing for a program. A test plan may be developed, which itemizes the test conditions to be covered during testing. The test plan can be a simple list for the developer's use or a more formal document if the functional office will be involved in testing or verification. In general, testing should cover the following:

- Testing every function performed by the program.
- For event-driven programs (e.g., online programs), testing every event and error conditions.
- Testing "boundary" conditions, such as testing the program's response to the maximum and minimum allowed values (for example, if an online program is designed to handle up to ten entries on a screen, then a test of entering ten or eleven entries and a test of entering zero or one entry should be performed).

Test results will be reviewed by the application developer, project leader, functional office, or a combination of these individuals or teams. The review of test results may be completed by the application developer, by the Project Leader, by the functional office, or by a combination of these staff.

System Testing

Purpose

System testing should be performed to ensure that all parts of the system work correctly as specified and work together. It is important because different components of the system are developed and tested independently, and system testing ensures that the entire system functions properly.

System Test Plan

The test plan must outline the steps and conditions for testing the system. It should identify who is responsible for developing test data, conducting the testing, and verifying the results. The functional office, which should be closely involved in developing the test data, verifying test results, and testing any online portions of the system. For some projects, the functional office may be heavily involved in preparation of the test plan as well.

The test plan should also specify the criteria for determining when testing is complete and who is responsible for making that determination. A schedule should be established for the test plan activities.

System Testing

System testing involves various types of testing based on the application requirements:

- Testing batch and online processes in conjunction with one another, such as testing data entry online and subsequent batch processing using the entered data.
- Testing different cycles of processing, such as daily and monthly processes, fiscal year-end closing processes, etc.
- Volume testing to ensure the system can handle a large amount of data effectively.
- Performance testing to confirm that the system responds adequately within acceptable time frames.
- Testing backup and recovery procedures to ensure data can be restored in case of failures.
- Testing procedures and processing for receiving files from other government sites or external organizations.

- Testing network interfaces like printing (lpr), file transfer (FTP), client/server processes, and other relevant processes.
- Testing workflow queue processing to verify the system handles queued tasks correctly.

Additionally, the following types of testing should be performed if appropriate for the application:

- Testing conversion processes or one-time data load processes.
- Parallel testing for systems that will replace all or part of an existing system.
- Testing interface processing for both incoming and outgoing interface files and the creation of outgoing interface files.

Pilot deployment

Phase 1

Phase 1 of the pilot deployment should include identifying a small group of users from the inspectorate. These users should be trained on how to use the system and given access to a test environment where they can explore its features and provide feedback on its functionality. The pilot should focus on a limited scope of the system's features and processes, to ensure that it can be effectively tested and evaluated. As the pilot progresses, the feedback from users should be used to refine the system and make improvements to its design and functionality. The success of the pilot will be measured based on how well the system meets the needs of users and improves the efficiency and effectiveness of the targeted processes. Once the pilot is complete, the lessons learned should be documented and used to inform the full-scale deployment of the system.

Phase 2

Phase 2 of the pilot deployment should include identifying one office for deployment. The users should be trained on how to use the system and given access to the real environment where they can explore its features and provide feedback on its functionality. This phase of the pilot should include all the system's features and processes, to ensure that it can be effectively tested and evaluated. As the pilot progresses, the feedback from users should be used to refine the system and make improvements to its design and functionality. The success of the pilot will be measured based on how well the system meets the needs of users and improves the efficiency and effectiveness of the targeted processes. Once the pilot is complete, the lessons learned should be documented and used to inform the full-scale deployment of the system.

Bug fixes

During Phase 2 of the pilot, refinements to the system should be made through a structured process that involves identifying, documenting, and prioritizing issues, and then addressing them in a timely and effective manner. The process typically includes the following steps:

- Issue identification: The first step is to identify the issues or bugs that need to be fixed or refined. This can be done through user feedback, system monitoring, or other means.
- Issue documentation: Once an issue is identified, it should be documented in a bug tracking system or issue tracker. This includes detailed information about the issue, including steps to reproduce it, severity, priority, and any relevant screenshots or logs.
- Issue prioritization: The next step is to prioritize the issues based on their severity and impact on users. This helps ensure that the most critical issues are addressed first.
- Issue resolution: After issues are prioritized, the development team can begin working on resolving them. This involves analyzing the root cause of the issue, developing a fix or solution, and testing it thoroughly to ensure it resolves the issue without introducing new problems.
- Testing and quality assurance: Once the fix or solution is developed, it should be tested thoroughly to ensure that it works as expected and does not introduce new issues. This includes unit testing, integration testing, and user acceptance testing.

Final Deployment

The final deployment to the other four office of an ECMS should entail a thorough testing and quality assurance process to ensure that the system is fully functional and meets all the necessary requirements. The deployment should include the migration of all necessary data and documents from the existing systems to the new ECMS (if data is available in a uniform and homogenized form). All associated user trainings, manuals, and documentation should be disseminated at this point.

Post deployment service/warranty/maintenance

This will include activities and services provided by the service provider after the system has been deployed and is in use. These services are meant to ensure that the system continues to operate effectively and efficiently and that any issues that may arise are addressed promptly. For the duration of the project, this includes:

- Bug fixes and software updates: The service provider will provide regular updates to the system to ensure that any bugs or issues that may arise are addressed promptly and that the system remains up-to-date with the latest technology and security features.
- Technical support: The service provider will provide technical support to the client, either remotely or on-site, to troubleshoot any issues that may arise and provide guidance on how to use the system effectively.
- Training: Depending on the institutional readiness plan, the service provider may provide additional training to users to ensure that they are using the system correctly and efficiently.
- Maintenance: The service provider will perform routine maintenance on the system, such as database backups, to ensure that it remains secure and operating effectively.
- Warranty: The service provider should offer a warranty period during which any defects or issues with the system will be addressed free of charge.

► Deliverables

Payments will be processed upon completion of each deliverable as expressed below.

All deliverables shall be submitted to the Technical Specialist for Strategic Compliance, Valkyrie Hanson (hanson@ilo.org) per the schedule.

To ensure that the ECMS is responsive to the needs of the Ministry of Labour, the ECMS development team will operate in close coordination with the established ECMS Task Force and the ILO.

Deliverable	Timeframe	Cost
Deliverable 1: Inception Report and change management strategy The inception report is a document outlining the work plan with proposed timeframes and processes to deliver according to the system requirements described in the scope of work. The document must onboard comments from inception meetings with ILO staff and the ECMS task teams and demonstrate review of the technical documents (workflows, wireframe, SRS, and others). The change management strategy is a document outlining how change will be managed during the development and deployment of the system and include a communication and training plan and an adjustment and maintenance strategy as outlined in the scope of work.	4 weeks	10% of contract amount

Deliverable 2: Development of the ECMS Modules Develop and validate the modules outlined in the scope of work. Validation sessions should be conducted with ILO staff and the ECMS task team after the development of each individual module and changes onboarded prior to the handover for payment under this deliverable. Development includes the setup of the infrastructure and application environments and code configuration; building the core ECMS application including database, unique identifier setup, security, language, and bootstrap customization of base forms/tables; development iterations (customization, review, and further modifications/configurations) of modules and associated functionality.	18 weeks	30% of contract amount
Deliverable 3: Pilot deployment and bug fixes Upon acceptance of the modules, the application must be pilot tested in two phases as described in the scope of work. Changes must be onboarded, and glitches and bugs must be fixed before payment under this deliverable. This includes Quality Assurance, including System Testing, Field Testing, and User Acceptance Testing.	6 weeks	10% of contract amount
Deliverable 4: User Documentation This includes Key Technical and User Documentation as required based on the updated technical design.	2 weeks	10% of contract amount

Deliverable 5: Final Deployment This includes the development of the final iteration based on feedback, and preparation of operational readiness and deployment in the remaining four offices.	5 weeks	20% of contract amount
Deliverable 5: Warranty Period	24 weeks	20% of contract amount

► Required Qualifications

- At least 7 years' relevant experience in design, development and deployment of Management Information Systems for government programs and systems, preferably in Kenya;
- Strong analytical skills to extensively analyze case management and workflows.
- A consultant with a team comprising Team Leader/Project Manager, Senior Full-Stack Software Developer, Software Developer, Systems Analyst/Quality Assurance Analyst and a Database Administrator with demonstrable experience in management information system deployment;
- Excellent communication and facilitation skills, including in multi-cultural settings.
- Command of English.
- Understanding of government structure and inter- government relations.

► Request for Proposals

Technical proposal

The Technical Proposal will be submitted in electronic (PDF) format. The Technical Proposal should include but not be limited to the following:

- a) **Request for Proposals for Services Form** (provided above).
- b) **Presentation of the Bidding Individual consultants**, including:
 - Name of the individual consultant;
 - Date and country of registration/incorporation;
 - Summary of corporate structure and business areas of the consultant;
 - Corporate directions and experience by the consultant;
 - Location of offices or agents relevant to this proposal;
 - Number and type of employees;
- c) **Relevant References** of the proposer (past and on-going assignments) in the past five-seven years. ILO may contact references persons for feedback on services provided by the proposers.
- d) **Samples or Links to Samples of Previous Relevant Work** listed as reference of the proposer (at least three), on which the proposed key personnel directly and actively contributed or developed the Management Information systems. Actual work examples for key services and solutions are appreciated.
- e) **System Development and Operationalization Methodology and Approach**. There is no minimum or maximum length.
- f) **Work Plan**, which will include as a minimum requirement the following:
 - General work plan based on the one proposed in the TOR, SRS with comments and proposed adjustments, if any; and
 - Detailed timetable by activity (it must be consistent with the general work plan and the Financial Proposal).
- g) **ECMS project development Team**:
 - Summary presentation of proposed experts;
 - Description of support staff (number and profile of developers, quality assurance and others etc.);
 - Level of effort of proposed experts by activity (it must be consistent with the Financial Proposal); and
 - CV of each expert proposed to carry out the MIS development and operationalization

NB: Only the technical proposal with the technical specifications should be shared. Individual Consultants who meet the technical specifications sought will be requested for financial proposals later.

Any submission in breach will automatically be disqualified.

All technical proposals should be shared by 15th December 2023.

Email: nboprocurement@ilo.org

Subject: Electronic Case Management System (ECMS) for the Ministry of Labour of Kenya