Expression of Interest (EoI)

Consultancy for Development DCI extensions for the Social Registry of Rwanda

Reference number: 83494786

1 Context

The Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH is a federally owned international cooperation enterprise for sustainable development with worldwide operations. The GIZ Office in Kigali covers GIZ's portfolio in Rwanda and Burundi. GIZ Rwanda/Burundi implements projects on behalf of the German Federal Ministry for Economic Cooperation and Development, the European Union and other commissioning authorities in the following priority areas: Sustainable Economic Development, Good Governance, Climate, Energy and Sustainable Urban Development, Digitalization and Digital Economy, Mineral Governance, Peace and Security in the Great Lakes Region.

1.1 DCI

The Digital Convergence Initiative, DCI, launched in 2021 under the Global Partnership for Universal Social Protection (USP2030), seeks to accelerate universal social protection through digital transformation and interoperability. DCI is supported by the EU's multi-Donor Action, co-financed by BMZ, and implemented by GIZ with partners like Expertise France, FIIAPP, ILO, and the World Bank, DCI aims to harmonize data sharing to improve program outcomes. This initiative aligns with the goal of achieving USP2030 by standardizing and integrating social protection systems globally, fostering collaboration among stakeholders, and leveraging digital solutions for inclusive, efficient social protection.

As part of DCI's commitment to enhance social protection delivery systems, DCI has been working on developing standards for the integration of seven key interfaces with Social Protection Management Information Systems. These interfaces include Civil Registration and Vital Statistics (CRVS), Integrated Beneficiary Registry (IBR), Social Registry, Disability Registry, Farmer Registry, ID-Systems, and Payment Systems.

The consensus-based interoperability standards focus on common processes, data elements, and APIs to enable organizational, semantic, and technical interoperability. The standards also align with the layers of the EU interoperability framework.

As part of EU Action, DCI is developing a knowledge product on best practices for consensus-based development, implementation, and management of interoperability standards. DCI is seeking one or a group of consultants with specific expertise to develop the knowledge product in collaboration with GIZ.

1.2 Social Protection in Rwanda

Social protection in Rwanda became a formal sector in 2008, after the first national social protection policy was developed in 2005, and the first economic development and poverty reduction strategy (EDPRS 1) was developed shortly after in 2007. To alleviate poverty through inclusive development, citizen participation, and support for overcoming socio-economic shocks, the country developed additional social protection-enhancing instruments, such as the 2011 national social protection strategy and the updated version of the national social protection policy released in 2020.

Rwanda's Ministry of Local Government (MINALOC) recently updated the social protection sector strategic plan (2024 to 2029), which is still undergoing some revisions. This new SP-SSP aligns with Rwanda's Vision 2050 and the new National Strategy for Transformation (NST2) and upholds Rwanda's commitment to reducing poverty, as enshrined in the country's constitution. The SP-SSP seeks to reduce poverty, empower vulnerable households, and build resilience in overcoming various socio-economic shocks. These goals are captured in the SP-SSP overarching objectives: protect people in poverty, promote people to move out of poverty and prevent people from falling (back) into poverty. The plan will halve poverty by half over the next 5 years by implementing well-defined strategic priorities (see Table 1).

Strategic Priorities	Brief Description
Create an enabling environment that empowers households to sustainably graduate out of poverty	Through the provision of safety nets, coaching, asset transfers, and financial literacy programs, the SP-SSP aims to empower households to achieve long-term economic independence.
Strengthen social protection systems to provide adequate benefits, while expanding coverage for poor and vulnerable people	Expanding coverage and improving benefits for vulnerable groups, including older persons, persons with disabilities, and children, is essential to achieve both coverage and poverty reduction targets.
Ensure that social security is extended to all people	Ensuring broader participation and coverage of social security schemes for the formal and informal sector workers, while expanding initiatives like Ejo Heza.
Ensure that all populations have access to health insurance	Ensuring 100% health insurance coverage, especially for the poorest, through the Community-Based Health Insurance.
Strengthen the contribution of social protection to prevent and reduce malnutrition	Strengthening income support and access to nutrition especially for children under five, pregnant women, and vulnerable mothers.
Ensure that all vulnerable groups have access to high quality social care services	Enhancing social services for vulnerable populations, including psychosocial support, reintegration packages, community-based rehabilitation and livelihood support.
Strengthen shock responsive mechanisms for all vulnerable people at risk of being pushed into poverty as a result of shocks	Developing disaster risk reduction strategies and shock-responsive cash and in-kind transfers to mitigate the effects of climate change and other crises.
Strengthened governance, M&E systems, evidence generation and cross cutting interventions	Improving institutional coordination and monitoring to track progress, ensure accountability and generate increased investment.

1. Table 1: SP-SSP Strategic Priorities between 2024 – 2029

Under the "protect" objective, the SP-SSP intends to enforce measures that safeguard poor households without labor capacity by ensuring they have access to minimum living standards through access to essential services and income support. Similarly, the plans will, under the "promote" objective, foster an enabling environment that offers income-generating opportunities to households with capacity labor so that they pursue improved livelihoods and move up the poverty ladder. Additionally, poor households' human capacity will be enhanced to pursue economic opportunities in the job market or as entrepreneurs. Lastly, the "prevent" objective ensures that no one falls back into the poverty trap. This will be achieved by putting

in place mechanisms to track households' progress and putting investments at their disposal to help them be resilient in the face of shocks that may affect their livelihoods.

The plan also recognizes the importance of cross-sector alignment for successful and comprehensive poverty alleviation programming. It integrates aspects of private sector development, financial inclusion and access to health services. With ongoing technological advances in Rwanda, the SP-SSP recognizes the role digital technologies and data can play in its realization. More specifically, the existing digital solutions in the social protection domain are crucial to the plan monitoring and evaluation system. The plan refers to three major systems that will serve as a reference for impact measurement for social protection interventions countrywide. They include the social registry information system owned by MINALOC, the monitoring and evaluation information system owned by LODA and the soon-to-be-developed graduation management information system.

1.3 Project background

Rwanda is actively pursuing the digital transformation of its social protection systems to enhance service delivery and improve outcomes for its vulnerable populations. Rwanda developed over the last years its own social registry system (called "Imibireho" Dynamic Social Registry (DSR)).

The Imibireho-DSR was a crucial step in the digitalization of the social protection sector. However, as the interoperability of the Imibireho-DSR with other administrative systems and with social protection MIS's is work in progress with integrations at different levels of progress including some not initiated yet, the current digital social protection landscape is still characterized by fragmented and siloed systems that limit the efficient sharing of data from other administrative systems and coordination with various social protection programs.

The Digital Convergence Initiative (DCI) aims to support the activities to address these challenges by supporting the interoperability between the social registry and other government systems and enabling business transformation of service delivery. DCI will thus support seamless data sharing, improve the tracking and management of beneficiaries, reduce the need for manual data collection and ultimately enhance the effectiveness of social protection programs. The initiative also seeks to align Rwanda's digital infrastructure with global standards to ensure the sustainability and scalability of the solutions implemented. The DCI initiative for Rwanda is embedded into the broader GIZ social protection program in Rwanda, collaborating closely with the World Bank to foster sustainability.

1.4 GovStack and other Enterprise Architecture approaches

The adoption of GovStack or similar enterprise architecture methodologies can play an important role during the implementation of this initiative.

GovStack as an example defines a methodology for the establishment and usage of building blocks to support platform based development.development. Rwanda has already implemented several building block based DPGs, among others:

- Government Business Intelligence Solution
- Government Enterprise Service Bus considered as information mediator building block
- Government Content Management Solution
- Government Workflow Solution
- Payment Platform Mojaloop, RSwitch

In addition it builds capacities throughout the digitization of Government services – on the governmental as well as non-governmental side and focuses on:

- **Awareness building:** across public and private stakeholders by trainings, participation on conferences, workshops, especially with:
    - Local private implementation partners
    - Government clients
    - Government institutions
- **Capacity Building:** enabling civil servants to understand and use the GovStack approach for improved service implementation
- **Operationalize** the adoption of the GovStack approach by establishment of implementation capacity.
- **Technical support:** support of ministries to adopt the GovStack approach by using four building blocks and supporting in the implementation of use cases to create evidence for the rapid adoption rate.

Utilizing the approach described, Govstack adheres to seven core principles during the stages of design, development, and roll-out.

For comprehensive specifications and more detailed information about Govstack, please refer to the following link: https://govstack.gitbook.io/specification/

2 Objective of the commission/subject of the procurement

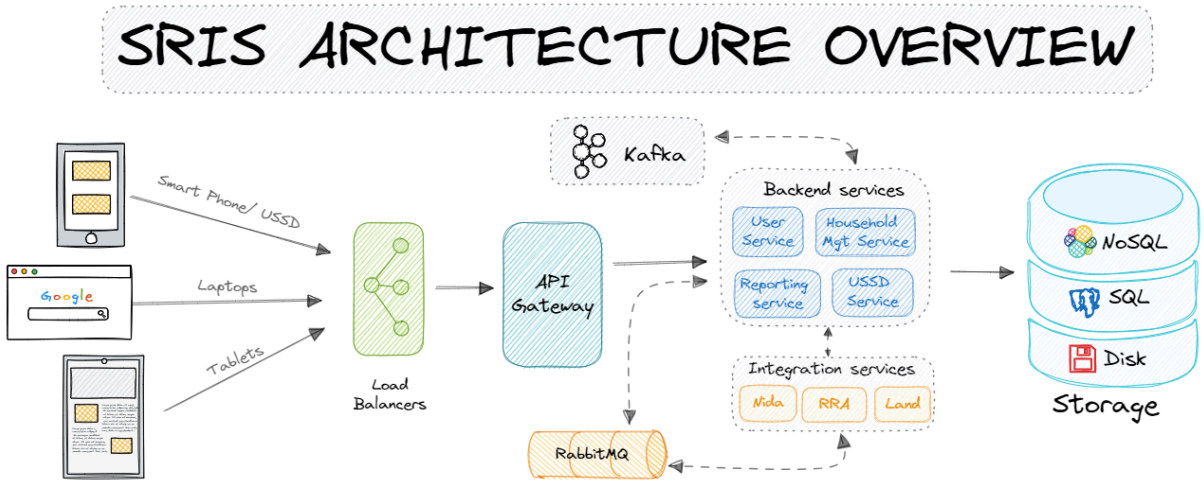
To strengthen Rwanda's social protection systems by establishing a harmonized and interoperable digital ecosystem that improves service delivery, data management, and beneficiary outcomes by

1. Promoting Interoperability and integration of social protection information systems.
    i. To achieve interoperability and integration based on standards between the social registry and four additional government systems (such as CRVS, RSSB (Rwanda Social Security Board), disability registry, farmer registryy), MINEMA MIS or Early Warning Information System (Ministry in Charge of Emergency Management)), facilitating efficient data sharing.

    While the integration of these systems with the Social Registry was already started, data exchange has not yet become fully operational and further work needs to be done. There will be a regular stock-take to assess where the integration stands and if these four systems remain the most relevant ones to focus on.

    ii. To implement an adapter for the Rwanda information mediator (Government Enterprise Service Bus) to integrate the above and other external systems based on interoperability standards with the Social Registry. (*The adaptor is a software component that serves as a bridge to connect any system to the information mediator*.)
2. Developing the design of the integrated beneficiary registry in a consultative process with the relevant stakeholders based on Social Protection data standards available and implementing a proof of concept.

2.1 Architecture



The SRIS is the core social registry for the Rwandan Government. It is divided into:

- Backend: Data Storage and Business Logic
- Frontend: UI/UX
- Business Intelligence Layer
- API Gateway: REST API access inbound
- Integration Layer:
    - Asynchronous via Kafka/RabbitMQ
    - Synchronous

It is connected to several endpoints already. None of the integrations is currently using a specific data sharing standard.

Integration Endpoints	Business Process	Integration Technology	SRIS type of data integration	Real time updates	Status
NIDA	During registration of a new applicant in the SR. Pulling demographic information like: • Identity • Age • Gender • Civil Status • Names	REST API via GESB	consumer	No	productive
LAND	During registration of a new applicant in the SR. Pull land information like: • Land	REST API via GESB	consumer	No	productive

	owned				
CRVS	Event based: • Birth • Death Used when initial creation and update based on new data.	Pub/Sub via Kafka	consumer	YES	productive
RRA (eTax)	During registration of a new applicant in the SR. Pull tax information, like: • Business owned • Income	REST API	consumer	No	In development
MoH (CHW), RSSB Mutuelle	Providing household composition like: • Head of household • Members • Location	REST API	producer	No	In development
DMIS	During registration of a new applicant in the SR. Pull land information like: • Disability category	REST API	consumer	No	In development

A further component for implementation is the GESB.

2.2 General Requirements

2.2.1 Onboarding, architecture validation, testing and QA approach.

The Contractor will be onboarded by MINALOC and GIZ, to understand the context, goals, approach, and results of the analysis done already. This will happen in several workshops, possibly with the involvement of example users. At the start of the project, the contractor, GIZ and a representative of MINALOC will clarify the expectations for the cooperation arrangement, the technical platform for cooperation, the relevant responsibilities, and the project schedule. The first meeting also allows substantive questions to be clarified regarding the issues, objectives to be defined, requirements to be established and other contextual information to be presented. All parties will set up the necessary recurring meetings for

planning events. In these workshops the vision for the project, a high-level product roadmap and corresponding assumptions dependencies etc. will be shared.

Also, the overall target architecture and resulting technical decision, especially regarding possible dependencies will be shared by the contractor in cooperation with MINALOC and GIZ. The Contractor is expected to lead these efforts and bring deep technical expertise, an independent outside view, and a focus on maintainable and sustainable operation.

The detailed testing approach for the user stories will be defined.

i. Report assessing target architecture, including proposed changes (pros, cons, etc)
ii. Agreed upon final target architecture.
iii. Shared understanding and formalized product roadmap and vision
iv. Formalized and agreed upon testing approach.
v. Well-groomed backlog with enough content for first sprints (items for sprint 2 can be detailed out in sprint 1, as they would normally).

2.2.2 Development Environment

The Contractor will set upand/or use least the following three environments:

i. Development environment on their own IT infrastructure (to be provided by contractor)
ii. Testing, integration, and staging environment on the MINALOC IT infrastructure.
iii. Production environment on the MINALOC IT infrastructure.

The contractor ensures that at least on the stage of the testing and integration environment installations are done through automated deployments where applicable including a set of automated tests that ensure at least that no broken build is deployed into the stage. The Contractor will help in automatic test data generation, if necessary, always following the guidance of MINALOC where applicable.

The Contractor will define and set up respective deployment and integration processes taking into consideration MINALOC processes. The deployment pipeline as well as environments need to be transferred or replicated to the MINALOC at the end of the project. The above environments shall have the same set up and configuration.

The implementation concept is drafted together with the contractor and other relevant stakeholders, and includes:

- Development methodology, schedule, and release plan
- Revised and prioritized functional requirements
- (Provisional) system architecture
- Depending on the methodology: description of the areas of application and system specifications or backlog, for instance with user stories
- Visualizations and outlines (e.g., mock-ups, user journeys, process outlines, ER and use case diagram)
- A documented “Definition of Done”
- A documented definition of production readiness
- Implementation concept
- Fully set up system environments
- Documentation about all environments

2.2.3 Code, Test, Deployment and Hand over

Testing requirements encompass a range of activities designed to validate that the system functions correctly and meets specified requirements. This includes unit testing, where individual components are tested for correct operation; integration testing, which ensures that combined components work together as intended; system testing, which validates the complete and integrated software system; and user acceptance testing (UAT), where actual users verify that the system meets their needs and is ready for production. Additionally, performance testing assesses the system's responsiveness and stability under load, while security testing identifies potential vulnerabilities. System resilience testing as well as fault tolerance testing are further necessary tests. Comprehensive documentation of test plans, cases, and results is essential to provide a clear audit trail and support future maintenance and troubleshooting efforts.

Deployment requirements involve the processes and procedures necessary to move the tested system into the production environment. This includes creating deployment plans that outline the steps for installation, configuration, and integration of the system. Automation tools are often utilized to streamline deployment processes and reduce the risk of human error. Pre-deployment testing in a staging environment that closely mirrors the production environment is critical to identify any last-minute issues. Rollback procedures should be clearly defined to allow for the system to revert to its previous state in case of deployment failures. Post-deployment, monitoring tools should be in place to ensure the system is functioning as expected and to quickly identify any issues.

Handover requirements involve transferring the ownership of the project from the development team to the operations or maintenance team, ensuring a smooth transition. This process typically includes the delivery of all relevant documentation, such as user manuals, system architecture designs, and maintenance procedures. Adequate training for the end-users and support staff is also critical to ensure they can effectively use and maintain the system. Additionally, the handover phase should include the establishment of a support framework, detailing how issues will be managed post-deployment, including escalation procedures and support contact details. The final acceptance sign-off from the client or end-users signifies that the system meets all agreed-upon requirements and is ready for operational use, marking the official conclusion of the project development phase.

2.2.4 Documentation

The contractor must provide detailed documentation of the functionalities and the source code annotation in good time and an appropriate manner. The contractor is obligated to make the latest documentation available for inspection at any time.

Work results to be provided by the contractor:

Documentation preferably based on a conventional standard (e.g., arc42 – arc42 is an example of a documentation standard)

1. The documentation must include the following items in particular:
    a. Software stack and dependencies
    b. System requirements, system specifications and system architecture
    c. Diagrams and outlines (e.g., use case, ERD, process outlines, mock-ups)
    d. Other technical documentation (e.g., interfaces, (clearance of) faults)

Continuously provide technical documentations which will facilitate the MINALOC technical team in operating and using it successfully on various phases of Solution implementation including the deployment, system administration and databases

Continuously provide user manuals which will facilitate the users in operating and using it successfully in various phases of the implementation.

2. Provide frequent technical knowledge sharing with the MINALOC technical team and other government stakeholders in various technical meetings during the implementation

of the Solution.

2.2.5 Continuous user support and operation

While the Contractor will not be tasked with operating the IT Solution, the contractor will be in close contact with the MINALOC support and operations team, which will in turn be assisted by the consultant assisting MINALOC and the other government stakeholders .

The following duties do not involve access to live systems and do not entail any tasks that could be interpreted as data processing of personally identifiable production data.

2.2.5.1 User-Support

The Contractor shall help resolve 2nd and 3rd level requests, where needed. Over time, the Contractor's involvement should decrease, with MINALOC having the tools, resources, and knowledge in place to run this support without the Contractor involvement, at the end of the contract. Until that point, Contractor personnel can also be asked to be part of incident response teams.

- 2nd Level Support: Classify and systematically process requests from 1st level support, contact users directly by phone or in writing, maintain a knowledge base on common problems or incidents, and forward/ re-classify unsolvable issues to 3rd level support.
- 3rd Level Support: Processing of inquiries regarding IT-administrative or operational errors or malfunctions, high specialization on respective software and hardware, no direct contact with end users

2.2.5.2 Operations

The Contractor will advise on the organizational and technical operation of the platform.

The Contractor will work together hand in hand with the MINALOC Technical Team on the operation of the platform.

This includes defining processes and roles, as well as giving guidance on improving the technical set up (e.g., deployment pipelines, code repositories etc.) – this shall be done in sync with the respective capacity management.

2.3 Functional requirements and Epics

The following building blocks are particularly in scope for the implementation of this tender.

Epics describe aggregated overarching functionality which consists of features and user stories.

2.3.1 Epic 1: System Architecture Definition and Validation

2.3.1.1 Covered components

- Social Registry
  - Backend: Data Storage and Business Logic
  - Frontend: UI/UX
  - Business Intelligence Layer
  - API Gateway: REST API access inbound
  - Integration Layer
- GESB

2.3.1.2 Scope and Business Background

This epic encompasses a comprehensive assessment of the existing integration processes and defining the architectural framework for the systems, creating low-fidelity prototypes and conducting experiments(A/B tests) to validate the proposed solutions. The proposed systems architecture, prototypes should meet the project requirements, objectives and get the stakeholder buy-in.

The scope of this epic covers the following objectives:

- Define the high-level architectural components, including infrastructure,user types, data flows, integrations points, and system interactions, to establish a solid foundation for development.
- Using design thinking approach, develop different low-fidelity interface designs (sketches, wireframes, mockups) to explore different architectures approaches and gather early feedback from all relevant stakeholders/users in the chain of custody. The prototypes should cover every level of data collection including tagging, approving, transporting and validating package information, considering every needed verification by different user types.
- Plan and execute experiments for the proposed interfaces aiming to assess their effectiveness and user preferences across all user types.
- Define and propose the technologies, frameworks and platforms to be utilized to meet the project requirements and get stakeholder buy-in.
- Compile all findings, including architectural decisions, A/B test results, and user feedback and any, into a comprehensive Product Requirements Document (PRD).

2.3.2 Epic 2: Integration of Backend Systems

2.3.2.1 Covered components

- Social Registry
    - Backend: Data Storage and Business Logic
    - API Gateway: REST API access inbound/outbound
    - Integration Layer
- MINEMA
- CRVS (adding further events)
- LAND (add near real time updates)
-
- NIDA (add near real time updates)
- DMIS (add near real time updates)
- GBIS push data
- RSSB (finalize implementation)

- Farmer registry

2.3.2.2 Scope and Business Background

Implement process integration for four additional government systems (currently planned CRVS, RSSB (Rwanda Social Security Board), DMIS, farmer registry, MINEMA MIS or Early Warning Information System (Ministry in Charge of Emergency Management)).

For each system the following topics should be covered:

- Assessment of processes to be covered for integration
- Decision for type of integration (asynchronous vs. synchronous)
- Assessment of data standard to be used
- Implementation of integration if possible, using the dci data standards

2.3.3 Epic 3: Standard GESB connector

2.3.3.1 Covered components

- Social Registry
    - Backend: Data Storage and Business Logic
    - API Gateway: REST API access inbound
    - Integration Layer
- GESB

2.3.3.2 Scope and Business Background

This epic involves the development of a software connector that enables systems such as the Integrated Beneficiary Registry (IBR), social registries, or BOMS to interact with the GESB—a custom-built middleware platform used by the Government of Rwanda for system integration and secure data exchange. The connector will be designed to ensure compatibility with globally recognized data exchange formats, such as the Social Registry Data Interoperability Standard from SPDCI. It will support both sending and receiving structured data payloads via GESB APIs, ensuring encryption, authentication, and schema validation. The connector will also be modular, extensible, and well-documented to support reuse across multiple systems.

Objectives:

- Understand the integration protocols, authentication mechanisms, and technical specifications of the GESB.
- Align the connector with standardized data structures (e.g. SPDCI for social registry, OpenSPP standards if relevant).
- Build and test a connector that can transmit and receive structured data securely via GESB endpoints.
- Validate the connector through integration with at least one live or test system (e.g. social registry or BOMS).
- Provide clear documentation and configuration guidance for other developers and system integrators.

Key Features:

- Support for common data exchange formats (JSON/XML) based on SPDCI standards
- Integration with GESB authentication and routing mechanisms (e.g. API keys, certificates)
- Mapping and transformation layer between local system schemas and standard formats
- Error handling, logging, and retry mechanisms for robust data delivery
- Plug-and-play architecture for reuse in different systems

Deliverables:

- Successful transmission and receipt of standard-compliant data payloads via GESB
- Demonstrated interoperability with at least one target system through GESB
- Compliance with defined GESB security and protocol standards
- Documentation including API specs, deployment guide, and data mapping templates
- Reusability confirmed by integration into at least one additional pilot system

2.3.4 Epic 4: Design and proof of concept for an integrated beneficiary registry

2.3.4.1 Covered components

- Social Registry
    - Backend: Data Storage and Business Logic
    - Frontend: UI/UX
    - Business Intelligence Layer
- IBR solution
- GESB

2.3.4.2 Scope and Business Background

This epic focuses on the conceptualization and prototyping of an Integrated Beneficiary Registry (IBR) that does not act mainly as a system of primary data entry, but instead serves as a federated aggregation layer. The IBR will access, link, and consolidate beneficiary data from existing sectoral or program-specific systems (BOMS or PMIS) in real time or near-real time. It aims to enable holistic beneficiary visibility, support program coordination, improve duplication detection, and enhance data-driven decision-making. The system architecture will emphasize interoperability, privacy-by-design, scalability, and alignment with digital public infrastructure principles.

Objectives:

- Define the technical and organizational requirements for a federated IBR.
- Design a high-level architecture for data integration, including APIs, interoperability mechanisms, and data harmonization strategies.
- Develop a Proof of Concept with selected BOMS to demonstrate data aggregation and linkage.
- Validate the consolidated beneficiary view with key stakeholders.
- Produce recommendations for scaling and production implementation.

Key Features:

- Federated data access through APIs or an information mediator (no central data storage)
- Unique beneficiary identification and linkage across systems
- Role-based access control and privacy safeguards
- Visualization of a unified beneficiary profile from multiple sources
- Scalable and modular architecture to integrate additional programs

Deliverables:

- Agreed-upon system architecture and data model across stakeholders
- Functional PoC connecting at least two BOMS and demonstrating successful data consolidation
- Demonstrated ability to retrieve and present linked beneficiary information
- Documented insights, challenges, and roadmap for scaling the IBR

2.3.5 Epic 5: Knowledge Transfer

2.3.5.1 Covered components

- Social Registry
    - Backend: Data Storage and Business Logic
    - Frontend: UI/UX

    - Business Intelligence Layer
    - API Gateway: REST API access inbound
    - Integration Layer
- GESB

2.3.5.2 Scope and Business Background

The Contractor shall conduct technical trainings, including on-the-job trainings, of the IT staff of MINALOC to build up the knowledge and capacities for sustainable operation.
Training will be formalized and well documented for major releases or when necessary due to new functionality etc. User trainings (except for admins) will not be part of the Contractor's tasks.

Capacity development will be continuous and entail three main blocks:

1) concrete tasks necessary to operate the platform via frequent exchange, alignment, and demonstrations.
2) best practices and principles in managing a digital product / service and steering the respective implementation and delivery via workshops based on expressed needs and current capacities.
3) guidance in setting up and implementing the necessary information security best practices via workshops and formal trainings sessions based on existing processes.

Respective activities shall be oriented towards the target group and be documented. Materials to be used here, shall be made available to MINALOC. The use of publicly available resources is encouraged. Concerning the knowledge transfer, the following services must be provided by the contractor to the concerned MINALOC staff through workshops and trainings on:

- Providing required technical knowledge and skills on the programming languages used in the development;
- Providing required technical knowledge and skills on databases;
- Providing required technical knowledge and skills on Solution API and integration with all required systems;
- Providing required technical knowledge and skills on the deployment and/or installation of the solution
- Providing required technical knowledge and skills on the solution management and/or administration;
- Providing required knowledge and skills on usage of the solution to the selected users.

2.4 Non-functional requirements

The following non-functional requirements must be considered by the contractor when implementing the service. The minimum baseline are as follows

1) **Portability**:
    - The solution shall always be able to run on both Linux and/or windows platforms.
    - The solution should run on latest Windows and MacOS systems with similar UI experience.
2) **Security:**
    - The implemented single-sign-on feature/module for the solution external will continue to be considered in further development of the system to allow users to log in and be redirected seamlessly to any other applications provided in

the future by MINALOC.
    - Develop the solution with all the standard security such as Owasp 10 web application standards security which can be in-built features to ensure confidentiality, integrity, and availability of data.
    - Ensuring that the solution have user access roles through which MINALOC technical team especially with administrator's rights can assign or revoke rights of a specific user to a function, data, element, action, or activity.
    - implement measures to protect collected data from unauthorized access, manipulation, or disclosure. This includes encryption of data during transmission and storage, user authentication mechanisms, and adherence to relevant data privacy regulations such as the MINALOC data policy and the MINALOC Member states data protection and privacy law
3) **Maintainability**: The solution will easily be updated, modified, or maintained over its lifecycle. It should easily be adapted to changing requirements with minimal effort, reducing downtime and costs associated with updates and enhancements.
4) **Reliability**: The solution system should consistently and accurately perform it's intended functions without failures or errors. A monitoring system should be put in place to track errors in real time.
5) **Scalability**: The solution system should handle the increase in requests without significant loss of performance.
6) **Performance**: The solution system should have a fast response time that enables the user to complete tasks quickly.
7) **Reusability**: The solution developed modules should easily be reused in different part of the the solution system or future modules.
8) **Flexibility:** The solution is developed with the mind of REST/JSON or any other API-based approach to enable future integration of the solution with other systems
9) **Compatibility**:

- The solution Web Applications (front and backend) shall be cross-browser compatible and cover at least the following browses:
    - Chrome (>version 55.0)
    - Firefox (> version 50.1)
    - Edge Chromium (> version 2020)
    - Safari (> version 16.6)
- The solution Mobile Application (to be developed) shall run on many versions of the mobile operating systems.

10) **Offline Data Collection**: Provide functionality for data collectors to capture data even in offline or low-connectivity with a mechanism to synchronize data with the national minerals databases once connectivity is restored.

2.5 Use of open-source software (OSS)

The solution, as a measure commissioned by MINALOC, must be available to the MINALOC free of charge. The following principles must be followed:

- Digital solutions must be built in such a way as to ensure handover to the partner organisation
- Solutions must lead to the strengthening of local capacity and digital resources
- The solution sets global technical standards; positioning MINALOC as an "early adopter" in the field of digital solutions
- Increasing efficiency through collaborative innovation processes
- Solutions have to be built to enable benefiting from international cooperation and alliances (e.g. DCI, GovStack).

The concept and infrastructure must therefore also be structured in such a way that they can be freely handed over to MINALOC and that MINALOC can also control support, operation and further development independently. This shall be achieved if the contractor only uses freely available open source components for the development of the application and makes it possible to hand over the infrastructure as an open source-licensed product.

Licensing Compliance: OSS components and their use must comply with their respective licensing terms. The contractor must ensure that all licensing conditions are met.

Documentation: The contractor must clearly document all OSS used, including the specific versions and configurations. The documentation shall outline the rationale for selecting each tool and detail how the OSS integrates into the broader system architecture.

2.6 Hosting

The contractor is responsible for furnishing a dedicated development environment to facilitate all development and testing activities. MINALOC will, in turn, supply staging and production environments to accommodate all deployment needs.

2.7 Further specifications/general conditions

Not applicable.

2.8 Other Requirements

The contractor's staffing profile should be balanced in terms of gender and age. GIZ supports the empowerment for people with disabilities. It would be beneficial if the supplier can include this into the personal concept.

3 Responsibilities of the contractor

The contractor must deliver the following services and work packages (along with the corresponding milestones). The work packages have no chronological order and can also be implemented on an integrated basis, depending on the development methodology.

3.1 Use of Agile Methodology

This project will be developed, delivered, and sustained in a consulting contract. The target is to go along agile methodology elements using a framework orientating on the agile frameworks. The proposed methodology seems to be appropriate because:

- general scope is pre-defined, but the periodization of requirements is not stable over the whole development process.
- learning about user behaviour and preference should be incorporated quickly into the product design.
- incremental development with integrated testing limits risks associated with large IT implementations and allows to achieve value-add quickly.
- it is a well-known and well described practice framework.

As this is a new way of working for MINALOC, the Contractor, together with the GIZ project are expected to act along principles of agile development, while also paying attention to context and organization-specific needs.

Iterative development based on the values of inspection, adaption and transparency will remain key, however if needed there are deviations from pure agile development (e.g., with regards to the stronger need for documentation, or the naming of specific roles).

The following main artefacts/roles will be used.

3.1.1 Sprint

Each sprint is a time boxed development phase which will be used to deliver ready to use products. The intention is, to add small features and user stories in each sprint to deliver an incrementally improved product. Each sprint shall have a two-week time box. The duration of the standard sprints can be adjusted as part of the retrospective.

3.1.2 Iteration/Product Increments (PI)

Each iteration is a collection of sprints, usually timeboxed with 3-month cycles.

3.1.3 Feature/User Story

Features and user stories are the artefacts which define the deliverables inside a sprint. They need to be described and documented. The team must agree on the “definition of done” for an agreement of completion of the respective artefacts. The difference between “user story” and feature for MINALOC is mainly the distinction between deliverables with a concrete impact on users (resp. user stories) like implementation of a specific dashboard or workflow or deliverables with no specific impact on users (resp. features) like implementation of a core data model.

3.1.4 Backlog

The Backlog covers the list of all features and user stories which are in scope or will be in scope for implementation. It acts as the pipeline for to be implemented artefacts.

3.1.5 Daily Stand-ups

Daily stand-ups are a standard approach as part of the SCRUM methodology. The scrum team coordinated by the team leader meets at a dedicated fixed and short time slot (usually 15 minutes) and answers one by one the following questions:

- What did I do yesterday?
- What will I do today?
- What are obstacles on my way?

Based on experience we have the DO’s and DON’T DO’s:

DO’s

0. Create and support an open environment and atmosphere.
1. Schedule follow ups for identified obstacles.
2. Be firm, be brief, be open.

Don't DO’s

3. Don’t use it for individual tracking.
4. Don’t expand the timeslot by going too much into the details (rather schedule follow up)
5. Don’t blame.

3.1.6 Retrospective, Review & Planning

As the iterations in MINALOC are quite short, best practice has been established to combine retrospective, review, and planning session. During this session the following activities are to be performed:

0. Review the result of the features planned for the current sprints based on the "definition of done".
1. Accept or reject completion status.
2. Review the "definition of done".
3. Review the preparation of features in the backlog.
4. Plan features or user stories for the current sprint
5. Adjust the approach if necessary.

3.1.7 Scrum team

The scrum team is the team which will deliver the final solution. As per the currently planned (to be revised setup) it consists of members of:

- Implementation team of the consulting team
- Implementation team of MINALOC and GoR

3.1.8 Product owner

The MINALOC project manager acts as the product owner for this project. He/she will provide priorities for project artefacts and finally accept or reject the implemented features or user stories.

3.1.9 PM-System and collaboration systems

The MINALOC and/or GoR uses "OpenProject" or "Trello" for project tracking and planning. This system shall be used for project planning and reporting by the contractor.

3.1.10 CI/CD Environment

The contractor shall use the MINALOC Data Cloud to share the source codes. However, depending on the assessment to be conducted prior to resuming the development of the solution, the contractor should use the GoR Gitlab in addition for versioning and CI/CD.

3.1.11 Continuous tasks for each sprint (Definition of Done)

In the planning, the development team agrees on a goal together with GIZ and MINALOC. The Sprint Goal is the single objective for the Sprint. Although the Sprint Goal is a commitment by the Developers, it provides flexibility in terms of the exact work needed to achieve it. The Sprint Goal also creates coherence and focus, encouraging the Development Team to work together rather than on separate initiatives. The sprint goal will be documented by the contractor as a user story or feature in the defined project management system and signed off for delivery as part of the sprint planning.

All the work necessary to achieve the product Goal happens within the sprint. In each sprint the following should be done (in addition to the delivery of the respective user stories for this sprint according to best practices):

3.1.11.1 Testing and quality assurance

For each user story there will be in-depth testing by the Contractor, but also by the proxy product owner (or deputy) provided by MINALOC. Final sign off will be given by the product owner based on the acceptance criteria and definition of done. While this process will evolve

over time, it is expected that security and privacy by design and by default is key in this implementation and a focus of the respecting testing efforts.

3.1.11.2 Documentation

Detailed documentation of the functionalities and commentary of the source code is to be provided by the contractor for all delivered user stories.

Overarching documentation (functional and technical documentation, architecture diagrams) is incrementally updated with each sprint and will be reviewed as part of each sign-off of user stories. It shall always update to reflect current system status.

The client sets up a test environment and, during and after the development process, conducts the relevant recommended tests (e.g., unit, integration, load). Tests are also conducted regularly with future users of the IT solution.

Work results to be provided by the contractor:

- A usable increment deployed at least into the testing and integration environment.
- Test documentation

3.1.11.3 Knowledge Sharing

For each implemented feature the MINALOC staff confirms that the following knowledge was transferred:

- How to use the feature;
- How to do administration of feature;
- How to troubleshoot the feature;
- How to do further adjustments on the feature; and
- How to deploy the system.

3.1.11.4 Iteration Review

Within this review the contractor, MINALOC and GIZ will have a look at the status of the product and discuss next steps and features which are expected from the contractor. In deviation to agile methods, the meeting does not constitute a formal acceptance or confirmation of performance. Nevertheless, results and agreements done within the meeting have to be documented by the contractor and will be assessed in following iteration reviews by the review attendances.

3.1.11.5 Time Reporting

The contractor is obliged to report the delivered hours against the defined user stories and features in the project management system of MINALOC. MINALOC will review these time sheets and forward them to GIZ for approval. MINALOC shall evaluate the performance of the contractor based on the deliverables set in the epics and iterations.

3.2 Continuous project management

The Contractor shall appoint an experienced project manager as a permanent contact person for the performance of the services over the term of the contract. The project manager who shall be responsible for project management on the part of the Contractor, including:

i. Regular progress reports, after each sprint (can be exports of project management tool)

ii. Provide monthly report for the ongoing progress in line with the implementation of the solution to the Technical Working Group (TWG) set by MINALOC and recommendation for future the solution functionality improvements.

iii. Input to high level product planning; feasibility assessments and high-level product design/ vision sessions that will be necessary before actual backlog items/ user stories are defined.

iv. Mobilizing additional expertise from respective support roles as needed

3.3 Planned Iterations/Product Increments (PI)

Each iteration is timeboxed with a timeline which shall be agreed on with the contractor during the assessment. It is a best practice to aggregate 6 sprints (each 2 weeks) per iteration. As per project management methodology the user stories and features for each iteration will be prioritized at the beginning of each iteration. The following description describes the current plan for the focus in each iteration. This focus can be adjusted as part of the iteration planning.

3.3.1 Product Increments 1:

The following epics will be the key focus for Iteration 1:

- Epic 1: Assessment and Architecture
- Epic 2: Analysis and roadmap planning,
- Epic 3: Gathering requirements, design
- Epic 4: Gathering requirements
- Epic 5: na

3.3.2 Product Increments 2:

The following epics will be the key focus for Iteration 2:

- Epic 1: Review against architecture
- Epic 2: pilot development for two connectors
- Epic 3: Pilot
- Epic 4: Design
- Epic 5: na

3.3.3 Product Increments 3 & 4:

The following epics will be the key focus for Iterations 3 & 4:

- tbd

4 Granting of rights of use

GIZ's and the partner's rights of use for the open source components are subject to the license agreements with the rights holder under the terms and conditions of the relevant open source license(s). The use of the open source components is ruled solely by the relevant open source license(s).

The provisions set out in sections 1.9 of the local GIZ Terms and Conditions do, however, apply to the software components developed by the contractor, unless these must be licensed as open source software because of obligations arising from an applicable open source license (copyleft effect). The contractor is responsible for checking whether any requirement of this nature applies and is required to inform GIZ of the outcome. If copyleft requirements apply, and the contractor has informed GIZ of this, the previous paragraph shall apply.

5 Data protection and information security

5.1 Data Protection

When the GIZ hires a contractor to build or upgrade a data processing system (platform, website, app etc.) on behalf of a local partner, who determines the purposes and means of the data processing activity, the GIZ does not bear ANY responsibility for such processing. Although the GIZ builds such systems in conformity with the highest data protection standards, however, its responsibilities end with the handing over of the systems to the partner. As a data controller, the partner must ALONE comply with all local and regional laws applicable to such processing (including the GDPR, where applicable). Consequently, the data protection principles such as lawfulness, data minimization, accuracy, purpose limitation, storage limitation, transparency, integrity and confidentiality, and accountability, as well as the numerous rights of the data subject should be paid due attention. We equally recommend the partner to conclude data protection agreements with the hosting service provider(s) and the maintenance service provider(s), where applicable. The GIZ would be available to support the partner whenever the need arises.

The contractor should comply with the data protection and privacy law according to the data protection offices of MINALOC Member states.

5.2 Information security

The following points must be considered by the contractor and if they are not within the contractor's responsibility or scope of work, they must at least be discussed with the partner's project team in order to close any existing security gaps.

The Contractor must inform the Client immediately and in an appropriate form about security incidents that may affect the Client. If the Customer has appointed an IT security officer or another person to receive such information, the information must be sent directly to this person.

A firewall must be installed upstream of the server (e.g., authorized IP addresses/GEO blocking or address ranges for logging on to the system can be entered here or also excluded for this purpose).

Up-to-date anti-virus software must be used on the server and configured accordingly for automatic updates.

Network communication between the components of the application should be encrypted.

Hard-coded keys (symmetric/asymmetric) should not be included in the application. If this is

unavoidable, the handling of the key must be described. The information security risks related to the storage of the key must be evaluated.

The transmission of authentication information (especially passwords) must be encrypted. The storage and transmission of sensitive and/or personal data must comply with current encryption standards.

Session cookies used for logins must be deleted after logging out from the client.

Separation of application and data is to be provided, i.e. an application server and a separate server for the database and file storage is provided, with communication through a firewall.

A system log is to be implemented in which at least logins and logouts of all users and actions such as updates, backups, uploads and downloads, changes to account data and authorizations, as well as all security-relevant actions and events are to be logged and documented. The inclusion of further log data is still to be discussed in detail with the project. The system log is to be documented in the operating manual.

The error messages generated by the application (especially exception handling/exceptions) must not provide any information that allows conclusions to be drawn about the architecture or software/software versions used.

When configuring the web server, you must pay attention to the following**:**

- Disable Trace HTTP Request
- Run as a separate User & Group
- Disable signature
- Disable banner
- Restrict access to a specific network or IP
- Use only TLS 1.2
- Disable Directory Listing
- Remove unnecessary DSO modules
- Disable Null and Weak Ciphers
- periodically updates of the system -> stay current!
- periodically checks of the system log files

The system must be hardened against SQL injection. In detail, this concerns the validation, filtering and cleansing of user input. The inputs may only have expected properties and characters and may not contain any unauthorized metacharacters that are passed to the SQL interpreter.

When implementing API interfaces, it is essential to harden them against malicious code injection (SQL injection, etc.) via the URL.

The system must be protected against Cross Site Scripting (XXS) on the client side. The server(s) must be protected against reflected or persistent cross site scripting by securing the server source code. All data to be processed by the server must be validated before execution.
Whitelists of permitted data can be used for this purpose. General conversion of certain script characters is also a popular method. It is to be prevented that executable metacharacters of the scripts are read by the server. Cookies should only be read by the server (HttpOnly) and not by JavaScript in the browser.

A password policy must be implemented, which should look like this:

- minimum number of digits e.g. 12
- latin capital letters (A-Z)
- lower case Latin letters (a-z)
- basic digits (0-9)
- non-alphanumeric characters (like !, $, #, -
, &)
- your password must not contain the whole or parts of your login name!
- after 5 wrong entries the account should be locked for 3 minutes
- max. password age 90 days
- password history, at least 5 different passwords in before a previously used password is accepted again, new passwords that differ only by consecutive numbers should not be accepted.

Passwords must not be stored in plain text. Passwords may only be stored as hash values. The hash algorithm must conform to the current recommendations of the BSI (technical guidelines).

Hard-coded passwords must not be included in the application. The transmission of authentication information (especially passwords) must be encrypted.

2-factor authentication is to be implemented; Google Authenticator is not to be used for this. 2FA is to be possible via multiple channels (app, SMS or e-mail).
A role and authorization concept must be implemented that includes at least the roles of system admin (full authorization to the entire system), CMS admin (+account management), editor and author (editing content/articles). The application to be developed must be operable with minimal system rights. Only the following user groups may have access to the backend: Developers and administrators of the Contractor as well as employees for editorial maintenance of the Contractor. Nevertheless, the contractor will only have access to the anonymized data in the development and staging environment.

Access to the backend at the operating system level may therefore only be granted to very limited user groups with the appropriate expertise.

There must be a documented authorization concept for each application (e.g. in the operating manual).

In order to minimize operating errors (human errors), the ergonomics of the application should be designed safely according to the need for protection.

Changes to account data that are required for registration may only be made by the administrators and are to be blocked for the user.

For the upload of files, appropriate file filters are to be provided so that no files with executable content (scripts, programs or SQL codes) can be uploaded and executed.

The regular backups of the complete system are to be carried out by the Contractor and checked accordingly for usability (restore). The backup can be stored on the server, but a copy must always be stored offline to prevent loss through hacker attacks. The intervals for the backups are to be coordinated with the project.

Important backups always belong offline on another system and must be validated!

The deletion procedure must be proven upon request. Legal retention obligations remain unaffected.

6 Language

The services are to be provided in English.

7 Technical-methodological concept

In the conceptual design of the tender (technical-methodological approach, project management, if necessary other requirements), the tenderer is required to take specific objectives and requirements into consideration and describe them, as explained below.

7.1 Requirements for the technical-methodological concept (section 1 of the assessment grid)

In the tender, the tenderer is required to show *how* the services specified in section 3, where relevant taking account of other specific methodological requirements (section 2), are to be provided (technical, methodological concept).

7.1.1 Assessment of the requirements:

The tenderer must assess the objective and the requirements of the IT solution (see sections 1 and 2) in relation to feasibility and to what particular (non-)technical difficulties must be considered in the IT solution to be developed by the tenderer regarding the objective (section 1.1 of the assessment grid).

7.1.2 Project management and development methodology:

The tenderer should consider the design of the project management process and describe his or her methodology for development/implementation, considering the described requirements (section 2 and 3) and compliance with the milestones (section 3) (section 1.2 of the assessment grid).

7.1.3 Operational plan/personnel assignment plan:

The tenderer must create and explain an operational plan that also includes a personnel assignment plan for all the specialist staff that he or she offers. The operational plan must depict the assignment periods (time and expert days) and describe the necessary work steps and take account of and, where necessary, supplement section 3.3 (section 1.3 of the assessment grid).

7.1.4 Test and documentation concept:

The tenderer must describe the process for testing and documenting the IT solution and the IT security and documentation standards used (section 1.4 of the assessment grid).

8 Human resources

8.1 Human resources concept

The tenderer is required to provide staff for the positions (‘experts’) referred to and described here in terms of the scope of tasks and qualifications based on corresponding CVs (see section 7).

The qualifications specified below meet the requirements for achieving the highest score in the technical assessment.

Expert 1: Team Leader, Architect and Project Manager (Section 3.1 of the assessment grid)

Tasks of the Expert

- Overall responsibility for the advisory packages of the contractor (quality and deadlines and scope).
- Coordinating and ensuring communication with GIZ, MINALOC, partners and others involved in the project.
- Personnel management, identifying the need for short-term assignments within the available budget, as well as planning and steering assignments and supporting local and international short-term experts.
- IT Architecture for the solution
- Regular reporting in accordance with deadlines; and
- Making himself/herself available when needed by the GIZ and MINALOC as beneficiary.

Qualifications:

Education/training (section 3.1.1 of the assessment grid):	University qualification (Masters, Bachelor or equivalent) in computer science, Computer engineering, or relevant field with skills in project management or having certificate from a recognized institution like PMI or Prince2, A is added advantages
Language (section 3.1.2 of the assessment grid):	Good business language skills in English (C1), with good Kinyarwanda language skills (C1)
General professional experience (section 3.1.3 of the assessment grid):	7 years of professional experience in the IT sector
Specific professional experience (section 3.1.4 of the assessment grid):	2 years of professional experience with the architecture design of Complex systems (Front-end, Back-end, mobile app, integrations with minimum 5 other systems) with the use of open-source software as well as professional experience in business analysis and product management
Leadership/management experience (section 3.1.5 of the assessment grid):	5 years of project management experience as IT project team leader in a company or as a lead architect overseeing a team of developers.
Development cooperation and regional experience (section 3.1.6 of the assessment grid)	1 year of experience in projects in Africa (region) and 1 year experience working with development cooperation.

Expert pool 1 'Software Development Team' with minimum of 1 to maximum 3 experts Section 3.5 of the assessment grid)

The experts can be exchanged during the contractual period in consultation with the officer responsible for the commission.

A CV for each expert must be added to the tender.

Exclusion criterion: If one of the marked exclusion criteria is not fulfilled the entire offer will be excluded.

Task of the Expert Pool

- Support team leader in the implementation of the defined tasks

Qualifications:

Education/training (section 3.5.1 of the assessment grid):	All experts with university qualification (Masters or Bachelor or equivalent) in computer science, Computer engineering, or relevant field
Language (section 3.5.2 of the assessment grid):	All experts with good business language skills in English (C1), all experts with good Kinyarwanda language skills (C1)
General professional experience (section 3.5.3 of the assessment grid):	7 years experience in web-based software development.
Specific professional experience 1 (section 3.5.4 of the assessment grid*):*	Additional experience in software integration will be assessed. 2 years is the baseline, and 5 years as scores the maximum. 1 expert with a 3 years experience in the development of state of the art software integration and backend implementation.
Specific professional experience 2 (section 3.5.5. of the assessment grid):	Additional experience in devops. 2 years is the baseline, and 4 years as scores the maximum. 1 expert with 3 years experience in the development of state of the art devops implementation.

Expert pool 2 'Business Analyst Team' with minimum of 1 to maximum 3 experts Section 3.6 of the assessment grid)

The experts can be exchanged during the contractual period in consultation with the officer responsible for the commission.

A CV for each expert must be added to the tender.

Task of the Expert Pool

- Support team leader in the implementation of the defined tasks specifically in the area of business analysis

Qualifications:

Education/training (section 3.6.1 of the assessment grid):	All experts with university qualification (Masters or Bachelor or equivalent) in computer science, Computer engineering, or relevant field
Language (section 3.6.2 of the assessment grid):	All experts with good business language skills in English and with good Kinyarwanda language skills
General professional experience (section 3.6.3 of the assessment grid):	All experts with a minimum of 5 years of professional experience in business analysis. Additional experience in business analysis for web-based software development will be assessed. 5 years is the baseline, and 7 years as scores the maximum.

The tenderer must provide a clear overview of all the proposed experts and their individual qualifications.

Soft skills of all team members

In addition to their specialist qualifications, the following qualifications are required of team members:

Physical availability at the beneficiary site when required.

9 Costing requirements

Fee days	Number of experts	Number of days per expert	Total	Comments
Expert 1	**1**		**140**	To be delivered in Kigali
Expert pool 1	**1-3**		**200**	To be delivered in Kigali
Expert pool 2	**1-3**		**100**	To be delivered in Kigali

10 Requirements on the format of the tender

The structure of the tender must correspond to the structure of the ToR. It must be legible (font size 11 or larger) and clearly formulated. The language in which the tender must be written is English.

The technical-methodological concept of the tender (section 7 of the ToR) is not to exceed 12 pages (not including the cover page, list of abbreviations, table of contents and brief introduction).

The CVs of the staff proposed in accordance with section 0 of the ToR must be in the EU format and not exceed four pages in length. The CVs must clearly show what position the proposed person held, which tasks he or she performed and how many expert days he or

she worked during which period in the specified references. The CVs should be submitted in English.

We strongly request that you do not exceed the number of pages specified.

11 Submission of the offer

11.1 Technical offer

Technical offer must include the following documents:

Eligibility documents:

- Self-declaration of eligibility for the award
- Company administrative documents: registration certificate (RDB), VAT registration certificate and Valid Tax clearance certificate
- Three Company References for the completion of similar assignments in the last 3 years, as described in the eligibility assessment grid

Technical proposal:

- Technical Proposal (**attached template for technical proposal MUST be used)**
- Up to date CVs of proposed experts

11.2 Financial offer:

Financial offer indicates the all-inclusive total contract price, supported by a breakdown of all costs as described in the specification of inputs. The costs **must be in RWF and VAT** excluded (**Price sheet must be used**).

Your EoI has to be submitted in **2 separated emails** to **RW_Quotation@giz.de** until latest **27.11.2025:**

1. **The technical offer** has to be submitted in 2 **PDF file format (eligibility/technical)** and **as attachment to the email** with the subject: **83494786 -Technical offer.**
2. **The financial offer** has to be submitted in **PDF format** and **as attachment to the email** with the subject: **83494786 - Financial offer.**

If the emails exceed the default email size of **30MB**, offers can be exceptionally submitted through **https://filetransfer.giz.de/, as indicated. The subject of recipient notification must be edited with the subject indicated above** and the notification message **must include the password to access the files.**

Offers submitted through any other sharing platform, as google documents or similar will not be considered.

Without the subject mentioned, your offer may not be considered

Offers submitted in hard copy will not be considered.

GIZ reserves all rights.

Annexes:

Annex 1 - Eligibility assessment grid
Annex 2 - Self-declaration of eligibility for the award
Annex 3 -Technical assessment grid
Annex 4 - Technical Proposal template
Annex 5 - Price sheet
Annex 6 – General terms and conditions

12 List of abbreviations

API	Application Programming Interface
CRVS	Civil Registration and Vital Statistics
CV	Curriculum Vitae
DCI	Digital Convergence Initiative
GBIS	Government Business Intelligence Solution
GESB	Government Enterprise Service Bus
GIZ	German Agency for International Cooperation
GoR	Government of Rwanda
IBR	Integrated Beneficiary Registry
ICT	Information and Communication Technology
IT	Information Technology
JSON	JavaScript Object Notation
LODA	Local Administrative Entities Development Agency
MINALOC	Ministry of Local Government

NLA	National Land Authority
REST	Representational State Transfer
RISA	Rwanda Information Society Authority
SP-SSP	Social Protection Sector Strategic Plan
SRIS	Social Registry Information System
ToR	Terms of Reference