Terms of Reference (ToR) for the procurement of IT services

Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

CONFIDENTIAL

Project title:	**Processing number/cost centre:**
Strengthening Development Finance through Combating Illicit Financial Flows and Effective Debt Management (SFIFD)	**G-012142-009**
Country: Ethiopia	**Transaction number:**
Works/services to be put out to tender:	**10034893**
Development and Implementation of a Website and integrated Content Management System	

0. Abbreviations 4

1. Context 7
1.1 The Company 7
1.2 Project Background 7
1.3 Objective of the commission/subject of the procurement 8

2. Requirements for the IT solution 8
2.1 Framework concept for the IT solution 8
2.1.1 Description of the application/use of the IT solution 8
2.1.2 General conditions at the partner end (where relevant) 9
2.1.3 Use of open-source software (OSS) 10
2.2 Infrastructure Requirements 10
2.2.1 Deployment Environments 10
2.2.2 Hosting 11
2.2.3 Technical Security Requirements 11
2.3 Functional requirements 12
2.4 Non-functional requirements 13
2.4.1 Interfaces 14
2.4.2 System requirements/technical framework 15
2.4.3 Sustainability 15
2.5 Further specifications/general conditions 16

3. Responsibilities of the contractor 17
3.1 Work package 1: Kick-off 17
3.2 Work package 2: Drafting the implementation concept 17
3.3 Work package 3: Technical implementation 18
3.4 Work package 4: Testing and quality assurance 19
3.5 Work package 5: Documentation 19
3.6 Work package 6: Training 20
3.6.1 Administrative training 20
3.6.2 User training 20
3.7 Work package 7: Support (and operation) 21
3.8 Work package 8: Project management 21
3.9 Work package 9: Monitoring and reporting 22
3.10 Work package 10: Deployment and Handover 22

4. Term, schedule and milestones 23

5. Granting rights of use 24

6. Data protection 25

7. Information security 25

8. Language 26

9. Technical and methodological concept 26

9.1 Requirements for the technical and methodological concept (Section 1 of the assessment grid) 27

9.1.1 Assessment of the requirements 27

9.1.2 Project management and development methodology 27

9.1.3 Operational plan/personnel assignment plan 27

9.1.4 Test and documentation concept 27

10. Human resources 27

10.1 Key Expert 1: Team Leader / IT Project Manager (Section 3.1 of the assessment grid) 28

10.2 Expert 2: Business Analyst / Solution Architect (Section 3.2 of the assessment grid) 29

10.3 Expert 3: UI/UX and Accessibility Specialist (Section 3.3 of the assessment grid) 30

10.4 Expert 4: DevOps, Hosting and Security Engineer (Section 3.4 of the assessment grid) 30

10.5 Expert 5: QA, Testing and Acceptance Specialist (Section 3.5 of the assessment grid) 31

10.6 Expert 6: Documentation, Training and Knowledge Transfer Specialist (Section 3.6 of the assessment grid) 32

10.7 Expert 7: Content, Localization and Stakeholder Support Specialist (Section 3.7 of the assessment grid) 33

10.8 Expert 8: Pool 1 ‘Senior Full-Stack / CMS Developer’ with 2 experts (Section 3.8 of the assessment grid) 34

10.9 Expert 9: Pool 2 ‘Backend/API and Database Developer’ with 2 experts (Section 3.9 of the assessment grid) 36

11. Costing requirements 37

11.1 Assignment of experts 37

11.2 Travel expenses 38

11.2.1 Travel – sustainability considerations 38

11.2.2 Travel expense requirements 38

11.3 Materials and equipment 39

11.4 Workshops, training 39

11.5 Hosting 40

11.6 Other costs 40

11.7 Flexible renumeration 40

12. Requirements on the format of the tender 40

13. Annexes 41

0. Abbreviations

Abbreviation	Meaning
AML/CFT	Anti-Money Laundering / Countering the Financing of Terrorism
API	Application Programming Interface
AU	African Union
BMF	Federal Ministry of Finance
CDN	Content Delivery Network
CI/CD	Continuous Integration / Continuous Deployment
CMS	Content Management System
CO^2	Carbon Dioxide
CSS	Cascading Style Sheets
CT	Case Tracking
CV	Curriculum Vitae
DB	Database
DR	Disaster Recovery
eGP	Electronic Government Procurement
ERD	Entity Relationship Diagram
EU	European Union
EVB-IT	Supplementary Terms and Conditions for the Procurement of IT Services
FAQs	Frequently Asked Questions
FATF	Financial Action Task Force
FHC	Federal High Court
Figma	Collaborative Interface Design and Prototyping Tool
FR	Functional Requirement
GIZ	Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH
GWB	German Competition Act

Abbreviation	Meaning
HA	High Availability
HTML	Hypertext Markup Language
HRM	Human Resource Management
HTTPS	Hypertext Transfer Protocol Secure
ICT	Information and Communication Technology
IFFs	Illicit Financial Flows
IP	Internet Protocol
IT	Information Technology
MFA	Multi-Factor Authentication
NFR	Non-Functional Requirement
OSS	Open-Source Software
PDF	Portable Document Format
PHP	PHP: Hypertext Preprocessor
QA	Quality Assurance
RBAC	Role-Based Access Control
SaaS	Software-as-a-Service
SDG	Sustainable Development Goal
SDLC	Software Development Life Cycle
SLA	Service Level Agreement
SMTP	Simple Mail Transfer Protocol
SRD	Software Requirements Document
SRS	System Requirements Specification / Software Requirements Specification
SSL	Secure Sockets Layer
TLS	Transport Layer Security
ToR	Terms of Reference

Abbreviation	Meaning
UAT	User Acceptance Testing
UI	User Interface
URL	Uniform Resource Locator
UX	User Experience
VgV	German Ordinance on the Award of Public Contracts
WCAG	Web Content Accessibility Guidelines
WP	Work Package

1. Context

1.1 The Company

The Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH supports the German Federal Government in achieving its objectives in the field of international cooperation for sustainable development and international education. The company is active in several fields: economic development and employment; governance and democracy; peacebuilding, security, reconstruction and civil conflict transformation; food and nutrition security, health, basic education, environmental protection, resource conservation and climate change mitigation.

1.2 Project Background

Countries lose billions of dollars every year due to illicit financial flow (IFFs). A substantial share of these funds could be used to fight poverty and hunger, and to invest in a sustainable future. In addition, ensuring the integrity of the financial system through the implementation of international Anti-Money Laundering/ Countering the Financing of Terrorism (AML/CFT) standards is an important prerequisite for a jurisdiction in order to mobilize private and public finance for investment.

GIZ is a co-implementing partner of the #TeamEurope project called SecFin Africa which is implemented by a consortium of Expertise France, GIZ, Civipol, FIIAPP and the Swedish Tax Authority. The SecFin Africa project aims to support Sub-Saharan Africa countries to prevent and combat illicit financial flows (IFFs), by strengthening anti-money laundering and countering the financing of terrorism (AML/CFT) efforts, in line with international standards. By aligning with the African Union's Agenda 2063 (e.g., Goal 20 on Financing Development) and the United Nations Sustainable Development Goals (e.g., Target 16.4 on reducing IFFs), SecFin Africa contributes to boosting domestic resource mobilization, fostering sustainable development and promoting security across the continent.

One pillar of SecFin's three-pillar approach is the country level support: The EU Action aims at strengthening AML/CFT compliance and effectiveness with partner countries by providing tailored, demand-driven technical assistance and training covering the entire chain – from detection, assessment, investigation, prosecution to asset recovery – ensuring alignment with the international standards of the Financial Action Task Force (FATF).

The background of the assignment hereby put out for tender is part of the program field of intervention "financial investigation" and "asset recovery", specifically referring to the support of key actors in the AML/CFT space, namely the Judiciary. The Federal High Court (FHC) of Ethiopia currently lacks an official website, a gap that significantly impedes its ability to disseminate vital judicial information and deliver online services to the public, legal professionals, and key institutional stakeholders.

The lack of a unified digital presence at the FHC reduces transparency, delays access to legal resources, and limits service efficiency for litigants and stakeholders.

Therefore, GIZ aims to support the FHC to develop a website with an integrated digital judgment repository and access system which shall serve as a centralized, secure, and efficient mechanism for the systemic storage, management, and retrieval of court judgments.

1.3 Objective of the commission/subject of the procurement

GIZ and FHC have already completed the scoping and design phase of the project. The System Requirements Specifications and a Figma prototype of the envisioned system are attached as annexes and shall serve as the main functional and design reference for the assignment.

Accordingly, the subject of this procurement is the validation, refinement, development, implementation, testing, deployment, handover and support of the FHC website and related administrative functions. The contractor shall develop the system in accordance with the System Requirements Specifications and shall use the Figma prototype as the main orientation for user interface and interaction design. The contractor is not expected to conduct a full new discovery or re-design exercise, but shall validate assumptions, clarify dependencies, refine the implementation concept, and prioritise delivery jointly with FHC and GIZ before development begins.

In case of inconsistency between the SRS, Figma prototype, these ToR, and the agreed implementation concept, the contractor shall identify the inconsistency during the validation phase and submit it to FHC/GIZ for decision. The written SRS and the agreed implementation concept shall prevail for functional scope, while the Figma prototype shall serve primarily as the visual and interaction design reference.

2. Requirements for the IT solution

The IT solution shall be developed as a secure, scalable, responsive, and user-oriented website for the Federal High Court of Ethiopia. It shall serve as the official digital platform for court-related information, public communication, selected online services, judgment/publication access, content management, and controlled interaction between the Court and its stakeholders. The solution shall be implemented in accordance with the System Requirements Specification, the approved Figma prototype, applicable government ICT requirements, data protection principles, accessibility standards, and the functional and non-functional requirements described below.

2.1 Framework concept for the IT solution

The framework concept is based on the establishment of a centralized, authoritative, and sustainable digital platform for the Federal High Court. The solution shall combine a public-facing website with a secure administrative and content-management environment, enabling authorized staff to manage court information, notices, judgments/publications, vacancies, tenders, feedback, and other approved content through role-based workflows. The system shall be implemented using an open-source PHP-based solution. The bidder shall propose and justify the selected technology stack against the requirements of these ToR. The bidder shall justify the selected technology stack against the requirements of these ToR.

2.1.1 Description of the application/use of the IT solution

The primary objective of the FHC website is to modernize the interface between the judiciary and the public by establishing a secure, reliable, and centralized digital platform for court-related information, selected online services, public communication, and controlled content management.

To achieve this, the IT solution shall support the following strategic objectives:

- Design and implement a secure, reliable, and centralized source of court-related information.
- Enhance access to court services, procedural guidance, judgments, notices, publications, and announcements.
- Provide a responsive, user-friendly, and multilingual-ready digital platform.
- Improve transparency through the publication of judgments, legal resources, public notices, vacancies, tenders, and institutional updates.
- Provide selected public-facing digital services, including case/appointment information, fee calculation, downloadable forms, feedback submission, and vacancy/tender information.
- Support internal and external stakeholders with role-appropriate access to information and services.
- Enable efficient and controlled content management by authorized court administrators through approval workflows, version control, and audit trails.
- Strengthen public engagement through moderated feedback and controlled public interaction.
- Ensure high standards of data security, system performance, accessibility, and compliance with applicable government and judicial IT policies.
- Support smooth deployment, quality assurance, user acceptance testing, documentation, knowledge transfer, and post-deployment support.
- Promote long-term sustainability through scalable architecture, open-source technology, structured content governance, and handover to the FHC IT team.

2.1.2 General conditions at the partner end (where relevant)

The FHC of Ethiopia recognizes the growing need for a centralized and authoritative digital platform that provides reliable access to court information and services. As the volume of judicial information and public interaction with the court continues to increase, reliance on manual processes and informal communication channels has created challenges in accessibility, transparency, and efficiency.

Establishing an official website will address these challenges by serving as the primary source of accurate and up-to-date information for the general public, judges, court staff, legal practitioners, and litigants.

The proposed website will function as a comprehensive digital gateway to the FHC, reflecting the institution’s mandate, improving public engagement, and supporting the broader objectives of access to justice and judicial transparency.

Against this background, the website shall be a fully responsive, secure, and scalable web-based system accessible on all modern browsers. It shall cater to public users and administrators. The platform shall enable content publishing, user interaction, administrative management, and integration with third-party services.

The administrators of the website and content management system will be for technical, and security matters the ICT Directorate and for content matters the Communication and Strategic Partnership Directorate of the Federal High Court.

2.1.3 Use of open-source software (OSS)

The solution shall be implemented using open-source software and PHP-based technologies. Suitable technologies may include Drupal, Laravel, Symfony or equivalent open-source PHP frameworks/CMS platforms, provided that the proposed stack can meet the functional, security, maintainability, accessibility and long-term sustainability requirements specified in Sections 2.3 and 2.4, including the technical framework and sustainability requirements in Sections 2.4.2 and 2.4.3 of this ToR.

The contractor shall propose and justify the selected technology stack in the implementation concept. The justification shall include suitability for structured content management, role-based access control, workflow management, auditability, multilingual readiness, security maintenance, availability of local/regional skills, long-term maintainability, and compatibility with the hosting environment.

For a content-heavy institutional website with structured workflows, role-based content governance, versioning and multilingual readiness, an established open-source CMS should be considered particularly suitable, where the contractor demonstrates clear advantages for custom workflows, case-tracker integration, vacancy management, or administrative modules.

The contractor shall comply with all applicable open-source licence conditions and shall document all third-party components, licences, versions, dependencies and update obligations. The use of proprietary components, paid plugins or cloud-only services shall require prior written approval by GIZ/FHC and must not create avoidable vendor lock-in.

2.2 Infrastructure Requirements

The IT solution shall be implemented on a secure, reliable, and scalable infrastructure that supports public access, administrative operations, content management, integration readiness, backup, monitoring, and long-term maintainability. The infrastructure shall be designed to ensure stable operation under varying network conditions and shall comply with applicable Ethiopian government ICT standards and institutional security requirements.

The infrastructure requirements shall cover at least the following areas:

2.2.1 Deployment Environments

The contractor shall configure and maintain separate staging and production environments for development, testing, user acceptance, deployment and operational handover. The staging environment shall be used for validation of new releases, security checks, content workflow testing and user acceptance testing before production deployment.

The contractor shall establish CI/CD pipelines or an equivalent controlled and traceable deployment mechanism appropriate to the designated hosting environment. deployment automation for reliable and traceable updates. Access to environments, repositories, credentials and deployment pipelines shall be role-based and auditable.

2.2.2 Hosting

Procurement and payment of the hosting service are not part of this contract. FHC/GIZ will provide or separately procure the required hosting environment. The contractor shall provide the minimum infrastructure and configuration specifications required for staging and production and shall support configuration, deployment, testing and handover within the designated environment.

The hosting environment shall comply with the requirements specified in these ToR and with applicable publicly available Ethiopian laws, regulations and government ICT requirements. Any additional FHC or government standards that are binding for implementation shall be made available to the contractor. If an appropriate government-approved or e-government data centre / hosting environment is designated by FHC or the competent government authority, the contractor shall support deployment and configuration within that environment. If such hosting is not available or not designated during the assignment, a suitable hosting service shall be selected separately from this tender, and the contractor shall provide the technical hosting requirements needed for such selection.

The contractor shall not assume ownership of hosting. However, the contractor shall provide all technical specifications required for hosting, including operating system/runtime requirements, database requirements, storage, backup, bandwidth, SSL/TLS, monitoring, logging, security hardening, availability, disaster recovery and access management requirements.

Hosting and performance considerations include secure and reliable hosting aligned with government ICT standards; performance optimisation for varying network conditions; content caching and asset optimisation; high availability where supported by the hosting model; regular backups; restoration procedures; and monitoring mechanisms to support business continuity.

2.2.3 Technical Security Requirements

Security is a core requirement of the FHC website and shall be addressed through multiple layers of technical and procedural controls. The contractor shall apply security-by-design principles throughout development, deployment, testing, and handover.

Security measures shall include:

- Role-based access control to restrict system administration, content management, publishing, vacancy management, feedback handling, and configuration functions.
- Secure authentication mechanisms for administrators, content publishers, reviewers, and other authorized staff users.
- Strong password rules, secure password reset, account lockout after repeated failed login attempts, and secure session management.
- Protection against common web security threats, including unauthorized access, privilege escalation, SQL injection, cross-site scripting, cross-site request forgery, malicious file uploads, spam submissions, and data manipulation.
- Secure handling of uploaded files, including file-type restrictions, file-size limits, malware-risk controls, and restricted access to sensitive applicant or internal documents.
- HTTPS/TLS encryption for all public and administrative access.
- System monitoring and logging to detect, investigate, and respond to security events.

- Audit trails to track user login, role changes, content updates, approvals, publishing actions, vacancy/application handling, feedback handling, and administrative configuration changes.
- Protection of audit logs against unauthorized modification or deletion.
- Secure backup, restoration, and disaster-recovery procedures.
- Security testing and vulnerability remediation before production deployment.

Security configurations shall be reviewed and validated prior to production deployment. The system shall only be approved for go-live once critical and high-risk security findings have been resolved or formally accepted by FHC and GIZ.

2.3 Functional requirements

The IT solution must meet the following functional requirements. The detailed requirements in the SRS and Figma prototype remain binding references and shall be validated during the implementation concept phase.

1. **Authentication and Access Control:** The system shall provide secure authentication for administrators and authorised staff users, including secure login/logout, password policies, password reset, session handling, account status management and account lockout after repeated failed login attempts. Public users shall not be required to authenticate for access to public content or for submitting permitted feedback/comments.
2. **Authorization and Roles:** The system shall implement role-based access control (RBAC) with granular permissions for content authors, reviewers, publishers, administrators, system auditors and other roles agreed during validation. Role assignments, permission changes and sensitive actions shall be logged.
3. **User Profile Management:** Authorised staff users shall be able to view and update their profile information, manage passwords, and maintain account status in accordance with assigned permissions.
4. **Search, Filter, Sort and Navigation:** The system shall provide public and administrative search, filtering, sorting, metadata tagging, indexed retrieval, breadcrumbs and consistent navigation. Search results must respect role-based access restrictions and must not expose non-public or restricted content.
5. **Notifications and Communication:** The system shall support internal notifications for review/approval workflows, website notifications, and email notifications where users have subscribed or where operationally required. Notification templates, scheduling, delivery status and notification logs shall be manageable by authorised administrators.
6. **Administration Dashboard:** The system shall provide a secure administrative dashboard for user management, role management, content workflow monitoring, system settings, pending approvals, audit logs, notifications, vacancy management, tender management and relevant reports/statistics.
7. **Site Architecture and Public Content Sections:** The website shall provide the public-facing sections described in the SRS, including Home Page, About the Court, Court Services and Information, News/Events/Notices/Announcements, Resources and Gallery, Contact/Support/Feedback, FAQs, Vacancy, Tender, Terms and Conditions, Privacy Policy and controlled Social Media elements.
8. **Case Tracker and Court Appointments:** The website shall provide access to case-status / court-appointment information as defined in the SRS and confirmed during implementation concept validation. The implementation approach shall depend on the

availability, quality and accessibility of existing FHC systems and data sources. Where API integration or periodic data synchronisation is required, the contractor shall document dependencies, data fields, security controls, update frequency, fallback process and responsibilities of FHC/third-party system owners. Real-time case synchronisation shall only be implemented if explicitly included in the agreed scope and technically enabled by the source systems.

9. **Court Fee / Charge Calculator:** The website shall include a configurable court fee / charge calculator based on rules, formulas and fee data supplied and approved by FHC. The calculator shall clearly indicate that results are indicative unless FHC confirms them as legally binding.
10. **Vacancy Module:** The system shall allow authorised administrators to publish, update, close and archive vacancies. Public users shall be able to view vacancies and, where included in the agreed scope, submit applications and upload supporting documents. The system shall support applicant review, filtering, status management, shortlisting and applicant notifications in accordance with privacy and security requirements.
11. **Tender Module and eGP Redirection:** The system shall allow authorised administrators to publish tender announcements and related information. Tender submissions shall not be handled by the FHC website unless separately commissioned. Users shall be redirected to the official Ethiopian Government Procurement (eGP) portal for detailed tender submission processes.
12. **Feedback and Moderated Public Interaction:** The system shall allow users to submit feedback, inquiries or comments through controlled forms. Public display of comments, if any, shall be subject to moderation and approval by authorised FHC staff. The system shall support routing, categorisation, review, response tracking and audit logging for submitted feedback/comments.

For more information on the sub-pages, the bidder may refer to the Annex 1 – Federal High Court Website Proposal Version I of the terms of reference.

The contractual baseline scope comprises the functional requirements listed in items 1–12 of this Section and the related requirements specified in Annex 1, subject only to the explicit scope boundaries and external dependencies identified in Section 2.5. The implementation concept may refine implementation details, sequencing and technical approaches, but shall not reduce the contractual scope defined in these ToR.

For avoidance of doubt, Section 2.3 defines the contractual functional scope. Annex 1 provides detailed descriptions, process information and test/reference material relating to these requirements and does not independently expand the scope unless expressly referenced in these ToR.

2.4 Non-functional requirements

The IT solution must meet the following non-functional requirements:

1. **Usability and UI/UX:** The solution shall follow the approved Figma prototype and provide intuitive, consistent and user-friendly interfaces for public users, content contributors, reviewers, publishers, administrators and staff users.

2. **Responsiveness and Cross-Browser Compatibility:** The website shall be fully responsive for desktop, tablet and mobile devices and compatible with modern browsers including at least Chrome, Firefox and Edge.
3. **Accessibility:** The website shall be designed and tested against recognised accessibility principles, preferably WCAG 2.1 AA or an equivalent standard agreed with FHC/GIZ. Accessibility shall cover navigation, forms, contrast, keyboard access, screen-reader compatibility, document listings, alternative text and error messages.
4. **Database and Information Architecture:** The system shall use efficient, maintainable and scalable data models for users, roles, permissions, content, judgments/publications, comments/feedback, vacancies, applications, tenders, notifications, subscriptions, audit logs and configuration records.
5. **Security:** The solution shall implement HTTPS/TLS, secure authentication, secure session handling, password policies, RBAC, input validation, secure file uploads, audit logging, least-privilege access, secure backups and protection against common web application threats.
6. **Performance and Availability:** The system shall be optimised for page-load speed, caching, image/document optimisation, efficient database queries and reliable access under expected load and varying network conditions.
7. **Backup, Recovery and Maintainability:** The system shall provide documented backup and restore procedures, maintenance instructions, dependency documentation and operational runbooks. Backup and restoration must be tested before final acceptance.
8. **Multilingual Support:** The CMS system shall support Amharic and English content structures, labels and publishing workflows. The solution shall be technically designed so that further languages can be added in future without fundamental redevelopment.
9. **Interoperability and Integration Readiness:** The architecture shall allow future integration with internal court systems, case management systems, registry platforms, notification services, analytics, document storage and eGP redirection, while protecting non-public information and respecting access-control requirements.
10. **Sustainability:** The system shall minimise vendor lock-in, use maintainable open-source technologies where possible, document dependencies and licences, and enable FHC IT and content staff to operate and maintain the system after handover.

2.4.1 Interfaces

The FHC website shall support controlled and auditable interaction with external channels and services. The system shall not automatically publish content to external platforms unless this is explicitly approved by FHC/GIZ and the required platform credentials, API access and governance arrangements are available.

Social media requirements shall be limited to controlled sharing, linking and embedding. The system may display links to verified official social media accounts and may embed approved public social media feeds in selected website areas with prior administrative approval. Where content is marked for social media dissemination, the system shall support authorised staff by providing controlled sharing links or prepared content snippets; however, direct API-based publishing shall not be assumed as part of the baseline scope.

All social media-related configuration and sharing/embedding actions performed within the system shall be restricted to authorised administrators and logged for audit and accountability.

The tender module shall redirect users to the official Ethiopian Government Procurement (eGP) portal for tender submission. The FHC website shall not receive tender submissions unless a separate integration is explicitly commissioned.

Any integration with case-tracking systems, appointment systems, email gateways, analytics tools or document repositories shall be confirmed during the implementation concept phase and shall depend on the availability of source systems, interface documentation, credentials, security approvals and data-sharing arrangements.

2.4.2 System requirements/technical framework

The FHC website shall be designed and implemented using a secure, scalable, standards-compliant and maintainable technical approach. The technology approach shall be an open-source and PHP-based solution in accordance with Section 2.1.3.

The tenderer shall propose and justify the technology stack in its technical offer. Following award, the contractor shall confirm and refine the selected approach as part of the implementation concept. The recommendation must explain why the selected stack is suitable for: structured content management, approval workflows, RBAC, audit logging, secure file uploads, search, vacancy management, fee calculator, case-tracker access, multilingual readiness, documentation, deployment, maintenance and long-term local capacity.

The architecture shall be modular and layered, separating presentation, application logic, data persistence, content management, administrative functions, integration services and deployment/operations concerns. Public-facing functions shall be clearly separated from restricted administrative functions.

The solution shall include reusable templates/components, documented APIs or integration points where relevant, configurable content types, maintainable database structures, secure file storage, and clear configuration mechanisms. The architecture shall support future integration with internal court systems, including case management or registry platforms, without exposing restricted data to public users.

The contractor shall deliver source code, configuration files, deployment scripts or instructions, database migration scripts, dependency lists, licence information and technical documentation sufficient for future maintenance by FHC or another authorised service provider.

The website shall be designed to protect user data, administrative data, applicant data, feedback/comment data, notification subscription data and any case-status or appointment information made available through the system.

2.4.3 Sustainability

The contractor shall promote the long-term sustainability of the system through maintainable open-source technologies, scalable architecture, structured content governance,

comprehensive technical, operational, user and handover documentation as specified in Sections 3.5 and 3.10 , and effective knowledge transfer to the FHC IT and content teams.

The solution shall be designed to reduce dependency on a single vendor by ensuring handover of source code, configuration, deployment instructions, dependency lists, licence information, user manuals, administrator manuals, and operational procedures. The contractor shall avoid unnecessary proprietary components, paid plugins, or cloud-only services unless technically justified and subject to prior written approval by GIZ, following consultation with FHC where relevant.

The system shall support future maintenance, security updates, content expansion, and possible integration with relevant court or government systems without requiring a complete redevelopment.

2.5 Further specifications/general conditions

The following scope boundaries apply to this contract. Any subsequent modification of the contractual scope shall be handled through the applicable contractual change procedure and requires written approval by GIZ.

1. The FHC website shall not replace existing official case-management, registry, HRM or procurement systems. Replacement or redevelopment of these systems is outside the scope of this contract..

2. Case Tracker and appointment information shall depend on the availability and approval of source data from existing FHC systems. If no integration-ready system is available, the contractor shall propose a controlled interim approach, such as manual upload, periodic import or administrative data entry, for written approval by FHC/GIZ. The contractor shall propose a controlled interim approach, such as manual upload, periodic import or administrative data entry. The approach shall be documented in the implementation concept, technically validated by FHC and approved in writing by GIZ.

3. Tender submissions shall be handled through the official eGP portal; the website shall publish tender announcements and redirect users accordingly.

4. The fee/charge calculator shall be based on FHC-approved calculation rules and data. The contractor shall not be responsible for defining legal fee rules.

5. Full multilingual CMS workflow, real-time case synchronisation, SMS notifications, advanced security analytics, CDN/auto-scaling and advanced vacancy analytics shall be reviewed during the implementation concept phase and prioritised jointly with FHC and GIZ. Their implementation shall depend on agreed scope, available technical dependencies, hosting readiness, third-party service access, data availability, security approvals, and the approved implementation schedule.

6. FHC shall provide timely access to required content, logos/branding materials, fee-calculation rules, forms, judgments/publications approved for publication, branch/bench information, and nominated focal persons for validation, UAT, training and handover.

For more information about the target users and related actions, the bidder may refer to pages 9 and 10 of the Annex documents “Federal High Court Website – Project Proposal”.

3. Responsibilities of the contractor

The contractor will deliver the following services and work packages (along with the corresponding milestones). The work packages may be implemented in an integrated and iterative manner, depending on the agreed development methodology. However, logical dependencies between validation, development, testing, deployment, handover and support shall be respected:

3.1 Work package 1: Kick-off

At the start of the project, the contractor, FHC and GIZ shall clarify the cooperation arrangements, communication channels, responsibilities, decision-making process, project schedule, technical collaboration environment, and acceptance procedure.

The kick-off shall also confirm the use of the SRS and Figma prototype as core references, identify immediate assumptions and dependencies, and agree on the structure for the implementation concept phase.

Services to be rendered by the contractor:

- Preparation and facilitation of the kick-off meeting;
- Documentation of agreements, decisions, open issues, assumptions and dependencies;
- Establishment of an online collaboration/work environment;
- Confirmation of communication, reporting and escalation arrangements;
- Initial project schedule and next-step plan.

Outcome to be delivered by the contractor:

- Kick-off minutes;
- Initial project plan;
- Initial risk, issue, assumption and dependency log.

3.2 Work package 2: Drafting the implementation concept

This work package shall focus on validation and refinement of the existing SRS, Figma prototype, annexes and tender requirements. The contractor shall not repeat a full scoping or design phase but shall confirm assumptions, identify gaps, document dependencies, and convert the existing requirements into an implementable delivery plan.

The implementation concept shall determine the delivery sequence, technical implementation approach and dependency management without reducing this contractual scope, including public website sections, CMS/content governance, admin portal, RBAC, audit logs, search/filter/sort/navigation, publication workflows, notifications, moderated feedback/comments, resources and document publication, vacancy module, tender announcements with eGP redirection, fee/charge calculator, and Case Tracker/court appointment access according to the integration approach approved in the implementation concept.

The implementation concept shall include:

- Confirmed mapping of the functional and non-functional requirements defined in Sections 2.3–2.5 to the implementation backlog, delivery sequence, dependencies and acceptance criteria.
- Implementation phasing and prioritisation within the contractual scope defined in these ToR; The implementation concept shall not add, remove or materially alter the contractual scope defined in these ToR.
- Confirmation and justification of the technology stack in accordance with Section 2.1.3.
- Final/provisional system architecture and deployment model.
- Content model, role-permission matrix, content workflows and moderation workflows.
- Approach for case tracker, court appointments and fee calculator, including dependencies and source-data assumptions.
- Approach for vacancy, tender/eGP redirection, notifications, feedback and moderated comments.
- Release plan, iteration plan and acceptance criteria.
- Diagrams and outlines such as use cases, ERD, process outlines, integration diagrams and user journeys.
- Updated risk and dependency register.

Outcome to be delivered by the contractor:
Validated implementation concept, including release plan, architecture, backlog/user stories, acceptance criteria, dependency register and updated implementation schedule.

3.3 Work package 3: Technical implementation

The IT solution shall be developed on the basis of the validated implementation concept, SRS and Figma prototype. The contractor shall implement the functionality defined in Sections 2.3–2.5 using the technology approach confirmed through the implementation concept using the approved open-source PHP-based technology stack and shall follow the agreed release/iteration plan.

The implementation shall cover the contractual functionality defined in Sections 2.3–2.5.

Where the Case Tracker requires integration with existing court systems or branch-level data, the contractor shall implement only the agreed integration or import approach for which FHC can provide access, interface documentation, sample data, credentials and security approvals. Real-time synchronisation shall not be assumed unless explicitly included.

Outcomes to be delivered by the contractor:

- Operable and executable application;
- Source code and configuration files;
- Annotated source code where necessary;
- Database schema and migration scripts;
- Implementation progress documentation and change log;
- Deployment instructions/scripts;
- Updated backlog and release notes.

3.4 Work package 4: Testing and quality assurance

The contractor shall set up and maintain a test/staging environment and conduct testing during and after development. The testing approach shall be aligned with the SRS test cases and shall cover public-facing, administrative, workflow, integration, security, accessibility and operational requirements.

Outcomes to be delivered by the contractor:

- Testing concept and test plan;
- Test cases and acceptance checklist mapped to the SRS requirements;
- Functional testing of all public website features and CMS/admin workflows;
- Testing of case tracker/court appointment access and fee/charge calculator;
- Testing of vacancy module, including application submission, document upload, applicant filtering, status management and notifications where included;
- Testing of tender module and eGP redirection;
- Testing of feedback/comment moderation and routing;
- Security testing, including authentication, RBAC, secure file upload, session handling, input validation and audit logs;
- Performance testing under expected load and common network constraints;
- Accessibility and usability testing;
- Cross-browser and cross-device compatibility testing;
- Backup and restoration testing;
- UAT support with designated FHC representatives;
- Defect log, remediation evidence, test report and final QA recommendation.

Only systems that meet the agreed functional, quality, accessibility and security criteria shall be recommended for production deployment.

3.5 Work package 5: Documentation

The contractor shall provide comprehensive technical, operational, user and handover documentation. The documentation shall be sufficient to support system operation, administration, maintenance, future updates, troubleshooting and transfer to FHC IT or another authorised service provider:

- Selected open source/PHP technology stack, third-party components, licences and dependencies;
- CMS content types, content workflows, roles and permissions;
- Case Tracker / appointment data model, integration/import approach and dependencies;
- Fee/charge calculator rules/configuration approach;
- Vacancy module data handling, upload handling and applicant-status workflow;
- Tender/eGP redirection configuration;
- Backup, restoration, monitoring and incident-response procedures;
- Release/deployment procedures and environment configuration;
- Handover checklist and post-deployment support procedures.

3.6 Work package 6: Training

The contractor shall design and deliver practical, hands-on training to ensure that FHC staff are able to operate, administer, and maintain the website independently after handover. The training shall cover the Content Management System (CMS), administrative portal, content workflows, role and permission management, notifications, moderated feedback/comments, vacancy and tender modules, resources/judgment publication, fee calculator configuration where applicable, and basic operational troubleshooting.

The training shall be delivered in English and Amharic or with adequate Amharic language support. The Content, Localization and Stakeholder Support Specialist shall support the preparation and delivery of Amharic/English examples, labels, training exercises, and content-management guidance.

The objective is to build internal capacity within FHC, reduce dependency on the contractor after go-live, and ensure that website operations follow the agreed content governance, security, and administrative procedures.

3.6.1 Administrative training

The contractor shall conduct 2 days of administrative and technical training for FHC Ethiopia IT personnel and designated system administrators. This training shall focus on the technical and administrative operation of the website and shall include, at minimum:

- Managing users, roles, and permissions
- Operating the administrative dashboard and CMS configuration areas
- Managing content approval workflows, audit logs, and publishing controls
- Monitoring notifications, feedback/comments, tenders, vacancies, and public submissions
- Managing backups, basic troubleshooting, and routine maintenance procedures
- Understanding security procedures, access control, and escalation arrangements
- Reviewing deployment, hosting, and support documentation relevant to FHC IT staff

The training content shall be documented in writing and shall include practical exercises using realistic FHC-related examples.

3.6.2 User training

The contractor shall conduct 3 days of user training for FHC staff who will use the website and CMS for content creation, review, approval, publication, and day-to-day operational tasks. This training shall cover, at minimum:

- Creating, editing, reviewing, approving, publishing, unpublishing, and archiving content
- Managing pages, news, notices, announcements, FAQs, resources, judgments/publications, gallery items, vacancies, and tenders
- Handling moderated feedback/comments and contact inquiries
- Applying correct metadata, categories, tags, document naming, and accessibility practices
- Using notification templates and publication scheduling where applicable
- Following content governance, quality assurance, and approval procedures

The following materials shall be produced and handed over:

- Training materials
- User manual
- Administration manual
- Quick-reference sheets
- Practical exercises
- Guidelines for updating manuals and training materials after handover

3.7 Work package 7: Support (and operation)

The contractor shall provide support and operational assistance from production deployment until the end of the 8-month contractual term. Support shall include bug fixing, corrective maintenance, security updates for the agreed software stack, support for content/workflow issues, deployment support for agreed updates, monitoring of reported incidents, backup/restore support where required, and communication with the hosting provider or FHC IT team in case of critical incidents.

Support shall not include major new functionality, real-time integration work, large content migration, or substantial design changes unless separately commissioned.

Outcomes to be delivered by the contractor:

- Support and incident log;
- Report on support enquiries addressed;
- Report on operational and maintenance activities;
- Security/update log;
- Final support and handover closure report.

3.8 Work package 8: Project management

The contractor shall appoint an experienced project manager as the permanent contact person for the entire contract term. The project manager shall be responsible for planning, coordination, delivery monitoring, risk management, communication, and reporting on behalf of the contractor.

Project management shall include:

- Compiling and validating FHC's technical, functional, operational, and content-related requirements based on the ToR, SRS, Figma prototype, and agreed implementation concept.
- Preparing and maintaining a shared project plan, resource plan, release plan, and iteration plan.
- Coordinating all project activities with FHC, GIZ, the contractor's technical team, and relevant hosting/service providers.
- Managing dependencies, assumptions, decisions, change requests, risks, issues, and acceptance criteria.
- Ensuring that the project plan reflects the agreed prioritisation, especially where requirements are linked to Scenario A, Scenario B, or optional enhancements.
- Organising regular progress meetings and documenting decisions, action points, risks, and open issues.

- Ensuring timely delivery of all work packages, documentation, training, testing, deployment, and support obligations.

Outcomes to be delivered by the contractor:

- Project plan and resource plan
- Release/iteration plan
- Risk, issue, decision, and action-point log
- Regular progress reports
- Updated delivery schedule where changes are agreed

3.9 Work package 9: Monitoring and reporting

The contractor shall actively support results-based monitoring and reporting throughout the contract term. Monitoring shall cover progress against activities, milestones, deliverables, quality requirements, risks, and agreed acceptance criteria.

Regular monitoring activities shall cover at least the following areas:

- Degree to which planned activities and work packages have been implemented.
- Degree to which objectives, indicators, milestones, and deliverables listed in the ToR have been achieved.
- Progress against the agreed implementation concept, release plan, and prioritised requirements.
- Status of development, testing, security review, documentation, training, deployment, and post-deployment support.
- Risks, issues, dependencies, change requests, and mitigation measures.
- Results achieved within the contractor's sphere of responsibility.
- Results or delays caused by external dependencies, including hosting, access to systems, content availability, stakeholder feedback, or third-party services.

The contractor shall submit a concise monthly progress report to FHC and GIZ throughout the contract term, as well as the final completion/support report to FHC and GIZ.

Outcomes to be delivered by the contractor:

- Regular monitoring/progress reports
- Risk and issue updates
- Milestone and deliverable status updates
- Final completion/support report

3.10 Work package 10: Deployment and Handover

The contractor shall transition the website from development to operational status in a controlled, secure, and fully documented manner. The objective is to ensure that the website is technically stable, secure, tested, accepted, and ready for operation by FHC staff.

Deployment and handover activities shall include:

- Installing and configuring the website on the approved production hosting environment.

- Configuring databases, CMS, administrative portal, user roles, permissions, workflows, notifications, backup procedures, and monitoring arrangements.
- Migrating or uploading agreed initial content, documents, images, judgments/publications, vacancies, tenders, FAQs, and other approved materials where applicable.
- Verifying that all agreed features, integrations, content workflows, access controls, and public-facing pages function as intended.
- Conducting final pre-go-live checks, including functional, security, accessibility, usability, performance, cross-browser, and device testing.
- Resolving critical and high-priority defects before production approval.
- Supporting UAT and obtaining documented acceptance from FHC/GIZ before go-live.
- Handing over source code, deployment instructions, system credentials, technical documentation, user manuals, administrator manuals, training materials, backup/restore procedures, and support contacts.
- Providing post-deployment support until the end of the contract term.

Outcomes to be delivered by the contractor:

- Deployed production website
- Deployment and handover report
- Final test and UAT documentation
- Source code and technical documentation
- System credentials and access handover record
- Backup, recovery, maintenance, and support procedures
- Final acceptance documentation

4. Term, schedule and milestones

The expected term of the contract is 8 months. The implementation shall be organised in iterative releases. The following indicative milestone structure shall apply and shall be refined during the implementation concept phase.

Milestones	Delivery date/period	Responsible
Kick-off, validation and implementation concept: Kick-off meeting, review of ToR, SRS and Figma prototype, validation of scope, assumptions, dependencies, methodology, communication structure and acceptance process	Month 1 after contract start	Contractor with FHC/GIZ
Technology stack, architecture, backlog and release plan approved: Confirmation of open-source PHP-based technology approach, system architecture, prioritised backlog, release plan, hosting assumptions and implementation schedule	End of Month 1	Contractor with FHC/GIZ
Core website, CMS, admin portal, RBAC and content workflow implemented in staging: Public website structure, CMS, administrative portal, user/role management, approval workflows, audit logs and basic content templates available in staging	Months 2–3	Contractor

Functional modules implemented in staging: Search/navigation, notifications, resources/judgments, vacancy module, tender publication with eGP redirection, moderated feedback/comments, fee calculator and agreed Case Tracker approach implemented in staging	Months 3–4	Contractor with FHC input on content/data
Hosting/deployment preparation, security hardening and integration validation: Production hosting preparation, performance configuration, backup/restore setup, monitoring/logging, security hardening and validation of agreed integrations	Months 4–5	Contractor with FHC IT / hosting provider
Testing, QA, security review, accessibility review and UAT: Functional, security, performance, accessibility, cross-browser, device compatibility and user acceptance testing completed; critical defects resolved before go-live	Months 5–6	Contractor with FHC representatives
Production deployment, documentation, training and formal handover: Production deployment, final content validation, handover of source code, credentials, manuals, deployment documentation, administrative and user training, and formal acceptance	Month 6	Contractor with FHC IT/GIZ
Post-deployment support, stabilisation and final closure: Warranty support, bug fixing, updates, security patches, operational support, support reporting and final closure report until contract end	Months 6–8	Contractor with FHC IT

If dependencies outside the contractor's control delay specific features, especially Case Tracker data integration, email gateway access, hosting readiness, official content provision, or third-party service availability, the contractor shall document the delay, propose mitigation measures, and agree revised prioritisation with FHC and GIZ.

5. Granting rights of use

The contractor grants the rights of use for the IT solution, as per Section 3 of the General Terms and Conditions for EVB-IT Service Contracts (EVB-IT-Service-AGB) to both GIZ and the Federal High Court of Ethiopia as per Section 3 of the General Terms and Conditions for EVB-IT Service Contracts (EVB-IT-Service-AGB).

Insofar, as the contractor provides the results of the services as Open Source Software, section 3.2 of the EVB-IT Service Contract applies.

Insofar, as the contractor uses OSS, the Contractor shall provide GIZ and BPRA with a documentation of OSS components (Annex 4) for each version, release or other materially updated status of the software.

Section 3.5 of the General Terms and Conditions for EVB-IT Service Contracts (EVB-IT-Service-AGB) applies to all pre-existing works (incl. third party works) protected by copyright.

6. Data protection

The performance of the Contract may involve the processing of personal data by the Contractor, such as (but not limited to) the processing of names and contact information. In such cases, the Contractor acts as an independent data controller and must comply with all applicable data protection obligations, including those arising from regional and local laws. The Contractor may only process personal data if the objective to be achieved cannot be achieved without this data. 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 must be observed. GIZ is in no way responsible for such processing.

In cases where the contractor follows the instructions of a GIZ partner, the partner is the data controller. The laws and standards applicable to it and the contractor must be complied with and implemented.

If the Contractor is not subject to the GDPR and the applicable laws do not contain any explanations of the data protection principles and rights mentioned here, the definitions of the GDPR (Regulation (EU) 2016/679) should be used.

Key data protection measures shall include:

- Compliance with applicable Ethiopian data protection, GDPR, judicial confidentiality and privacy requirements;
- Secure handling of user-submitted data from inquiry, feedback, vacancy application and subscription forms;
- Secure file-upload controls for CVs, certificates, documents and media;
- Clear separation of public content, restricted administrative content and any case-related information;
- Role-based access to applicant data, feedback records, internal notifications and audit logs;
- Defined data retention, archival and disposal rules;
- Auditability of administrative access and changes;
- Privacy notices and consent wording for forms that collect personal data.

The data protection and information security provisions set out in the most recent Special Terms and Conditions of Contract of GIZ (sections 1.5. Confidentiality and 2 Data Protection) apply.

7. Information security

The contractor shall ensure that all services are delivered in accordance with applicable information security requirements of GIZ, FHC, and relevant Ethiopian government ICT/security standards. Information security shall be considered throughout the full project lifecycle, including design, development, testing, deployment, operation, handover, and support.

The contractor shall implement appropriate technical and organisational measures to protect the confidentiality, integrity, and availability of the website, its administrative functions, user

data, uploaded documents, audit logs, source code, credentials, and operational documentation.

At minimum, the contractor shall ensure:

- Secure development practices and protection against common web application vulnerabilities.
- Role-based access control and secure authentication for all administrative users.
- Secure handling, storage, and transfer of data, documents, backups, credentials, and configuration files.
- HTTPS/TLS encryption for public and administrative access.
- Logging and audit trails for administrative activities, content changes, user management, and security-relevant events.
- Secure backup and restoration procedures.
- Vulnerability testing and remediation before production deployment.
- Immediate reporting of security incidents, vulnerabilities, or suspected data breaches to FHC and GIZ.
- Secure handover of credentials, source code, documentation, deployment procedures, and operational responsibilities to the FHC IT team.

The contractor shall ensure that only authorised personnel have access to project systems, hosting environments, repositories, data, and documentation. Any subcontractors or team members involved in the assignment shall be bound by appropriate confidentiality and information security obligations.

8. Language

In deviation from Sections 1.2, 6.1 and 8.1 of the General Terms and Conditions for EVB-IT Service Contracts, the contractor shall provide the services in English and/or Amharic as required for the relevant target group.

The main working and reporting language for communication with GIZ shall be English. Project management documents, progress reports, technical documentation, implementation concepts, testing documentation, handover documentation, and formal deliverables shall be prepared in English, unless otherwise agreed with GIZ and FHC.

Training, user guidance, content-management support, and operational explanations for FHC users shall be provided in English/Amharic, or with adequate Amharic language support. User-facing labels, training examples, content-management exercises, and relevant guidance materials shall be prepared in Amharic and/or English depending on the target user group and agreed operational needs.

The contractor shall ensure that communication with FHC staff can be effectively conducted in Amharic and English, especially during requirements validation, training, user acceptance testing, content handover, and operational support.

9. Technical and methodological concept

In the conceptual design of the tender (technical and 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.

9.1 Requirements for the technical and methodological concept (Section 1 of the assessment grid)

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

9.1.1 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 taken into account in the IT solution to be developed by the tenderer in order to achieve the objective (Section 1.1 of the assessment grid). The assessment shall also consider the suitability and justification of the proposed technology approach against the requirements in Section 2.

9.1.2 Project management and development methodology

The tenderer should consider the design of the project management process and describe their methodology for development/implementation, taking into account the described work packages (Section 3) and compliance with the milestones (Section 4) (Section 1.2 of the assessment grid).

9.1.3 Operational plan/personnel assignment plan

The tenderer must create and explain an operational plan that also includes a personnel assignment plan for all of the specialist staff that they offer. The operational plan must depict the assignment periods (time period and expert days) and, in particular, describe the necessary work steps and take account of and, where necessary, supplement the milestones as per Section 4 (Section 1.3 of the assessment grid).

9.1.4 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).

10. Human resources

The tenderer is required to propose personnel on the basis of relevant CVs for the positions (as experts) specified and described here in terms of the areas of responsibility and qualifications. **The requirements regarding the format and content of the CVs are set out in Section 12.**

The qualifications set out below reflect the requirements for achieving the maximum number of points in the technical assessment.

‘One year of professional experience’ is understood to mean 12 cumulative expert months with at least 18 expert days per month, provided no diverging definition is specified for individual qualifications.

10.1 Key Expert 1: Team Leader / IT Project Manager (Section 3.1 of the assessment grid)

This position is a key expert.

Responsibilities of Expert 1: (Team Leader / IT Project Manager)

- Act as the contractor's permanent contact person for FHC and GIZ throughout the full contract term.
- Lead kick-off, planning, stakeholder coordination, work-package integration, risk management, and decision tracking.
- Translate FHC's technical and operational requirements into a realistic project plan, release plan, resource plan, and iteration plan.
- Oversee implementation concept development, progress reporting, monitoring, quality gates, acceptance preparation, deployment, and handover.
- Coordinate the multidisciplinary team and ensure alignment between functional requirements, security requirements, hosting constraints, documentation, training, and support obligations.
- Ensure timely submission of deliverables including project plans, progress reports, monitoring reports, support reports, and final handover documents.

Qualifications of Expert 1: (Team Leader / IT Project Manager)

Education/training (Section 3.1.1 of the assessment grid)	University degree (master's degree or German Diplom equivalent), in computer science, information systems, software engineering, project management, public administration with ICT specialization
Language (Section 3.1.2 of the assessment grid)	Knowledge of English at C1 level in the Common European Framework of Reference for Languages.
General professional experience (Section 3.1.3 of the assessment grid)	7 years of professional experience in IT project management, software delivery, digital transformation, web-platform implementation, or public-sector ICT projects.
Specific professional experience (Section 3.1.4 of the assessment grid)	6 years of experience managing web application, CMS, e-government, GovTech, justice-sector, or comparable institutional digital platform projects, including requirements prioritisation, delivery planning, QA coordination, and client acceptance management.
Leadership/management experience (Section 3.1.5 of the assessment grid)	5 years of management experience in projects or organisations with responsibility for multidisciplinary teams of 5 persons *including* experience managing delivery budgets and technical experts and stakeholder governance
Experience in the field of development cooperation (Section 3.1.6 of the assessment grid)	3 years of experience in development cooperation, donor-funded, public-sector reform, justice-sector, or international cooperation projects.
Other (Section 3.1.7 of the assessment grid)	2 years of professional experience coordinating institutional stakeholders, management reporting, technical meetings, risk/issue tracking and milestone-based project delivery.

10.2 Expert 2: Business Analyst / Solution Architect (Section 3.2 of the assessment grid)

Responsibilities of Expert 2: Business Analyst / Solution Architect

- Lead requirements validation, prioritisation, and translation of the proposal and annex requirements into user stories, acceptance criteria, process flows, and backlog items.
- Design the provisional and final system architecture, including modular layering, CMS architecture, administrative functions, integration points, data flows, and deployment model.
- Prepare core diagrams and outlines, including use cases, user journeys, ERD, process outlines, role-permission matrix, content workflows, and integration diagrams.
- Advise on information architecture for public users, legal practitioners, judges, court staff, administrators, and guest subscribers.
- Support the development team with functional clarifications and ensure traceability between requirements, implementation, testing, and acceptance.
- Contribute to arc42-style technical documentation and handover materials.
- Validate SRS assumptions and convert them into backlog items, user stories, acceptance criteria and a release plan.
- Define the implementation approach for Case Tracker/court appointments, including data dependencies, integration/import options, fallback process and access-control risks.
- Define the fee/charge calculator rules-management approach based on FHC-approved formulas and data.
- Distinguish mandatory multilingual readiness from optional full multilingual CMS workflow.

Qualifications of Expert 2: Business Analyst / Solution Architect

Education/training (Section 3.2.1 of the assessment grid)	University degree in computer science, software engineering, information systems, business informatics, enterprise architecture, systems analysis,.
Language (Section 3.2.2 of the assessment grid)	Knowledge of English at C1 level in the Common European Framework of Reference for Languages.
General professional experience (Section 3.2.3 of the assessment grid)	7 years of professional experience in business analysis, solution architecture, systems analysis, enterprise architecture, or software requirements engineering.
Specific professional experience (Section 3.2.4 of the assessment grid)	5 years of experience in designing CMS-based or PHP/open-source web platforms with RBAC, content governance, search, workflows, data integration, and citizen-facing service modules including any experience with court, legal-information, e-government or comparable public-sector platforms.
Leadership/management experience (Section 3.2.5 of the assessment grid)	2 years of experience coordinating technical design workstreams or leading requirements and architecture workshops with multiple stakeholder groups.
Experience in the field of development cooperation (Section 3.2.6 of the assessment grid):	2 years of experience in development cooperation, donor-funded technical assistance, public-sector reform, or e-government projects
Other (Section 3.2.7 of the assessment grid)	2 years of professional experience applying , data modelling, content governance, software documentation standards,

	security-by-design, accessibility-by-design, and requirements traceability.

10.3 Expert 3: UI/UX and Accessibility Specialist (Section 3.3 of the assessment grid)

Responsibilities of Expert 3: UI/UX and Accessibility Specialist

- Design high-fidelity UI/UX concepts for public-facing pages, CMS interfaces, and the administrative portal.
- Prepare responsive mock-ups, wireframes, user journeys, navigation concepts, and reusable design components for desktop, tablet, and mobile devices.
- Develop an accessible and consistent visual design language aligned with institutional and federal government website conventions.
- Ensure accessibility considerations are embedded in page templates, forms, navigation, multimedia elements, document listings, feedback forms, and multilingual layouts.
- Support user acceptance testing by interpreting usability feedback and defining design improvements.
- Provide design specifications to developers and contribute to the user guide where interface behaviour must be explained.

Qualifications of Expert 3: UI/UX and Accessibility Specialist

Education/training (Section 3.3.1 of the assessment grid)	University degree or equivalent professional qualification in interaction design, UX design, human-computer interaction, digital media, graphic design, computer science,
Language (Section 3.3.2 of the assessment grid)	Knowledge of English at B2 level in the Common European Framework of Reference for Languages.
General professional experience (Section 3.3.3 of the assessment grid)	6 years of professional experience in UI/UX design, digital product design, web design, or human-centred design.
Specific professional experience (Section 3.3.4 of the assessment grid)	4 years of experience designing responsive, accessible, public-facing websites or digital service platforms, including CMS templates, navigation systems, search interfaces, forms, and administrative dashboards.
Leadership/management experience (Section 3.3.5 of the assessment grid)	Not Applicable
Experience in the field of development cooperation (Section 3.3.6 of the assessment grid):	Not Applicable
Other (Section 3.3.7 of the assessment grid)	2 years of professional experience applying WCAG 2.1/2.2 principles, responsive design, design systems, prototyping tools such as Figma or Adobe XD, and accessibility testing methods.

10.4 Expert 4: DevOps, Hosting and Security Engineer (Section 3.4 of the assessment grid)

Responsibilities of Expert 4: DevOps, Hosting and Security Engineer

- Configure staging and production environments, CI/CD pipelines, deployment automation, environment variables, access controls, and release procedures.
- Set up secure hosting aligned with applicable Ethiopian government ICT standards and the hosting provider's operational requirements.
- Implement HTTPS/TLS, server hardening, firewall rules where applicable, monitoring, logging, backup automation, disaster recovery procedures, and high-availability configuration within the agreed hosting model.
- Support security configurations for authentication, authorization, secrets management, audit logging, vulnerability management, and incident response procedures.
- Conduct or coordinate technical security testing, vulnerability remediation, performance checks, and pre-production deployment validation.
- Provide operational handover, runbooks, maintenance procedures, backup/restore instructions, and post-deployment technical support.

Qualifications of Expert 4: DevOps, Hosting and Security Engineer

Education/training (Section 3.4.1 of the assessment grid)	University degree in computer science, information security, network engineering, systems engineering, cloud engineering,.
Language (Section 3.4.2 of the assessment grid)	Knowledge of English at B2 level in the Common European Framework of Reference for Languages.
General professional experience (Section 3.4.3 of the assessment grid)	7 years of professional experience in systems administration, DevOps, cloud/hosting operations, cybersecurity engineering, or infrastructure operations.
Specific professional experience (Section 3.4.4 of the assessment grid)	5 years of experience deploying and operating secure web applications, including staging/production environments, CI/CD, monitoring, logging, backups, disaster recovery, vulnerability remediation, and performance optimization.
Leadership/management experience (Section 3.4.5 of the assessment grid)	Not Applicable
Experience in the field of development cooperation (Section 3.4.6 of the assessment grid):	Not Applicable
Other (Section 3.4.7 of the assessment grid)	Not Applicable

10.5 Expert 5: QA, Testing and Acceptance Specialist (Section 3.5 of the assessment grid)

Responsibilities of Expert 5: QA, Testing and Acceptance Specialist

- Prepare the testing concept, test plan, test cases, defect log, acceptance checklist, and test documentation for all website features and workflows.
- Conduct functional, regression, cross-browser, cross-device, accessibility, usability, performance, and workflow testing across public pages, CMS, admin portal, notifications, feedback, content moderation, tenders, vacancies, and social media controls.

- Coordinate security testing with the DevOps/security engineer and verify remediation of vulnerabilities and weak points.
- Support user acceptance testing with designated FHC representatives and document feedback, faults, weak points, improvements, and final acceptance status.
- Verify that only systems meeting defined quality and security criteria are recommended for production deployment.
- Provide QA reports, test evidence, and lessons learned for the final documentation package.

Qualifications of Expert 5: QA, Testing and Acceptance Specialist

Education/training (Section 3.5.1 of the assessment grid)	University degree in computer science, software engineering, information systems, quality assurance, or a related field. ISTQB or equivalent software testing certification.
Language (Section 3.5.2 of the assessment grid)	Knowledge of English at B2 level in the Common European Framework of Reference for Languages.
General professional experience (Section 3.5.3 of the assessment grid)	6 years of professional experience in software testing, quality assurance, user acceptance testing, or software quality management.
Specific professional experience (Section 3.5.4 of the assessment grid)	4 years of experience testing responsive websites, CMS platforms, admin portals, role-based workflows, search/filter functions, notification modules, security controls, accessibility, browser/device compatibility, and performance browser/device compatibility and performance/load testing of production web applications
Leadership/management experience (Section 3.5.5 of the assessment grid)	Not Applicable
Experience in the field of development cooperation (Section 3.5.6 of the assessment grid):	Not Applicable
Other (Section 3.5.7 of the assessment grid)	2 years of professional experience in test-case design, defect management, accessibility checks, performance testing, security-test coordination, browser/device testing and acceptance documentation.

10.6 Expert 6: Documentation, Training and Knowledge Transfer Specialist (Section 3.6 of the assessment grid)

Responsibilities of Expert 6: Documentation, Training and Knowledge Transfer Specialist

- Prepare comprehensive user and administrator documentation, including user manuals, administration manuals, maintenance guidance, backup guidance, troubleshooting guides, and guidelines for updating manuals.
- Coordinate with technical experts to compile arc42-style reference documentation covering software stack, dependencies, diagrams, architecture, database design, integrations, security procedures, and operational processes.

- Design and deliver two days of administrative training for FHC IT personnel, including hands-on system administration, maintenance, troubleshooting, backups, user roles, and security procedures.
- Design and deliver three days of user training for FHC website and CMS users, including content creation, editing, approval, publishing, notifications, tenders, vacancies, resources/judgment publication, feedback handling, analytics, and moderation.
- Prepare training materials, exercises, attendance records, knowledge-transfer notes, and training evaluation summaries.
- Support final handover by ensuring FHC staff can operate and manage the CMS and administrative portal independently.

Qualifications of Expert 6: Documentation, Training and Knowledge Transfer Specialist

Education/training (Section 3.6.1 of the assessment grid)	University degree or professional qualification in education, instructional design, information systems, computer science, technical communication, knowledge management,
Language (Section 3.6.2 of the assessment grid)	Knowledge of English at B2 level in the Common European Framework of Reference for Languages.
General professional experience (Section 3.6.3 of the assessment grid)	4 years of professional experience in technical documentation, digital training, IT user support, knowledge transfer, or change management.
Specific professional experience (Section 3.6.4 of the assessment grid)	3 years of experience preparing user manuals, administrator guides, training materials, SOPs, and hands-on training for CMS, web applications, digital platforms, or administrative systems.
Leadership/management experience (Section 3.6.5 of the assessment grid)	Not Applicable
Experience in the field of development cooperation (Section 3.6.6 of the assessment grid):	Not Applicable
Other (Section 3.6.7 of the assessment grid)	2 years of experience facilitation skills, ability to translate technical concepts into practical operating procedures, and experience with adult learning, training evaluation, and knowledge-transfer documentation.

10.7 Expert 7: Content, Localization and Stakeholder Support Specialist (Section 3.7 of the assessment grid)

Responsibilities of Expert 7: Content, Localization and Stakeholder Support Specialist

- Support preparation, structuring, migration, and quality review of initial website content, including court information, service guidance, judgments/publications, notices, announcements, vacancies, tenders, FAQs, contact information, privacy, and terms pages.
- Advise on content governance, editorial workflows, content ownership, publication approval, translation/localization readiness, and content-update procedures.
- Support multilingual readiness and quality assurance of Amharic and English content, including labels, menu structures, help text, feedback forms, and notification messages.

- Assist FHC administrators in organizing content assets, optimizing images/documents, and applying consistent naming, metadata, and accessibility practices.
- Support moderated public interaction design by advising on feedback/comment handling, response categories, and escalation procedures.
- Coordinate with the training specialist to ensure examples and exercises reflect real FHC content-management tasks.

Qualifications of Expert 7: Content, Localization and Stakeholder Support Specialist

Education/training (Section 3.7.1 of the assessment grid)	University degree or equivalent professional qualification in communications, journalism, law, public administration, digital content management, translation/localization, information management,.
Language (Section 3.7.2 of the assessment grid)	Knowledge of English at B2 level in the Common European Framework of Reference for Languages. (7 points out of 10 points) Knowledge of Amharic at B2 level of proficiency. (3 points out of 10 points)
General professional experience (Section 3.7.3 of the assessment grid)	5 years of professional experience in digital content management, institutional communications, website content governance, localization, or public-information services.
Specific professional experience (Section 3.7.4 of the assessment grid)	3 years of experience preparing or migrating structured website content, publication workflows, FAQs, notices, announcements, document metadata, image/document optimization, and multilingual content for institutional websites.
Leadership/management experience (Section 3.7.5 of the assessment grid)	Not Applicable
Experience in the field of development cooperation (Section 3.7.6 of the assessment grid):	Not Applicable
Other (Section 3.7.7 of the assessment grid)	2 years of professional experience applying of institutional communication standards, editorial quality control, content accessibility, privacy-sensitive publication, and legal or court-related terminology

10.8 Expert 8: Pool 1 ‘Senior Full-Stack / CMS Developer’ with 2 experts (Section 3.8 of the assessment grid)

A CV for each expert must be submitted with the tender.

The expert days specified for this pool are total pool days to be distributed across the two proposed experts. They are not expert days per individual expert.

The actual number of experts assigned from the pool may differ from the number of experts specified in Section 10 of the Terms of Reference. For experts not named in the tender, GIZ must confirm before the assignment that their qualifications are equivalent to those of the experts proposed in the tender.

Responsibilities of the Expert Pool 1: Senior Full-Stack / CMS Developer

- Lead technical implementation of the public website, CMS functions, content templates, administrative portal, user management, publishing workflows, comments, notifications, and multilingual readiness.
- Implement secure frontend and backend components based on the approved implementation concept, architecture, UI/UX designs, and release plan.
- Develop reusable components and templates for pages such as court information, judgments, notices, announcements, vacancies, tenders, FAQ, gallery, contact, feedback, privacy, and terms.
- Implement role-based access control, audit trails, versioning, moderation, scheduled publishing, and administrative dashboards as required.
- Create API endpoints and integration mechanisms for notifications, document storage, analytics, controlled social media linking, sharing support and embedding, where approved, and future court-system integrations.
- Produce annotated source code and contribute to technical manuals, source-code documentation, deployment notes, and troubleshooting guidance.
- Implement the approved PHP/open-source technology stack, preferably using Drupal, Laravel, Symfony or equivalent.
- Implement CMS content models, templates, workflows, RBAC, audit logs, public content sections, moderated feedback/comments, fee calculator, vacancy module, tender/eGP redirection and agreed Case Tracker functionality.

Qualifications of the Expert Pool 1: Senior Full-Stack / CMS Developer

Education/training (Section 3.8.1 of the assessment grid)	All experts with a university degree in computer science, software engineering, information systems, web development.
Language (Section 3.8.2 of the assessment grid)	All experts with knowledge of English at B2 level in the Common European Framework of Reference for Languages.
General professional experience (Section 3.8.3 of the assessment grid)	All experts with 7 years of professional experience in software development, web application development, full-stack engineering, or CMS implementation
Specific professional experience (Section 3.8.4 of the assessment grid)	All experts with 5 years of experience implementing secure CMS-based or custom PHP web platforms using technologies such as Drupal, Laravel, Symfony or equivalent, including content workflows, RBAC, search, notifications, secure uploads, API/integration mechanisms and administrative portals.
Leadership/management experience (Section 3.8.5 of the assessment grid)	All experts with 2 years of experience leading development tasks, reviewing code, coordinating developers, or serving as technical lead in multidisciplinary software teams.
Development cooperation experience (Section 3.8.6 of the assessment grid)	Not Applicable
Other (Section 3.8.7 of the assessment grid)	Not Applicable

10.9 Expert 9: Pool 2 'Backend/API and Database Developer' with 2 experts (Section 3.9 of the assessment grid)

A CV for each expert must be submitted with the tender.

The actual number of experts assigned from the pool may differ from the number of experts specified in Section 10 of the Terms of Reference. For experts not named in the tender, GIZ must confirm before the assignment that their qualifications are equivalent to those of the experts proposed in the tender.

The expert days specified for this pool are total pool days to be distributed across the two proposed experts. They are not expert days per individual expert.

Responsibilities of the Expert Pool 2: Backend/API and Database Developer

- Design and implement the database schema for users, roles, permissions, content, comments, publications, notifications, subscriptions, audit logs, and configuration records.
- Build backend services for authentication, authorization, content approval, moderation, version control, search, subscriptions, internal memos, website notifications, and email alerts.
- Implement secure data access, input validation, encryption where applicable, session handling, password management, logging, and auditability.
- Develop APIs for internal modules, third-party services, analytics, document storage, and controlled social media publication actions.
- Prepare migration scripts, backup and restoration procedures, database documentation, and operational troubleshooting notes.
- Support QA, security testing, performance tuning, deployment, and post-deployment defect resolution.
- Implement database structures and backend services for case-status/court-appointment access, fee-calculation configuration, vacancy applications, document uploads, applicant status tracking, notifications, subscriptions, feedback/comments, audit logs and eGP redirection configuration.
- Support API-based or import-based integration with existing FHC systems where access, documentation and approvals are available.

Qualifications of the Expert Pool 2: Backend/API and Database Developer

Education/training (Section 3.9.1 of the assessment grid)	All experts with university degree in computer science, software engineering, data engineering, information systems, or a related field
Language (Section 3.9.2 of the assessment grid)	All experts with knowledge of English at B2 level in the Common European Framework of Reference for Languages.
General professional experience (Section 3.9.3 of the assessment grid)	All experts with 7 years of professional experience in backend development, API development, database design, or web application engineering.
Specific professional experience (Section 3.9.4 of the assessment grid)	All experts with 5 years of Experience in secure PHP/backend development, relational database design, API integration, data import/synchronisation, secure file handling, audit logging, RBAC, search indexing,

	backup/recovery and performance tuning for production web systems.
Leadership/management experience (Section 3.9.5 of the assessment grid)	Not Applicable
Development cooperation experience (Section 3.9.6 of the assessment grid)	Not Applicable
Other (Section 3.9.7 of the assessment grid)	All experts with 3 years of professional experience applying database normalization, query performance, API security, logging, auditability, data protection principles, backup strategies, and maintainable backend architecture.

The tenderer must assign all the proposed experts to the required qualifications and clearly present them in a separate table preceding the CVs. The summary presentation must mention only qualifications that are actually indicated in the CVs. Evidence of professional experience must be rendered in the form of meaningful references in the CVs. It is advisable to make specific reference to each instance of professional experience.

Soft skills of team members

In addition to their specialist qualifications, all team members are also expected to have the following qualifications:

- Team players
- Initiative
- Communication skills
- Sociocultural and intercultural skills
- Efficient partner- and client-oriented working methods
- Interdisciplinary thinking

Soft skills will not be evaluated.

11. Costing requirements

11.1 Assignment of experts

In your tender, please do not deviate from the specification of quantities required in these ToR (number of experts and expert days, budget specified in the price schedule). This is part of the competitive tender and is used to ensure that the tenders can be compared objectively. Please note only services that were commissioned by GIZ and rendered by the contractor will be remunerated. We would also like to point out that it may not be necessary to make use of the total number of proposed expert days.

The number of expert days corresponds to full working days.

Expert	**Expert days**
Key Expert 1: Team Leader / IT Project Manager	**55**
Expert 2: Business Analyst / Solution Architect	**45**
Expert 3: UI/UX and Accessibility Specialist	**30**
Expert 4:	**35**

DevOps, Hosting and Security Engineer	
Expert 5: QA, Testing and Acceptance Specialist	**45**
Expert 6: Documentation, Training and Knowledge Transfer Specialist	**35**
Expert 7: Content, Localization and Stakeholder Support Specialist	**20**
Expert 8 (Expert Pool 1): Senior Full-Stack / CMS Developer	**80**
Expert 9 (Expert Pool 2): Backend/API and Database Developer	**55**
Total	**400**

11.2 Travel expenses

11.2.1 Travel – sustainability considerations

GIZ would like to reduce greenhouse gas emissions (CO_2 emissions) caused by travel. When preparing your tender, please incorporate options for reducing emissions, for example by selecting the lowest-emission booking class (economy) or using means of transport, airlines and flight routes that are more CO_2-efficient. For short distances, travel by train (second class) or e-mobility are the preferred options.

CO_2 emissions resulting from air travel must be offset. GIZ specifies a budget for this which enables carbon offsets can be settled against evidence.

There are many different providers in the market for emissions certificates, and they have different climate impact ambitions. The *Development and Climate Alliance* has published a *list of standards*. GIZ recommends using these standards.

11.2.2 Travel expense requirements

Travel expenses must be costed as follows by the contractor:

Travel expense item	Number/amount	Note
Total number of international flights (7 return flights)	7	Calculated as 7 return flights / 14 flight legs
CO2 offsets for flights	EUR 1,820.00	Fixed budget for CO2 offsets
Transfer costs	EUR 1,400.00 (unalterable budget, to be settled against evidence)	Linked to arrival/departure and local project movements
Per-diem allowances	28 days	Indicative assumption: 7 trips x 4 days
Accommodation allowances	28 nights	Indicative assumption: 7 trips x 4 nights
Costs of obtaining a visa	14 business visas	To be settled against evidence where applicable

Per-diem allowances are reimbursed as a lump sum up to the maximum amount of **44,00 EUR** as permissible under tax law for each country as set out in the country table in the circular from the German Federal Ministry of Finance on travel expense reimbursement (download at https://www.bundesfinanzministerium.de).

In addition, for the following items, reasonable costs can be settled against evidence up to the proposed amount.

- Flight costs
- Transfer costs
- Costs of obtaining a visa

Notes on settling accommodation allowances outside Germany.

For the country Ethiopia, tenderers may offer accommodation allowances up to EUR 159.00. This is the maximum amount permissible under tax law as per the BMF circular on travel expense reimbursement.

- If the contractor offers accommodation allowances at up to 75% (EUR 119.25) of the maximum amounts permissible under tax law as per the BMF circular on travel expense reimbursement, the expenses will be reimbursed **on a lump-sum basis** in the contractually agreed amount.

- If the contractor offers accommodation allowances at between 75% (EUR 119.26) and 100% (EUR 159.00) of the maximum amounts permissible under tax law as per the BMF circular on travel expense reimbursement, the corresponding **evidenced expenses** will be reimbursed up to the contractually agreed amount.

11.3 Materials and equipment

The contractor shall provide all equipment, software tools, development environments, communication tools, testing tools, and technical resources required for the performance of the assignment. This includes laptops, development tools, project management tools, source-code management tools, testing tools, and any other working materials required by the contractor's team.

FHC and GIZ are not responsible for providing contractor equipment. Any required access to FHC systems, hosting environments, official content, domain-related information, email gateways, or other institutional resources shall be coordinated during the implementation concept phase.

11.4 Workshops, training

No separate lump sum or additional budget for training delivery is foreseen. Preparation and delivery of the training activities specified under Section 3.6 shall be covered by the expert-days specified in this ToR.

Training venues and standard venue logistics required for the agreed sessions shall be provided or arranged by GIZ/FHC and shall therefore not be costed by the contractor.

11.5 Hosting

Procurement and payment of the production hosting service are not part of this contract. FHC/GIZ will provide or separately procure the production hosting environment.

The contractor shall provide the minimum technical hosting requirements and shall perform the configuration, deployment, migration, testing and handover activities required to operate the solution in the designated environment. These services shall be covered by the relevant expert days and shall not be priced as a separate hosting service.

No production-hosting subscription costs shall be included in the financial offer.

11.6 Other costs

No separate recurring licence, SaaS, plugin or other third-party service costs are foreseen under the scope of these ToR. Standard development and testing tools required by the contractor shall be covered by the contractor and shall not be charged separately..

11.7 Flexible renumeration

Budget for flexible remuneration: EUR 35,000.00

The fixed, unalterable budget above is given in the price schedule for flexible remuneration. Flexible remuneration is intended to facilitate the flexible management of the contract by the officer responsible for the commission at GIZ. The contractor can make use of the funds in accordance with Section 18.4 of the GIZ's Special Terms and Conditions of Contract.

The flexible renumeration may be used, for instance, for on-demand in-person meetings with the FHC at the FHC premises which entail travel costs.

12. 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 technical bid must be submitted in English.

The technical and methodological concept of the tender (Section 9 of the ToR) is not to exceed 15 pages (not including the cover page, list of abbreviations, table of contents and brief introduction). If any of the prescribed page limits is exceeded, the contents of the pages that are over the limit will not be considered in the assessment. Additional annexes not requested will not be assessed. External content (e.g. links to websites) will also not be considered.

The presented CVs must clearly and unequivocally show what position the proposed person held, which tasks they performed and how long they worked during which period in the specified references. The references contained in the CVs must therefore include the following information:

- Name of the company/organisation/reference project in which the expert worked
- Position held and task(s) performed by the expert in the company/organisation/reference project

- Work outcomes or products produced by the expert, or expert's contribution to the completion of these outcomes and projects (if relevant)
- Duration of the expert's assignment in the company/organisation/reference project per calendar year in full-time expert days, weeks or months (for example: 2019: 2 months, 2020: 10 months, 2021: 1 month)
- Leadership experience/management: clear information on the reference projects or fixed positions within the company/organisation in which the requirements specified in Section 10 were fulfilled (for example, period, number of persons for whom the expert had disciplinary responsibility, project budget) (if relevant)
- International professional experience/professional experience in the country of assignment: clear information on the reference projects or fixed positions in the company/organisation in which the requirements specified in Section 10 were fulfilled (for example, actual duration of assignment on the ground in full-time expert days, weeks or months) (if relevant)

In order to facilitate the assessment, we request that your number the references consecutively and provide only references that are clearly related to the object of this tender.

13. Annexes

Annex 1: Federal High Court Website Proposal Version I

Annex 2: FHC Website-CMS_Design Prototype

Annex 3: Documentation of OSS Components