United Nations Children's Fund

Child Survive and Development Section

Terms of Reference

Re-design, Enhancement and Support the CRVS (Digital Birth Registration) system for Ministry of Health, Iraq

- Background
- Purpose & Objectives
- Scope of Work
- Deployment Models and System Variants
- Key Deliverables, Performance Indicators and Duration
- Roles and Responsibilities
- Non-Functional Requirements
- Security Requirements
- Development Approach
- Team Composition and Qualifications
- Quality Assurance and Monitoring
- Intellectual Property and Data Ownership
- Coordination
- Reporting requirements
- Handover and Capacity Building
- Location and Duration
- Evaluation process and methods
- Payment Schedule
- Financial Administration
- General Terms and Conditions

March - 2026

Section	Content
Background	Civil Registration and Vital Statistics (CRVS) systems are foundational to effective governance, service delivery, and the protection of individual rights. In alignment with national digital transformation priorities, the Ministry of Health (MoH) has undertaken the development of a CRVS system to modernize Birth Registration and related civil documentation processes. Over successive development phases, the CRVS system has enabled the digitization of key registration processes and supported interoperability with government systems. However, accelerated implementation timelines, evolving legal and regulatory frameworks, and expanding system usage have introduced technical debt and highlighted gaps in scalability, resilience, user experience, and governance. The current initiative does not represent a new or standalone project, but rather a continuation and strengthening of existing investments, systems, and institutional capacity. The 2026 Roadmap is built directly on the existing CRVS platform and focuses on consolidating, improving, and future-proofing the work already completed. It emphasizes quality improvement, architectural refactoring, and compliance with both federal and KRG requirements, rather than replacement or duplication of systems. This TOR therefore supports a structured improvement phase aimed at strengthening a shared national CRVS platform while ensuring that jurisdiction-specific requirements particularly those of the National Data Center (NDC) at the federal level and the Department of Information Technology (DIT) in the KRG are fully met.
Purpose and Objectives	To strengthen the national CRVS/Birth Registration system and address the current system challenges through a secure, scalable, and digital-first platform that improves service delivery, data quality, system resilience, and interoperability across government entities, some main challenges are listed 1. Architecture Limitations: The current CRVS platform was developed incrementally over previous phases and includes several monolithic components that limit scalability, deployment flexibility, and independent service upgrades. This architecture introduces operational constraints when introducing new integrations or scaling system capacity. 2. User Experience Bottlenecks: Existing workflows were designed for paper-assisted processes. As usage expands across health facilities and civil registration offices, users require simplified digital-first interfaces, clearer workflow states, and improved data entry validation to reduce operational errors. 3. Integration Constraints: The current CRVS system requires stronger integration with external government platforms. Integration approaches currently vary across implementations. The system must support standardized data exchange mechanisms including RESTful APIs, OAuth2 /JWT authentication and HTTPS TLS 1.2 or higher encryption. 4. Federal and Kurdistan Deployment Divergence:

	The CRVS platform operates across both Federal Iraq and the Kurdistan Region, where infrastructure requirements differ. Maintaining a unified system while supporting jurisdiction-specific requirements remains a key architectural challenge. **Specific Objectives** 1. Transition of the CRVS system from paper-first to a fully digital-first model. 2. Improve system scalability, availability, and resilience. 3. Enhance interoperability with other health and external government systems. 4. Strengthen data access, search, analytics, and reporting capabilities. 5. Improve user experience, accountability, and security.
Scope of Work	**1. Digital-First CRVS Transformation** • Redesign and implement fully digital workflows for birth certificates, Qaid, and Huja records. • System-generated unique numbering and sequencing with conflict-free multi-server support. • Digitization and integration of legacy paper records. • Extension of digital record fields to support regulatory and data-quality requirements. **2. Interoperability and Integration (MoFA)** • Enhance system integration with MoFA services. • Implement secure authentication mechanisms, including dynamic client certificate-based authentication. • Align business workflows with MoFA operational and legal requirements. **3. System Architecture and Service Separation** • Refactor monolithic components into independent, scalable services. • Establish standalone services for: a) QR Code Generation and Validation b) National Data Center (NDC) Integration c) Background Job Processing **4. Search and Data Access Enhancement** • Refactor read-side architecture and repositories. • Implement advanced search features, including faceted search, filters, autocomplete, and advanced queries. **5. Authentication and Identity Management** • Design and deploy a standalone authentication and authorization service. • Enable secure access for external systems and third-party APIs. • Add Central Authentication Service (CAS) support for authentication via the Department of Information Technology (DIT) in Kurdistan, ensuring federation with government identity infrastructure. **6. User Experience (UX/UI) Redesign** • Redesign user interfaces to align with digital-first workflows. • Improve usability, accessibility, and operational efficiency. **7. User, Settings, and File Management** • Implement comprehensive user audit trails (login, logout, credential changes, profile updates).

	• Introduce an Admin-Configurable Settings Management Module to enable authorized administrators to manage system settings without code changes, including: a) Workflow toggles and business rules b) Numbering/sequence configuration parameters (where policy allows) c) Integration endpoints and certificates (securely stored) d) Notification templates and routing e) Feature flags and UI configuration f) Security and session configuration (within approved policies) • Apply full auditing for settings changes (who/what/when), versioning/rollback, and role-based access controls. • Upgrade file management to support: a) Multi-storage backends b) Document categorization c) Versioning and permissions d) File audit trails and advanced search **8. Dashboards and Notifications** • Develop real-time dashboards for operational, performance, and usage analytics. • Implement real-time notifications for record status changes and system alerts. **9. Database Modernization and Portability** • Introduce PostgreSQL support and enable migration from Microsoft SQL Server while maintaining data integrity, performance, and functional parity. • Deliver database abstraction and compatibility updates at application and reporting layers. • Develop and execute a migration plan, including: a) Schema conversion and data migration tooling b) Validation scripts and reconciliation checks c) Performance testing and indexing optimization d) Cutover plan and rollback procedures **10. Asynchronous Processing and Performance Optimization** • Implement a message broker (e.g., RabbitMQ or Kafka) for async processing and inter-service communication. • Deploy a distributed caching system (e.g., Redis or Memcached) to reduce database load and improve response times. **11. Integration with Catchment Areas and DHIS2** • Connect the CRVS system with health facility catchment areas definitions to ensure accurate geographic attribution of birth and vital events. • Enable linkage between CRVS records and District Health Information Software 2 (DHIS2) to support public health reporting, planning, and monitoring. • Ensure alignment of administrative boundaries, facility identifiers, and location hierarchies between CRVS, DHIS2, and relevant MoH systems. • Support automated, secure, and auditable data exchange mechanisms, respecting data protection, aggregation rules, and access controls. • Allow configuration-based mapping to accommodate jurisdiction-specific differences in catchment areas and reporting requirements. **12. Design and implement a dedicated registration form and associated system workflow for children of unknown parentage.** **13. Capacity Building for MOH technical team:** • Administrative Workflows: Managing user roles, permissions, and system audit logs

<table>
<tr><td></td><td>

Interoperability Maintenance: Training on creating and managing the API connectors to other systems.
Source Code & Repository Management: Training on how to manage the code within the repositories.
Database & Backup Management: Procedures for database maintenance and disaster recovery drills.
Reports and dashboards: Training on how to create and manage reports and indicators within the system.

14. Technical Support for the current and enhanced systems: The contractor shall provide continuous technical support and maintenance for the existing CRVS system starting after the contract commencement date, ensuring system stability and issue resolution.
Following the completion and deployment of the enhanced CRVS system, the contractor shall provide an additional three (3) months of dedicated technical support for the upgraded system, including bug fixing, performance optimization and minor enhancements.
</td></tr>
<tr><td>Deployment Models and System Variants</td><td>
The CRVS system currently supports separation between the federal (Baghdad) and Kurdistan Region (KRI) deployments through configuration-based mechanisms. This approach has enabled the system to address differing institutional, regulatory, and technical requirements while maintaining a shared platform.
This existing configuration-based separation will be assessed against evolving requirements from the MoH, NDC, DIT and UNICEF.
Based on this assessment, the implementation may include one or more of the following, subject to stakeholder agreement:

Continued enhancement of the configuration-based separation model
Progressive architectural divergence of selected components or services
A controlled fork into two related CRVS projects (federal and Kurdistan), if required to meet legal, governance, security, or operational constraints
Defined and secure integration and data exchange mechanisms between the two systems.

Any selected approach shall ensure compliance with federal and KRG regulations and policies
</td></tr>
<tr><td>Key Deliverables and Performance Indicators</td><td>
The contractor shall deliver the following outputs, each subject to technical validation, performance testing, and user acceptance by MOH and UNICEF. Deliverables will be implemented over a five (5) month development and enhancement phase, followed by a three (3) month post-deployment technical support phase for the enhanced CRVS system.
In parallel, continuous technical support and maintenance for the existing CRVS system shall commence from the start of the contract and continue throughout the full contract duration.
The overall contract duration is therefore eight (8) months, comprising implementation and support phases. Deliverables will be considered successfully completed only upon meeting functional, performance, and user acceptance criteria.
<table>
<tr><th>Milestone</th><th>Estimated Timeline</th></tr>
<tr><td>Modular, service-oriented CRVS architecture</td><td>Month 2</td></tr>
<tr><td>Advanced search and data access capabilities</td><td>Month 2</td></tr>
<tr><td>Standalone authentication service</td><td>Month 2</td></tr>
<tr><td>Redesigned UX/UI across CRVS modules</td><td>Month 2</td></tr>
<tr><td>Fully digital-first CRVS workflows</td><td>Month 3</td></tr>
<tr><td>Database Modernization and Portability</td><td>Month 3</td></tr>
<tr><td>Asynchronous Processing and Performance Optimization</td><td>Month 3</td></tr>
<tr><td>Implementing the Unknown Parentage Form</td><td>Month 3</td></tr>
</table>
</td></tr>
</table>

	Message broker and distributed caching systems	Month 3
	Operational MoFA integration with secure authentication	Month 4
	Enhancing the User, Settings, and File Management	Month 4
	Real-time dashboards and notification system	Month 5
	Integration with Catchment Areas and DHIS2	Month 5
	Capacity Building	Month 5
Roles and Responsibilities	• **Ministry of Health (MoH):** Strategic oversight, policy alignment, stakeholder coordination. • **CRVS Development Team:** System design, development, deployment, and documentation. **UNICEF / Development Partners:** Technical guidance, quality assurance, and alignment with international best practices (as applicable).	
Non-Functional Requirements	These sections (Non-Functional Requirements, Security, Handover, Team Composition, QA, IP, Coordination, Reporting, Evaluation, Payment) should be adapted from the TOR, with a strong emphasis on: • Integration: The ability to seamlessly connect with the current MIS is paramount. Bidders must demonstrate experience in integrating new modules into legacy systems. • APIs: Development of secure, well-documented APIs (e.g., using OAuth 2.0, JWT) for both current integration and future use. • Evaluation: The technical evaluation should prioritize proven experience in systems integration and the specific technologies proposed for the new modules and APIs. • Responsive web-based interface (mobile/tablet/desktop). • Arabic, Kurdish and English UI language support. • GDPR-compliant data handling and secure login protocols. • Open-source or license-free backend required. • Hosting Environment: The CRVS should be designed to support on-premise hosting at MOH's servers, system deployment should comply with MOH recommended approach and capable of future migration between hosting environments (cloud-to-on-prem or vice versa) without data loss. • The system shall be designed as a highly sensitive government information system and must meet the security, privacy, auditability, resilience, and hosting requirements defined in this TOR.	
Security Requirements	The CRVS system processes highly sensitive personal and civil registration data and supports a critical government service. For the purpose of this TOR, the system shall be treated as a highly sensitive government information system requiring the highest level of protection for confidentiality, integrity, and availability. This includes, at minimum, birth registration data, identity-related personal data, parent and child information, civil status data, supporting documents, audit records, and associated metadata. The service provider shall design, develop, deploy, and support the system in accordance with a security-by-design and data-protection-by-design approach. The requirements below shall apply to both the enhanced CRVS solution and any associated tools, integrations, services, environments, or infrastructure used in delivery. UNICEF and the Ministry of Health reserve the right to validate the adequacy and implementation of these controls. 1. General Security Requirements a. The Ministry of Health, with support from UNICEF where applicable, shall reserve the right to assess the quality and adequacy of outsourced software development, operational maintenance, hosting arrangements, and security controls through security	

	assurance testing, audits, vulnerability testing, penetration testing, and external assessments. b. The solution shall be protected from unwanted network traffic through appropriate segmentation, firewalls, filtering measures, secure gateways, and access controls. c. All servers, endpoints, and hosting components supporting the CRVS solution shall implement baseline protections including malicious code protection, host-based firewalls, secure configuration, and least-privilege access rules. d. Production, test, and development environments shall be logically separated, and where feasible physically separated, to reduce security and operational risks. 2. Data Classification and Protection a. All birth registration records and related civil documentation handled by the system shall be treated as highly confidential personal data. b. The system shall protect data throughout its lifecycle, including creation, storage, processing, transmission, backup, archival, and deletion. c. Access to personal and registration data shall be role-based, traceable, and limited strictly to authorized users and systems. d. Any deletion or disposal of sensitive data shall be performed in a manner that prevents reconstruction or unauthorized recovery. 3. Validation of Security Controls a. The Ministry of Health and UNICEF reserve the right to periodically validate the implementation of the security requirements through: • Security assurance testing • Vulnerability assessments • Penetration testing • Configuration and code reviews • Audits and on-site verification b. The vendor shall cooperate fully with these validation activities and remediate confirmed findings within agreed timelines. 4. Compliance and Certifications a. If the bidder proposes hosted infrastructure, managed platforms, or third-party hosting services, the bidder shall disclose the applicable security certifications and control framework in place. b. Hosting or managed service providers are strongly encouraged to demonstrate compliance with recognized standards such as ISO/IEC 27001, and where applicable provide supporting evidence such as certification status, statement of applicability, SOC reports, or equivalent documentation. c. Where government-hosted deployment is used, the vendor shall align with the applicable government hosting and security requirements of the Ministry of Health, National Data Center, or Department of Information Technology, as applicable. 5. Identification, Authentication and Authorization a. The solution shall enforce the principle of least privilege. Users, roles, service accounts, and device identities shall be uniquely assigned and controlled. b. The solution shall support centralized identity and access management and federation with approved government identity services where available, including DIT/CAS in the Kurdistan Region as applicable. c. Where password-based authentication is used, password controls shall follow current good practice, including complexity, storage, rotation, reset controls, and lockout protections. d. Multi-factor authentication shall be used for privileged accounts and for remote or external administrative access.

	e. Default accounts and credentials shall be removed, disabled, or changed before go-live. f. Creation, deletion, and modification of user and system accounts shall follow formal authorization procedures. g. Application source code, configuration files, scripts, or repositories shall not contain hard-coded credentials, tokens, or private keys. 6. Availability, Resilience and Backup a. The system shall be designed to meet the high availability needs of a critical registration service. b. The solution shall include backup, restore, and disaster recovery procedures appropriate to the criticality of the service. c. Recovery objectives, backup frequency, retention periods, and restoration testing shall be documented and agreed during implementation. d. The solution shall support continuity of service in the event of infrastructure failure, connectivity disruption, or component outage, including through failover, redundancy, or other agreed resilience mechanisms where applicable. 7. Cryptography a. Sensitive data shall be protected using strong cryptographic controls during transmission and, where applicable, at rest. b. Industry-standard secure communication protocols shall be used and kept current. Obsolete or insecure protocols shall not be used. c. Passwords and secrets shall be protected using strong hashing or encryption practices and secure key management controls. d. Encryption keys, certificates, and secrets shall be securely stored, access-controlled, and not embedded directly in application code. e. Personal data displayed in logs, reports, dashboards, or diagnostic tools shall be masked, pseudonymized, or otherwise protected where full exposure is not operationally required. 8. Secure Development a. The system shall be engineered using security by design and data protection by design and by default principles. b. Development and testing activities shall use fictitious, anonymized, or pseudonymized data wherever possible. c. Access to source code, repositories, specifications, architecture documents, and test artefacts shall be strictly controlled. d. All custom-developed source code shall undergo security review and appropriate testing before release. e. Production deployment shall not occur until functional testing, UAT, and agreed security checks are completed and approved. f. The system shall display generic error messages and must not expose sensitive system, account, database, or infrastructure information to end users. 9. Security Operations a. The system and its supporting infrastructure shall be hardened prior to production use. b. Only required services, ports, interfaces, and accounts shall be enabled. c. Patch management procedures shall be documented, including classification of critical and non-critical updates, testing approach, and deployment timelines. d. Critical security patches shall be applied on a priority basis within agreed timelines after appropriate testing. e. Development tools shall not be present in the production environment.

	f. Configuration files, source code, and customizations shall be protected from unauthorized access or modification and maintained under controlled backup and recovery arrangements. g. Malware protection measures shall be implemented and monitored where relevant to the hosting environment. 10. Vulnerability Management a. The vendor shall conduct security testing prior to launch and periodically thereafter during the support period. b. The vendor shall provide security scan reports and remediation updates to the designated Ministry of Health focal point and UNICEF focal point. c. Findings shall be classified by severity and remediated according to agreed timelines. d. No critical vulnerabilities shall remain unresolved at go-live unless formally risk-accepted by the authorized stakeholders. 11. Change Management a. Any change to the CRVS system, integrations, security configuration, or production environment shall follow a formal change management process. b. Post-baseline changes shall be documented with version/build number, purpose, risk assessment, testing evidence, and deployment outcome. c. Only trained and authorized administrators shall perform changes to operational software, applications, databases, certificates, and program libraries. 12. Log Management and Monitoring a. The system shall generate audit trails for all key actions involving personal data, user authentication, authorization changes, administrative activities, file actions, settings changes, and system integrations. b. Logs shall be securely stored, protected from unauthorized access or tampering, and retained according to agreed policy. c. Logs and events shall be structured in a format that supports monitoring, investigation, and integration with log management or SIEM tools where applicable. d. Integrity checking of logs shall be performed to help ensure consistency and detect unauthorized changes. e. The system, application, and supporting services shall be actively monitored. 13. Security Incident Management a. A security incident includes any actual or suspected unauthorized access, disclosure, alteration, destruction, loss, corruption, service compromise, or misuse affecting the CRVS system, its data, or supporting infrastructure. b. The vendor shall maintain and document a security incident notification and escalation process. c. Any security incident or suspected breach affecting the system shall be reported to the Ministry of Health and UNICEF within 24 hours of detection. d. An initial incident report shall be submitted within 72 hours, followed by investigation updates and a remediation plan. e. The vendor shall cooperate with the Ministry of Health, hosting authorities, and UNICEF in investigation, containment, recovery, and lessons learned activities.
Development Approach	The solution shall follow an Agile methodology with iterative deliveries, structured in the following phases: 1. Requirements Gathering & Systems Assessment 2. Design & Architecture Finalization 3. Development & Internal Testing 4. Piloting 5. System Administration Training & Capacity Building

	6. Deployment & Maintenance Handover.
Team Composition and Qualifications	Outline the expected minimum qualifications: • Project Manger • Front End Developer • Back End Developer • UI/UX Designer • Database Specialist • QA Tester
Quality Assurance and Monitoring	Quality assurance activities will include: • Weekly progress reviews with MOH and UNICEF • User acceptance testing with operational users • Performance testing under simulated system loads • Security validation testing • Verification of system availability and uptime metrics Successful completion of the project requires meeting the functional, performance, and security requirements defined in this TOR.
Intellectual Property and Data Ownership	• Data privacy must align with UNICEF policies, such as the UNICEF Data Protection Policy, and Iraq national regulations. • Source Code is owned by UNICEF and will fully delivered to MOH.
Coordination	• A technical steering committee shall be established to oversee the implementation of the project. The committee should include representatives from MOH and UNICEF. The committee will meet monthly and may convene additional ad-hoc meetings as needed to address emerging issues and ensure smooth coordination across stakeholders.
Reporting Requirements	• Weekly written progress reports. • Quarterly detailed reports. • Change and incident reports. • End-of-project final report summarizing activities and outcomes.
Handover and Capacity Building	The Contractor shall ensure a full and smooth transfer of the enhanced CRVS to MOH, including technical ownership and staff capacity building. The handover must include: • **Full System Delivery:** Transfer of all developed components, including the complete source code, database scripts, APIs, credentials, and system configurations. • **Technical Documentation:** Provision of complete system documentation, including architecture design, API specifications, installation manuals, administrator guides, and user manuals. • **Training and Knowledge Transfer:** Delivery of practical training sessions for MOH technical staff and system users, along with editable training materials (manuals, guides, FAQs). The training should cover system administration for all the integrated modules including all subsections. System technology orientation should be provided to MOH technical team. • **Final Handover and Acceptance:** All handover activities, including system deployment, training completion, source code delivery, and signed handover certificates, must be finalized before project closure.
Evaluation process and methodology	1. **Initial Technical Evaluation Pass/Fill approach:** Vendor must be passed all the requirements below to be considered for the technical evaluation process:

MANDATORY REQUIREMENTS	SUPPORTING DOCUMENTS	SCORE
Lead bidder is a legal entity regulated and licensed in Iraq.	A copy of the certificate of incorporation (i.e., company legal registration) or equivalent document verifying legal status is to be provided.	Pass / Fail
Lead bidder must demonstrate experience in MIS or digital system development in the public or Governmental sector.	At least two relevant examples, reference letters and supporting documents.	Pass / Fail

Then Bid shall be evaluated based on technical and financial criteria. The ratio weight between technical and financial criteria is (60:40).

2. **Technical Evaluation:**
   The Bid shall be technically evaluated as below:

	Technical evaluation Criteria	Max. Points Obtainable
i	**Company and organizational profile**	**15**
	Company Background and Presence in Iraq: Evaluation based on the firm's history, establishment, and understanding of the local context. The scores will be calculated as follows: Presence in Iraq = 5 points	5
	Relative Experience: Assessment of past similar projects and the firm's engagement/operations in Iraq or similar context with evidence considering the minimum 3 years requirement. The scores will be calculated as follows: 3-5 years=2 scores; 6 years=3 scores; 7 years=4 scores; +8 years=5 scores	5
	Reputation and Success Track Record: Consideration of the company's reputation, reliability, and success in delivering projects in Iraq. (Evidence provided for successful implementation of similar Projects in Iraq). The company provide evidence supporting this which could include client testimonials, industry reports, media coverage, online reviews, and feedback from stakeholders or partners. The scores will be calculated as follows: One evidence -2 points, two evidence – 3 points and three or more evidence provided – 5 points.	5
ii	**Proposed work plan and approach**	**30**
	Compliance with the ToR objectives and proposed system architecture aligned with modular design principles, API-readiness, and security-by-design principles appropriate for a highly sensitive government civil registration system. Bidders shall explain how their	15

		proposed architecture and implementation approach will meet the security obligations of a highly sensitive government civil registration system, including data protection, secure integrations, identity management, and operational security controls. System Architecture – 8 points Future Expansion Plan – 3 points Interoperability and Integration Architecture – 4 points	
		Proposed development approach (Agile/iterative preferred) and quality assurance strategy as following: Admin, Monitoring and Reporting Portals-4 points, QA plan- 2 points, Capacity Building Plan- 2 points, Development Approach- 2 points.	10
		Feasibility of timeline and clear project milestones.	5
	iii	**Company Key Resources**	**15**
		Appropriate technical resources with the right skills/expertise, qualifications (e.g certified developers) to deliver the outputs required; Key technical skills/expertise of Individual team members to be used to execute the assignment; Qualifications/level of education of key staff that will be assigned to this project, evidence of expertise/experience of each individual team member etc. The technical proposal should include the following: a) Technical Expertise and Skills of the team (12 points) The CVs of proposed team members, with the required qualification based on the required task. The CVs will be assessed against the depth and length of the experience and the strength of expertise and skills mentioned in this section. Relevant academic qualifications and certifications in information technology, cybersecurity, network infrastructure, or related fields will be necessary. Key qualifications and certifications of the team members will be evaluated and scored using the following criteria: Qualified Front End and Back End Developer/s = 4 points, Qualified Database Specialist/s = 4 points; Qualified UI/UX Specialist/s= 2 points: Qualified QA Specialist/s= 2 points. Certifications and qualifications are based on relevance as mentioned above. b) Expertise and Skills of the team leader (3 points) The CVs of proposed team leader/s with the required qualification based on the required task. The CVs will be assessed against the depth and length of the experience and the strength of expertise and skills mentioned in this section. Relevant academic qualifications and certifications in leading relevant technical projects will be required = 3 points.	15
		Total out of 60 (minimum passing score is 42)	**60**
	3. Financial Evaluation:		

<table>
<tr><td></td><td>The bidder will be financially scored based on formula below: The total weight of the bidder will be the cumulative of the formulas (Technical and Financial):
Bidder (A) = (Maximum score for price proposal (40 points) x Price of lowest priced proposal among technically passed bidders)/Price of proposal (A)</td></tr>
<tr><td>Payment Schedule</td><td>Payments are linked to successful delivery, validation, and acceptance of each milestone by MOH and UNICEF. A portion of the contract value shall be retained as a warranty retention, as defined below:
<table>
<tr><td>1</td><td>Modular, service-oriented CRVS architecture</td><td>30%</td></tr>
<tr><td></td><td>Advanced search and data access capabilities</td><td></td></tr>
<tr><td></td><td>Standalone authentication service</td><td></td></tr>
<tr><td></td><td>Redesigned UX/UI across CRVS modules</td><td></td></tr>
<tr><td>2</td><td>Fully digital-first CRVS workflows</td><td>40%</td></tr>
<tr><td></td><td>Database Modernization and Portability</td><td></td></tr>
<tr><td></td><td>Asynchronous Processing and Performance Optimization</td><td></td></tr>
<tr><td></td><td>Implementing the children of unknown parentage workflow</td><td></td></tr>
<tr><td>3</td><td>Operational MoFA integration with secure authentication</td><td>15%</td></tr>
<tr><td></td><td>Enhancing the User, Settings, and File Management</td><td></td></tr>
<tr><td></td><td>Integration with Catchment Areas and DHIS2</td><td></td></tr>
<tr><td>4</td><td>Real-time dashboards and notification system</td><td>15%</td></tr>
<tr><td></td><td>Technical documentation and Capacity Building for MOH technical team (Federal and KRI)</td><td></td></tr>
<tr><td colspan="2">TOTAL</td><td>100%</td></tr>
</table>
Payment dates will be counted from the start date of contract in link to the completion of the identified deliverables:
A) 30 % after 2 Months.
B) 40 % after 3 Months.
C) 15 % after 4 Month.
D) 15 % after 5 Months.

Warranty Retention:

UNICEF will retain a warranty amount equivalent to 10% of the contract value or the value of the completed work whichever is lower. Alternatively, the contractor may submit a Defect Liability/ (Warranty period) Bank Guarantee of the same amount, valid for three (3) months from the date of issuance of the Certificate of Substantial Completion.
The retained amount or bank guarantee will be released only after the successful completion of a three-month post-deployment technical support period for the enhanced CRVS system.
The release is subject to UNICEF’s confirmation that all deliverables have been satisfactorily met.
Any unresolved critical or major issues identified during the support period must be fully rectified before the retained amount or the bank guarantee can be released.</td></tr>
<tr><td>Financial Administration</td><td>UNICEF will make payments to the contractor in US $ Dollars if it’s an entity registered outside of Iraq with a bank account outside of Iraq or in IQD Iraq Dinar if the company is registered in Iraq, with a bank account in Iraq according to percentages of completed work</td></tr>
</table>

	certified by the supervising committee and approved by UNICEF focal person at Iraq Country Office. If the financial offer is in: 1. IQD (Iraq Dinars), it is important for a bidder to have an IQD bank account. 2. If a bidder quote in any other currency i.e. US Dollar (USD), below shall apply: a) Awards will be made based on the currency of their offer using the UN exchange rate at the date of bid submission. The bidder is required to have a bank account in the currency of their offer. If a bidder has quoted in USD (US Dollar) or any other currency, for evaluation purposes only, proposals submitted in USD or any other currency will be converted into IQD using the United Nations rate of exchange in effect on the submission deadline date
General Terms and Conditions	• Adherence to UNICEF's rules and regulations. b) Confidentiality clauses.

Prepared by:
Ali Abdulhusain
Health specialist 26th. 03.2026

Ali Rasheed
ICT/T4D Officer 26 March 2026

Endorsed by:
Ali Auob
OIC chief of CSD

26 Mar 2026

Reviewed by:
Lansana Sannoh
Supply & Logistics 26.03.2026

Approved by:
Laetitia Bazzi
Deputy Representative

30 Mar 2026