unicef
for every child

CRVS platforms

Key Findings for Practitioners

Glossary

API Application Programming Interface
CRVS Civil Registration and Vital Statistics
DPG Digital Public Good
FHIR Fast Health Information Resource
HMIS Health Management Information System
ICT Information Communication Technology
LMICs Low- and Middle-Income Countries
NGO Non-Governmental Organization
OCR Optical Character Recognition
SDGs Sustainable Development Goals
TCO Total Cost of Ownership
UNLIA United Nations Legal Identity Agenda

COVER
Chancelvie was born during the night of January 25 to January 26, 2022 at the Polyclinic Maman Henriette in N'Sele, Kinshasa. A nurse facilitated the declaration of her birth to the Civil Registry through the BIDA software. The French government is supporting the acceleration of universal birth registration through national capacity building in N'Sele, DRC. © UNICEF/UN0583927/Mulala

Content

1. **Overview**

About

This publication is for international development practitioners, both in programme and ICT divisions, who wish to understand and implement digitalised civil registration and vital statistics (CRVS) programmes. These findings highlight a selection of CRVS platforms. The platforms were selected after due consultations with stakeholders on existing CRVS offerings. Conducted by UNICEF (via a 3rd party vendor), the review assessed the functional and non- functional aspects, as well as maturity, of CRVS products.

The scope of this publication has limitations related to a) the exclusion of home-grown solutions and b) reliance on self-reporting by the vendors.

This publication is relevant to UN, government, and NGO actors. It is intended to guide planning, budgeting, technology selection, and implementation strategies. It is also intended to support planning and programme operations design that are fit for purpose and uphold value, feasibility, and sustainability principles.

Background

CRVS systems are key for measuring progress towards achieving Sustainable Development Goals (SDGs) such as:

- Improved child mortality, maternal health and other health services (SDG 3)
- Better education (SDG 4)
- Gender equality (SDG 5)
- Decent work (SDG 8)
- Reduced inequalities (SDG 10)
- Justice (SDG 16)
- Partnership (SDG 17, particularly 17.18: Availability of Data)

An effective CRVS system comprehensively documents all births, deaths, and other vital life events - including marriages, divorces, and adoptions.

Birth registration is a fundamental right recognized by the International Covenant on Civil and Political Rights and the Convention on the Rights of the Child. By registering births, the legal existence of a child is established, laying the foundation for securing a wide range of civil, political, economic, social, and cultural rights.

Furthermore, a dependable and current civil registry generates consistent demographic data that is robust, inclusive, secure and privacy-protecting. For example, this data can assist policymakers deciding where to invest in constructing new schools, allocating resources for social protection programs, or assigning healthcare and social workers to underserved areas.

The UN Secretariat has set out several principles and standards on CRVS through related **handbooks and guidelines**, which depict a well-functioning CRVS system that meets these requirements. The design of a CRVS system should be customised to suit the specific needs of the country it is intended for. A CRVS system should address the present as well as the future needs of stakeholders who will engage with the system, such as health departments and Ministries, and national identity agencies.

© UNICEF/UN0742462

2. CRVS Digitisation Needs and Challenges

Digital technologies offer unique opportunities to improve CRVS systems. Pages 8 and 9 show a diagram of an ideal, integrated CRVS system.

Opportunities

Digitisation of CRVS systems has the capacity to bring about significant enhancements by expanding registration coverage, standardising and simplifying civil registration and vital statistics procedures, consolidating data from multiple systems, and securely storing data on a large scale, all while remaining cost-effective.

To ensure successful implementation of CRVS digitisation, it is most important to select technology solutions that suit the country's context. This includes existing infrastructure and systems, e-Government policies, CRVS processes, human capacity, and operational procedures. Determining requirements requires a comprehensive analysis of these factors.

CRVS Digitisation Project Life Cycle

A: Preliminary	B: Analysis & Design	C: Implementation Planning
1. Define a Long-Term Vision for CRVS Digitisation 2. Develop a Business Case for CRVS Digitisation 3. Ensure legal framework is in place to support Digitisation	1. Initiate CVS Digitisation project 2. Define the CRVS Business Architecture 3. Conduct As-is Assessment of the CRVS Landscape 4. Identify CRVS Digitisation Opportunities and Limitations 5. Document the Target CRVS process 6. Define the CRVS Information Requirements 7. Define Target System Architecture 8. Define System Requirements	1. Document CRVS Digitisation Implementation Plan 2. Procure the digital CRVS System 3. Define the Change Management Approach and Plan 4. Define the Deployment Approach and Plan 5. Define the Training Approach and Plan 6. Define the Testing Approach and Plan 7. Define Operations Approach and Plan

Adapted from Civil Registration Digitisation Guidebook

Comprehensive guidance on how to approach the digitisation project, including the analysis of business processes leading up to implementation of the IT system, can be found in resources such as the CRVS Digitisation Guidebook, referenced in "CRVS Digitisation Project Life Cycle" above.

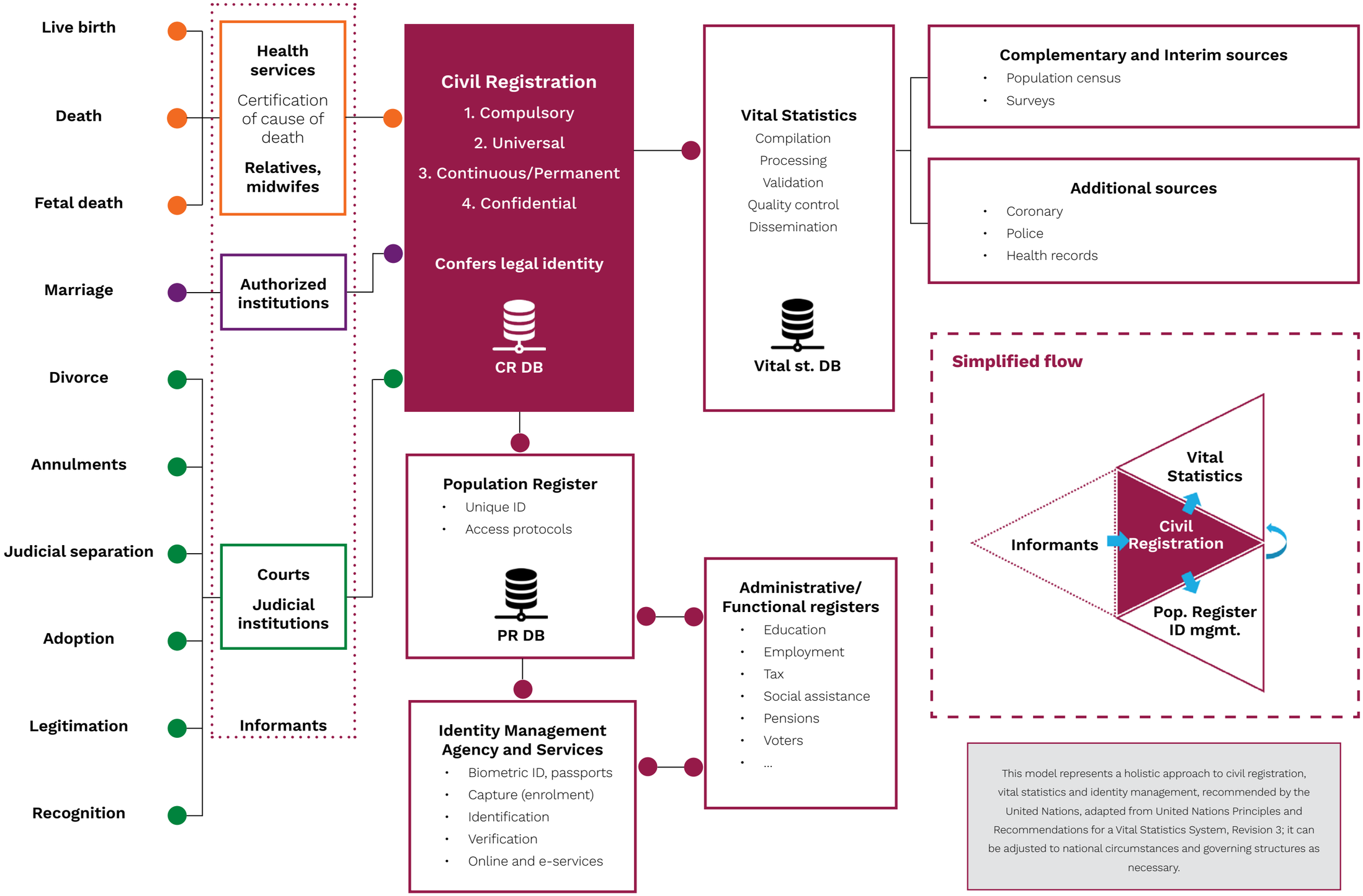
Challenges

CRVS digitisation can face numerous challenges. For instance, in many countries a portion of civil registration records are kept in decades-old paper forms stored in deteriorating books. This can create barriers for individuals seeking access to public services, even if their birth has been officially registered.

Keeping records in paper form requires considerable labour for government officials in comparison to digital record-keeping. Digitisation, when done correctly, will minimise risk of fraud, as well as help overcome difficulty in conducting legitimate affairs, such as authenticating birth certificates against records held in far-flung municipalities.

Converting CRVS systems from paper to digital format is a significant mechanical task, as it requires scanning a large volume of historical paper-based records using optical character recognition (OCR) technologies. Furthermore, OCR often is not suitable for low resource contexts due to the illegibility of historical records.

Civil Registration, Vital Statistics and Identity Management System



This model represents a holistic approach to civil registration, vital statistics and identity management, recommended by the United Nations, adapted from United Nations Principles and Recommendations for a Vital Statistics System, Revision 3; it can be adjusted to national circumstances and governing structures as necessary.

Source: United Nations Legal Identity Agenda: Fulfil the promise to Leave No One Behind

Once the CRVS digital system is up and running, there can be obstacles to capturing digital data accurately at the point-of-registration, as well as production of vital statistics from national databases dynamically updated with data from local registry offices.

Furthermore, the process of digitising CRVS systems may face an implementation hurdle as decision-makers may not anticipate sufficient tangible benefit in the near term to justify the project. Sustainable investment for CRVS systems relies on creating a stronger business case based on buy-in for the long-term advantages of digital infrastructure. This includes highlighting benefits that can be gained, such as improved accuracy, efficiency, and accessibility of data. All of these ultimately lead to more informed planning, decision-making, and resource allocation.

One way to counter common challenges is to use a systematic methodology for organising and prioritising product requirements at the onset of a CRVS digitisation project. This approach can play a key role in the development of product specifications. Strong specifications meet the needs of all stakeholders, including the decision-makers. These validated specifications also help ensure that the most critical requirements are given the highest priority. Understanding priorities in turn feeds into a detailed and realistic plan for how the project will be designed and implemented.

Requirement Hierarchy is one such product methodology. It begins with the high-level requirements. These feed into the user and then the system requirements. The benefit is to avoid starting with technical solutions that need to fit into a context.

Requirements Hierarchy Methodology

High-Level	**Business Requirements**	**Why is the project needed?**
User-View	**User Requirements**	**What do stakeholders need the system to do?**
Detailed	**System Requirements**	**What does the system need to do?**

Adapted from Civil Registration and Vital Statistics Digitisation Handbook

© UNICEF/UN0711951/Dejongh

3. Assessing and selecting CRVS Digital Platforms

Success in a CRVS digitisation project depends on more than just the technology employed. It is crucial to understand a country's opportunities and limitations in supporting a digital CRVS system before selecting appropriate technologies. Even if the pilot is at a sub-national level, the full country context generally should be considered so there is a path to scale.

Some key factors to be considered when assessing the feasibility of a CRVS digitisation project include:

- **Legal and regulatory framework.** The legal and regulatory framework must support the digitisation of CRVS systems. This includes laws and regulations related to data privacy, security, and confidentiality.
- **Governance structures.** Adequate governance structures must be in place to manage the implementation and maintenance of the digital CRVS system. This includes establishing roles and responsibilities for various stakeholders involved in the system.

- **Human resource capacity.** Sufficient human resource capacity must be available to implement and maintain the digital CRVS system. This includes having the necessary technical expertise, training, and capacity building for staff involved in the system.
- **Digital infrastructure.** The digital infrastructure must be sufficient to support the implementation of the digital CRVS system. This includes ensuring the necessary hardware, software, and network infrastructure.
- **User requirements.** The user requirements of the digital CRVS system must be understood and incorporated into the design of the system. This includes considering the needs of end-users such as civil registration officials, medical professionals, and the general public.

Understanding these opportunities and limitations enables the identification of suitable CRVS platforms that can be implemented in a digitisation project. This ensures that the technology chosen is relevant to the country's specific circumstances and increases the likelihood of the project's success.

Assessment of core functional and non-functional requirements in CRVS platform

Both functional and non-functional requirements are important to consider when selecting a CRVS digital platform, as they help ensure that the platform meets the needs of its users and provides a satisfactory experience.

Part of the requirements of a CRVS platform should be its configurability or customisability, unless it is built from scratch for a specific country. No two countries have the same legal, operational or procedural frameworks on the functional requirements.

Functional requirements refer to the specific features, capabilities, and functionalities that a CRVS digital platform is expected to provide in order to be considered effective and useful to its users. These include features such as data entry and retrieval, reporting, user authentication and authorization, integration with other systems, etc.

Checklist of CRVS platform functional requirements to fulfil CRVS milestones:

- ☐ Notification
- ☐ Declaration
- ☐ Validation
- ☐ Registration
- ☐ Corrections and Amendments
- ☐ Certification
- ☐ Archiving
- ☐ Sharing data
- ☐ Performance monitoring

Non-functional requirements define the quality attributes and performance characteristics of the CRVS digital platform. These are features of the platform that relate to how it is built, rather than whether the system covers all the "functional" steps involved in civil vital statistics registration.

Checklist of CRVS platform non-functional requirements:

- ☐ **Interoperability.** E.g., supports data exchange using open standards with other systems using appropriate standards-based APIs for notifications, IDs, reporting, verification of input data.
- ☐ **Scalability.** E.g., prepared to grow in terms of users, processing (hardware and software systems), data input sources, data cleaning, analysis and reporting.
- ☐ **Portability.** Cross-device and operating system platform access
- ☐ **Performance.** Monitorability; Steady service levels maintain as load increases; max latency 5 seconds when connection via online workstation for data entry and search; offline data sync; ID generation linked to National ID; change log; person-centric data records.

- **Availability.** Maximum 12hrs downtime per year; online/offline access.
- **Traceability.** Track and record changes to data by system and users.
- **Usability.** Intuitive and attention-grabbing design; prompts; viewable headers, labels and any software control values on page.
- **Flexibility.** Extensibility and configurability options; dynamic forms that can be edited with ease.
- **Archiving.** Capacity to archive all documents and legacy records permanently.
- **Data extraction.** Ability to extract/import non-personally identifiable information from the system in a non-proprietary format.
- **Messaging.** Capability to send automated messages to clients with reference numbers.
- **Data.** Quality checks; format support of date, time, currency, number; disaggregation by age, sex, location; registration by time frames; UN recommended core data items; interactive dashboard
- **Audit.** Logging of all activities and changes; permanent archiving; search logging; critical database tables changes logging.
- **Authentication.** Role-based authentication required to access the system.
- **Location.** Record of registration centres, unique IDs, location and geo-codes.
- **Language.** Multi-language support.
- **Security.** Unlimited roles, access levels; end-to-end data encryption; secure login and authentication; Two-factor authentication (2FA); role-based permission; no record deletion; data encryption plan; Multi-factor authentication (MFA); password storage; hardening standards; encryption of data at rest and in-transit; threat model; verification of secure components; generalized API developed with security best practices.
- **Backup.** Automated backup and restore functionality via backup server.
- **Error handling.** Comprehensive error handling regime; critical errors emailed.
- **Learning.** Self-service training for users embedded within product.

Checklist of CRVS digital public good non-functional requirements

- System is interoperable i.e., supports data exchange to and from other systems using appropriate standards-based APIs. Example systems include health information systems and identity management systems.
- Source code is licensed under an Open-Source Initiative approved license and is available on a publicly accessible repository.
- Documentation exists covering deployments, use cases, and functional requirements.
- System is designed to ensure privacy and security of data collected and stored.
- System is designed and developed to align with the standards, best practices, and principles as defined by the Principles for Digital Development.

Software maturity model

A maturity model can be a useful tool for organizations when selecting a solution. It provides a framework for assessing the capabilities and readiness of a particular option. A maturity model typically includes a set of defined levels or stages, each representing a progressively higher level of capability or maturity in each area, providing insights into the solution's strengths and weaknesses.

The use of a maturity model when selecting a CRVS digital platform facilitates well-informed decisions about the most suitable solutions for project requirements.

CRVS platform maturity categories

Global utility	Country support	Software maturity	Human resources
Scalability Country utilization Community governance CRVS business requirements Licensing and source code accessibility Open source Total cost of ownership Funding revenue and business model Ownership	Governance & leadership User documentation Software productization Network of solution providers	Adherence to best practices for digital development Adherence to privacy and applicable laws Security and privacy Interoperability & data standards Multi-lingual support Software roadmap	Capacity for solution maintenance & support Capacity building

Deployment at scale

Scaling up a CRVS digital platform deployment requires careful planning and consideration of various factors, including:

- **Business objectives.** Ensure that CRVS digital platform implementation aligns with the country's long-term CRVS goals, strategy and expected outcomes.
- **Technology.** Evaluate the current technology infrastructure and identify any gaps or limitations that need to be addressed before scaling up. The underlying infrastructure, software, and processes should be able to handle increased volumes of data, users, and transactions without a loss in performance or reliability.
- **Resources.** Budget for the resources required to scale up the project, including human resources, budget, and technology investments to support the increased scale of the project.
- **Stakeholders.** Identify and engage with all stakeholders. Communicate the goals and benefits of the project and seek feedback to improve the project.
- **Process.** Identify the processes that will be impacted by the CRVS digitisation and determine how they need to be adjusted or modified to support the increased scale. Ensure that the processes are designed to be efficient, effective, and scalable.
- **Data.** Determine the data requirements for the project and how it will be collected, analysed, and used. Ensure that the data is accurate, reliable, and secure.
- **Risk management.** Identify the potential risks associated with scaling up the project and develop a management plan to mitigate those risks.
- **Governance.** Establish governance processes and structures to ensure that the project is effectively managed and monitored. This includes establishing clear roles and responsibilities, decision-making processes, and metrics to measure success.

Assessing total cost of ownership

While making the choice of the solution to procure, it is important to consider the Total Cost of Ownership (TCO), which extends well beyond the initial costs of setting up the CRVS digital platform selected.

Estimating the TCO involves considering all of the costs associated with the project over its entire lifecycle. This includes both direct and indirect costs. A direct cost is a specific expense that is just for the CRVS project, such as a software license. An indirect cost includes the more general resources that must be pulled to make the project work, such as IT staff time. TCO will examine hardware and software expenses, implementation and integration costs, maintenance and support costs, and any ongoing operational expenses.

It is important to note that the cost of implementing CRVS systems is highly dependent on the technological infrastructure of the country and the extent to which the CRVS process mapping has been completed. Consideration of the different scenarios that a country might face when embarking on a CRVS system is key to understanding how the cost structure will vary. This includes, for instance, accounting for the cost of establishing a CRVS system in a country without an IT unit in the CRVS authority, versus in a country with an existing national IT agency.

Additionally, it is necessary to factor in the time and resources required to complete the CRVS process mapping, which can take up to two years in practice. In sum, there is a need for an appropriate TCO estimation model to be developed for each country's unique scenario in order to ensure the most effective implementation of a CRVS system.

Steps to estimate TCO

1. **Define the scope of the project.** Define the project's goals and objectives, and identify the specific technologies and systems that will be impacted by the project.
2. **Identify the direct costs.** Identify the costs associated with acquiring and implementing the necessary hardware and software, as well as any professional services required for implementation and integration.
3. **Estimate the indirect costs.** Consider any additional costs associated with the project, such as training and support for staff, ongoing maintenance and upgrades, and any operational expenses that will be required to support the new system.
4. **Calculate the total cost.** Add together all of the direct and indirect costs to estimate the total cost of ownership for the project.
5. **Consider the return on investment.** Compare the estimated TCO to the expected benefits of the project, such as increased efficiency, improved CRVS processes and cost.
6. **Review and update regularly.** TCO estimates may shift over time due to changes in the project scope or unexpected costs, so it is important to review and update the estimate regularly throughout the project lifecycle.

OpenCRVS, one of the platforms reviewed in this landscape assessment, has produced a tool to support TCO planning.

© UNICEF/UN0753050/Dejongh

4. CRVS Digital Platforms

UNICEF has conducted an assessment and landscape analysis of a select set of existing digital CRVS solutions. This involved a methodology that defines and assesses CRVS solutions against core requirements. The core requirements were identified within the scope of a landscape analysis, based on wide consultations including UNICEF country offices that have experience in the subject. The data that has been collected from the short-listed Solution Providers is self reported.

Methodology Overview

The CRVS Digital Solutions Landscape Analysis undertook a structured inquiry comprised of 5 core steps.

Step 1: Identify available CRVS digital solutions via a mapping exercise

- Review a subset of actual CRVS implementations via surveys
- 15 potential CRVS platform solutions identified via landscape mapping
- 5 solutions both completed fully the assessment process and were designated as viable

Step 2: Measure level of compliance against core requirements (self – reported)

- Questionnaire containing 110 Core Requirements (42 functional and 68 non-functional) to achieve 10 CRVS milestones.
- Information collected about on- and offline availability and dependency on other solutions.

Step 3: Observe live demos of the shortlisted solutions to validate the responses to the core requirement questions in Step 2

- The assessment tool was a demo-script with 11 Use Cases covering all the key activities of a CRVS digital solution.

Step 4: Measure the maturity of the shortlisted solutions against the globally defined DPG standards

- Maturity Model questionnaire covering 22 Questions classified under 4 Categories. All responses self-reported.
- Categories: Global Utility; Country Support; Software Maturity; Human Resources. (See section above, “Software maturity model.”)

Step 5: Synthesize findings to arrive at a weighted analysis of CRVS solutions

- Analysis based upon combined, comparative weighted scores for every requirement

Also, under consideration in the analysis was whether the CRVS solution is a Digital Public Good (DPG), or has high potential to become a DPG. The Digital Public goods Alliance (DPGA) defines Digital Public Goods (DPG) as "open-source software, open data, open AI models, open standards, and open content that adhere to privacy and other applicable best practices, do no harm by design and are of high relevance for attainment of the United Nations 2030 **Sustainable Development Goals** (SDGs)." Of the platforms reviewed here, DHIS2 and OpenCRVS are DPGs. DGIT, EveLIN, and HERA are proprietary, although DGIT shares its code with its partner governments.

CRVS Platforms listed in this section were those that provided sufficient data in response to UNICEF assessments, based on criteria as outlined in the previous section. They also fulfil most, and sometimes all, of the requirements of a Digital Public Good. For a full list of Core Functional and Non-Functional requirements assessed, please see the Appendices at end of this document.

From a compliance perspective, all platforms below work out-of-box to support a majority of functional and technical (non-functional) requirements of a CRVS digital system. Each platform can also be configured within certain parameters to meet specific programme needs. Configuration level of effort ranges from light to medium depending on the type of functionality required.

Below is a summary of key findings:

- The eCVRS market is fragmented with no clearly recommended solution. No solution has reached multi-country adoption.
- The Total Cost of Ownership (TCO) varied widely, between US$270,000 and US$61.5 million. The variance is largely due to some solution providers not considering all required cost drivers.
- Implementation of interoperability or data standards between eCRVS and other solutions like Health and Identity is inconsistent.
- Security considerations, such as encryption and decryption of data is not consistently implemented across most solutions and the use of globally recognized benchmarks such as CIS is not applied.

DGIT

Overview

Digital Governance Innovation and Transformation (DGIT) is an integrated CRVS and national ID platform built by UNDP. DGIT can be white-labelled (UNDP marking removed and replaced with government agencies) and customised for each government.

DGIT is available under special licensing. While not open source in the traditional way, beneficiary governments receive and own the full source code of their customised version. Furthermore, UNDP provides capacity building to local technical staff to support the continuous evolution of the solution.

Technical Analysis

Strengths	Weaknesses
Developed as a generic CRVS and national identity integrated solution Can undertake all day-to-day functions in both online and offline mode Adheres to 8 out of 9 Principles of Digital Development Fully implemented in two LMICs and currently being rolled out in a third LMIC. Implementation budgets are available in public domain. Already aligned to the **UNLIA model** as an integrated CRVS and ID management solution Not available off the shelf, but can be customised in partnership with governments Full source code is handed over to the beneficiary government and can also be made publicly available.	Does not provide a traditional open license and source code is not available in open repositories. Rather, UNDP provides an MIT license. Does not use FHIR for interoperability. However, APIs are developed as required. OpenAPI, OIDC, OAuth2 and others are available; the latter two are the dominant interoperability standards today for e-identification and authorization.

Country deployments:

Operational: Malawi, Nepal (for national ID project).

In production or pilot finished: Honduras, Guinea Bissau, Vanuatu, Trinidad and Tobago.

DHIS2

Overview

First released in 1996, DHIS2 is a robust, open-source web-based platform for data collection, management, and analysis. DHIS2 is the world's largest Health Management Information System (HMIS) platform. 3.2 billion people (40% of the world's population) live in countries where DHIS2 is used as a Health Information Management System.

Technical Analysis

Strengths	Weaknesses
Well-grounded solution and widely used in health sectors in many LMICs, including sending notification of vital events from health facilities to external CRVS systems Comes with open license and provides source code freely Can function in both offline and online mode Adheres to all the Principles of Digital Development Supports interoperability through fast health information resource (FHIR) data standards and other integration tools. Reported lowest Total Cost of Ownership (TOC) among all solution providers Transferring ownership to a government can be done without much upfront capital investment	Lower levels of compliance with functional core requirements, particularly around registration and validation Is yet to evolve as a core CRVS software, although has been tried out in a limited way in Liberia

Country deployments: Liberia (in progress).

Considerations

For DHIS2 to comply as a DPG for CRVS, the University of Oslo should be engaged to standardise the CRVS processes and develop a core CRVS package that can be launched in the public domain.

DHIS2 has an operational advantage in countries where the Ministry of Health is using the software already and also has responsibility for Birth Registration.

The CRVS package should be built as a standalone software for more seamless promotion and implementation in a CR environment. Time and financial resources would be needed for supporting the development of an end-to-end CRVS functions on DHIS2.

EveLIN

Overview

EveLin is a proprietary, packaged product developed by Digitech to meet the demand for vital records and statistics management software.

A French civil registry software, Digitech has adapted its products to the international market. The EveLIN is a software suite fully dedicated to the CRVS market.

Technical Analysis

Strengths	Weaknesses
High level of compliance with both functional and non-functional core requirements High state of readiness for carrying out day to day functions of registration Supports a number of data standards including FHIR for interoperability Deployed in France in over 100 cities with population from 50000 to 2 million inhabitants and in the Overseas Territories (New Caledonia) Solution available in different business arrangements: • Buying a product with a standard licence; benefit of product & service upgrade through an MCO contract • Buying a turnkey solution fully developed and own the source code • Co-develop the solution, own the source code, and build capacity to be autonomous Offline and Online versions available and in operation Capability to collect birth registration and process with central system in area without networks with 2G/GSM process	Almost all the core requirements, including entry of civil registration data, are reported to be available only online Open license is not currently provided, as source code is not available in open repositories Currently works only online

Country deployments:
Countrywide Operational: Ivory Coast, Niger, Mali, Republic of Congo, France.
Countrywide deployment, ongoing implementation: Senegal, Tunisia.

OpenCRVS

Overview

OpenCRVS is an open-source, standards-based software for civil registration that is designed to work in low resource settings. OpenCRVS is a DPG.

Technical Analysis

Strengths	Weaknesses
High level of compliance with core requirements 84% of the mandatory core requirements available 'Out of the box' signifying very high state of readiness All the basic registration functions are available 'Out of the Box' and most of them can work in both offline and online modes Open-source license made available and source code is publicly available Supports data standards including FHIR for interoperability Very high level of security features Adheres to all the Principles of Digital Development	Covers birth and death registration. Marriage and divorce registration modules will be available in release 1.3, planned for May 2023. Adoption will be available in 2024 based on demand for country implementation. Relatively new platform without large scale implementation references.

Country deployments:

Pilots and field tests: Bangladesh, Niue, Nigeria, Cameroon.

Considerations

OpenCRVS recommends a variety of implementation modes, including a Proof of Concept, which is a low-cost and low-risk way to understand the applicability of the solution in a country context.

WCC (HERA)

Overview

HERA is a proprietary CRVS solution to enable registration of vital events such as birth, death and marriage. HERA is delivered ready to use, pre-configured to meet international best practices and country-specific requirements.

HERA integrates with other systems like Population Registries, Biometric Systems, or Functional Registers (such as voter rolls, national ID systems, residency systems). In addition, it supports the OSIA (Open Standards Identity API) Initiative for civil identity systems, as recommended by the Secure Identity Alliance.

Strengths	Weaknesses
Functions of registration can be undertaken in both offline and online mode Modules can be all implemented at once, or one at a time, starting with the birth registration module Cloud-based or on-premise implementation is possible It supports the OSIA for interoperability with DHIS2 system and for integration of FIHR data Willing to deliver the source code on demand Currently implemented in one LMIC, and is in the initial stage of implementation in another Data is encrypted in transit and in storage	Open license not provided; source code is not available in open repositories

Country deployments: Gambia, Laos.

© UNICEF/UN0715845/Wenga

5. What next?

Recommendations

When considering procuring a CRVS digital platform, it is generally advisable to choose a platform that is already available and has been thoroughly tested by other CRVS projects. By doing so, there is a higher likelihood that the platform is mature and has been refined through previous implementations, resulting in a more stable and reliable product.

In contrast, unproven software can come with a higher risk of encountering technical issues or unanticipated challenges. Therefore, adopting an already established platform can help minimise these risks, while allowing for a faster implementation of the digitisation process.

Sometimes the implementer is the software provider. In other cases, it will be a third-party IT services firm. In that case, it is also advisable to select an implementing IT services partner/supplier that has expertise in the CRVS domain and with previous implementations. Selecting a supplier who is led by business process improvement and uses the digital CRVS solution to enable effective service delivery will result in better outcomes than a solution-driven approach.

Finally, when selecting a CRVS solution, it is important to consider whether the solution is or soon will be a DPG. DPGs have some advantages and disadvantages and several contextual factors, including donor preference would have to be taken into account before deployment.

Benefits of selecting an implementing partner/supplier with relevant CRVS expertise

- Increase the likelihood that the CRVS platform will meet the project's specific requirements and desired outcomes
- Gain more effective support and guidance during the project, given the supplier's familiarity with the domain. This can be crucial in ensuring that the project is completed successfully, on time, and within budget.
- Minimise potential risks associated with the development and implementation of a CRVS platform, as the supplier would have already encountered and addressed common challenges and issues. This can mitigate risks and promote a smoother implementation process.

In summary, opting for an experienced implementing partner to roll out a proven CRVS digital platform can yield significant benefits, ultimately leading to a more successful and cost-efficient project delivery.

CRVS RFP example deliverables

Deliverable / Activity
1. Inception Report. Detailed planning document specifying how each activity will be executed. This will include a comprehensive work plan.
2. Functional & Technical Design Documentation. Detailed design documents for the digital CRVS system, including details of how the application architecture promotes a flexible, scalable, secure and cost-effective development approach.
3. Prototype. Working prototype that demonstrates required functionality that can be field tested by end-users.
4. Hardware and Operating System Requirements. Clearly defined hardware and operating system requirements needed to support the digital CRVS system.
5. System Integration. Integration software that allows the integration of the digital CRVS system with XXX, as per the defined requirements.
6. Application & Integration Testing Plan. Detailed plan for all system testing including component, application, integration and user acceptance testing (UAT).
7. Application & Integration Test Scripts. Comprehensive test scripts that will be used to test the digital CRVS system in isolation and with other systems.
8. Application & Integration Testing & Report. • Conduct component, application and integration tests (including test environment setup) • Support UAT (lab and field). • Detailed write up of the outcomes of all tests, including resolution plans for outstanding bugs/ issues and fulfilment of acceptance criteria.
9. User training. Insert description of required training, to which audience etc.
10. User Manual. Comprehensive and easy to read user manual in English and [OTHER LANGUAGES] including screenshots
11. System documentation. Comprehensive technical documentation including: • Coverage: Code that is and is not documented is easily identifiable. • Accuracy: The code comments accurately describe the code reflecting the last set of source code changes. • Clarity: The system documentation describes what the code does and why it is written that way. • Maintainability: A single source is maintained to handle multiple output formats, product variants, localization or translation. • Synchronization: The code and documentation are linked to keep them in sync. • Completeness: All elements of the application are included in documentation.

Deliverable / Activity
12. Field Pilot & Report ([insert location and # of users]). **Period of Limited Deployment in order to Field Test the Solution.** • Deployment of all application components to the live environment. • Monitor the end-to-end registration process with users in their natural environment and modify application components as required. • All application component modifications must be documented a final report.
13. Deployment & Report ([insert location and # of users]). **Deployment period when solution is rolled out at maximum capacity.** • Deployment of all application components to the live environment. • Monitor the end-to-end registration process with users in their natural environment and modify application components as required. • All application component modifications must be documented a final report.
14. Support and maintenance. Insert length and type of support and maintenance support required.

Source: CRVS Digitisation Toolbox

Conclusion

Choosing a CRVS digital solution best suited to a country's deployment context is a complex decision. This summary of findings aims to help streamline this process and to suggest the key questions to answer throughout the process.

For additional information, please contact UNICEF at the details below for updates to this publication, and/or for technical advice.

- **Child Protection** - Programme Group at **childprotection@unicef.org**
- **Digital Centre of Excellence** - Information and Communication Technology Division at **dcoe@unicef.org**

© UNICEF/UN0711980/Dejongh

Appendices

Core functional requirements assessed

Administrative

- The system must be able to create, edit, delete system user
- The system must be able to define, assign and revoke system permissions for user(s)
- The system must allow task management feature for users, such as grouping applications by completion/pending status
- The system must support various processes at the local registration office (entry of forms, manage approvals, identify gaps, etc.)
- The system must allow user management (create, update and deactivate system users and assign permissions from those users)

Alerts

- The users are alerted on notifications, declarations received
- The system must be able to automatically detection and alert on duplicate records and provide options for merging or removal of records

Amendment

- The system should allow changing/editing of records name change/correction, address change/correction, based on necessary documentation

Certification

- The system should allow internal process for submission and approvals
- The system must be able to generate QR codes to verify legitimacy of the certificates
- The system must allow users to print paper forms and certificates for clients

Client features

- Clients must be able to create and submit declaration form remotely using a client portal
- The system must allow clients to upload documents and certificates or link online documents
- The system must allow clients to track their application status
- The system allows scheduling client appointments
- The system should allow download printing or re-printing of documents and certificates from a remote location

Data

- The system must allow generation of data quality, timeliness, error reports
- The system must be able to generate reports of cases of birth registered, completeness, certification, etc.

- The system must allow users to submit data for reporting purposes based on defined parameters
- The system must be able to analyze monitoring indicators such as number of registrations, issue of certificates by geographical locations, etc.
- Reports to have 2 configurable parameters entered by the user (period of time and area of catchment)
- Reports to be prepared in multiple formats, including CSV, JSON, PDF, and others as applicable

Data Sharing

- The system must allow users to create data sharing request with other entities

Messaging

- The user must be able to send customized messages to clients regarding notifications, confirmations, etc.

Registration

- The users must be able to create and submit a new registration
- On completion of validation steps, the system must prompt the user to verify all registration form information through a pop-up box
- The pop-up box that prompts the user to verify all registration form information must allow the user to “Save”, “Draft” or “Edit” the birth registration form
- The users must be able to accept e-signatures from clients
- The system is able to conduct biometrics authentication and link with client records
- The users must be able to complete notification, declaration, registration, amendment and other forms
- The system must be able to auto-generate and assign unique ID (alpha, numeric) automatically on certificates
- The system must provide prompts and alerts based according to protocol

Searchability

- The user must be able to search records based on smart fuzzy search and defined fields, such as, ID number, name, etc.

System monitoring

- The system must allow users to define performance management/operational reporting, monitoring report content. For e.g., timeliness and quality, completeness, certification, etc.
- The system must allow users to view performance management/operational reporting, monitoring report(s)
- The system must allow users to export performance management/operational reporting, monitoring report(s)
- The system must be able to generate reports on system performance and downtime, etc.

Validation

- The system must be able to validate submitted documents as proof using QR codes, bar codes, holograms, picture/selfie matching photo IDs, valid date of documents, etc
- If the system identifies errors validation with notification, declaration data for consistency, completeness, errors. The system must prompt the user to update specific fields
- The system must allow to accept or reject messages (eg notification/declaration from other sources) based on automated validation or user action for corrective action
- The system must allow registration agents to raise corner cases via the system so they can be logged and tracked to resolution
- The system must be able to validate submitted data against same items of information in accompanying documents

Core non-functional requirements assessed

Archiving

- The system must be able to archive all documents, including legacy birth and death records permanently

Audit

- The system must log all activities, changes, amendments by user, place and time.
- The system will keep the log of all changes for at least 6 months, and then archive it.
- No user can change the log of changes, not even the System Administrator.
- The system should log all the searches performed by the user and the individual data accessed / viewed by the user. The logged information should include the user ID, machine ID, timestamp and respective information (search criteria, etc.)
- All changes (including inserts and updates) to critical database tables are to be written to an audit table, recording the user initiating the change, the time and date of the change, and the before and after values.

Authentication

- The system must require each user to authenticate by role before gaining access to the system

Availability

- The system must not exceed 12 hours downtime per year.
- The system must allow users to work online and offline. If offline, data should be synchronized when an internet connection is available

Backup

- The system should provide automated backup and restore functionality via the backup server. Automated backup routines shall be run in non-peak periods on a regular basis

Data

- The system must be able to perform data quality checks, including, consistency, completeness and validation
- The system must be able to support a range of different formats for date, time, currency, number, etc.
- The system must allow capture and analysis of disaggregated data, specially by age, sex and location.
- The system must capture registration by timeframes (on-time, late and delayed)
- The system must be able to capture the UN recommended core data items
- The system must provide an interactive dashboard that supports registration managers to understand the performance of their system and staff, and subsequently identify low and high performing areas so they can respond accordingly

Data extraction

- The software must allow a mechanism for extracting or importing non-personally identifiable information (PII) from the system in a non-proprietary format.

Error handling

- All written software to be subject to a comprehensive error handling regime
- Error and warning messages should be informative and identify the error as completely as possible (e.g., identify the module, the procedure or functions, the identifier of the error, etc.)
- All error and warning messages shall be written into the system logs
- Critical error shall be emailed to all relevant software support personnel

Flexibility

- The system must support extensibility and/or the ability to accept new services or functionality
- Allow for flexible configurations based on the user environment
- The system must be easy to configure e.g., the form is dynamic, and fields can be added and removed and edited with ease

Interoperability

- The system must be able to support standards-based data exchange (sending and receiving notifications, unique IDs with National IDs, etc.) in CSV, JSON and xml formats, including USSD and SMS based.
- The system must be able to interface with open source or existing third-party reporting tools including USSD code
- The system must provide the capability for integration with other systems through an API, such as National ID systems, health information systems, etc.
- The system must use open standards to promote interoperability
- The system must be able to exchange data between systems ensuring semantic interoperability

- The system must be able to conduct verification of input data with 3rd party sources

Language

- The System must be able to provide multi-language support

Learning

- Allows training to be provided through the product, minimizing the need for in-person training and providing flexibility to training approaches and the release of new features.

Location

- The system must maintain a record of all registration centers with their unique IDs, location and geo-codes

Messaging

- The system must be able to send automated messages to clients regarding notifications, confirmations of submissions, when to travel to office to collect certificates etc. with reference numbers

Performance

- The system must be able to perform as load (users and transactions) increase following microservice design.
- The system transaction response to user data entry should be minimum 2 seconds (turn round time) and maximum 5 seconds (turn round time) on an online workstation
- The system must allow users to monitor system availability and performance
- The system can sync data with the main server (in case of offline use)
- The system can auto generate global unique IDs (GUID) (alpha, numeric), linked to a national ID
- The system must track and record all changes (update/add/delete) to the data by system and by users
- The solution must create person centric records and ability to search and view vital events of a person
- The system transaction response to user search should be minimum 2 seconds (turn round time) and maximum 5 seconds (turn round time) on an online workstation

Portability

- The system should be accessible from any computer device: personal computer, laptop, tablet, smartphones.
- The system should be accessible from any operating system.

Searchability

- The system should allow searching records based on defined fields, such as, ID number, name, birth, death, marriage etc.

Scalability

- The system must be designed in order to be prepared to grow, both in the number of users/accesses, data processor, data analytics, visualizations and reports.
- The system must be designed in order to be prepared to include data from different sources than the listed in the functional requirements
- The system's technical design (hardware, databases, etc.) must be able to scale to support projected transaction volumes over time
- The system must be able to identify duplicate records and deduplicate them

Searchability

- The system should allow searching records based on defined fields, such as, ID number, name, birth, death, marriage etc.

Security

- The system must support unlimited roles and access levels related to viewing, data entry, editing, deleting, reporting and auditing by field agents, registration officers, registrars, individual clients, etc.
- The system must be able to encrypt data end-to-end including storage
- The system must be able to encrypt and decrypt outgoing and incoming messages
- The system should allow role-based permissions to access data. Especially related to access and visibility to Personal identifiable information.
- The system must provide secure login and authentication, including 2FA. In case of password reset, a link should be sent to registered email
- The system must support generation of unique PIN for users to easy lock and unlock
- The deletion of records in the CRVS database is strictly forbidden. The records can be flagged or marked but they are not allowed to be deleted.
- All changes (including inserts and updates) to critical database tables are to be written to an audit table, recording the user initiating the change, the time and date of the change, and the before and after values.
- The solution provider should propose an MFA (Multi Factor Authentication) scheme that can use one or more of the following: Client certificate authentication; Token generation (e.g., push-based authentication; OTP; or email verification, physical token, etc.)
- The solution provider should propose a suitable scheme of secure storage of passwords in such a way that prevents them from being obtained by an attacker even if the application or database is compromised. The proposed scheme should use modern hashing algorithms (e.g., SHA-256, SHA-3, or stronger), and should be in combination with at least the salting technique. The Solution Provider is free to propose additional layers of security like pepper and work factors (number of iterations).
- The solution provider should utilize existing hardening standards such as the Centre for Internet Security (CIS) benchmarks or equivalent. These hardening

standards should be used for all hypervisors, operating systems, web servers, database servers, network devices and other components of the solution.

- The solution provider should ensure that key controls are in place to facilitate encryption of data at rest and in-transit. The same controls should be in place for the data stored locally in the offline workstations. A data encryption plan should be included in their proposal that aligns with current global best practices. In addition, the solution provider should develop “a threat model” where all the possible threats are defined, distinguished and treated with priorities.
- The solution provider needs to demonstrate that their supply chain has robust controls to address specific threats to the integrity of hardware and software products throughout the product life cycle. The end goal is to provide a product that has been designed, developed, and delivered with integrated security at every phase of the product life cycle. All the components used (open-source libraries or third-party dependencies) that will be used in the proposed CRVS solution should be verified as secure. While compliance is not required, ISO 20243 can be used as a reference point with regards to the required control framework
- The solution provider shall provide a generalized API that is developed based on security best practices (e.g., OWASP Top 10 or equivalent), including key considerations for encryption, authentication, authorization, data validation, audit logging, quotas/throttling, data validation, audit logging, API gateways, etc.

Traceability

- The system must track and record all changes (update/add/delete) to the data by system and by users

Usability

- The use of the tool should be easy and intuitive in order to reach users with different levels of computer use experience.
- The system should be able to capture the user’s attention and motivate them to interact with it, exploring and benefiting from all its features.
- The system should be able to generate prompts for users on actions or document verifications
- The system must provide the option on every page of CRVS system to view the headings, menus, labels, and any software control values on any page

UNICEF works in the world’s toughest places to reach the most disadvantaged children and adolescents – and to protect the rights of every child, everywhere. Across more than 190 countries and territories, we do whatever it takes to help children survive, thrive and fulfill their potential, from early childhood through adolescence. And we never give up.

Graphic design: Mireia Pérez Carretero

© UNICEF/UN0594636/Dejongh