# Practitioners Guide for Digital CRVS Systems:

## Principles, functional requirements, licensing, service and hosting options and considerations for procurement of Digital CRVS systems

### Draft of version 4

15/11/2023

## Contents

;

# Introduction

The management of Civil registration and vital statistics systems (CRVS) is an essential function of governments. By recording vital events, such as births and deaths in a country and issuing legal documents pertaining to these events, citizens and residents gain access to basic rights and services. Civil registration records and the resultant vital statistics enable governments and private sector to develop effective public policies and programmes and to streamline governance processes.

Information technology (IT) is critical to realising well-functioning and inclusive CRVS systems. Digital solutions can enhance the key functionalities of a civil registration system which is to collect, store, retrieve data, transmit, protect and manage vital event data within defined jurisdiction. Implementing a digital solution can make CRVS processes simpler, efficient, economical, accessible, and transparent. At the same time, if the digital solution is not well-designed to align to key recommended principles and key features of operations (including those outlined by the UN), it can obstruct the performance of a CRVS system, create risks to individuals concerning privacy of their personal data, therefore infringing on individual's fundamental rights, and even have a detrimental impact on a country's governance processes.

## Human Rights and digitalisation

The digitalisation of CRVS systems can positively impact human rights. Digitalisation has the potential to improve access and efficiency of civil registration services and products, hence enhancing the government's capacity to ensure the right to a name and nationality[1] and other related rights are realised by individuals. However, it is crucial to emphasize that digitalization should not be an end in itself. A person-centered approach must be adopted to ensure that individuals' and families' needs and rights are at the core of CRVS digitalisation design.

;.

[1] Civil registration doesn't confer nationality. Civil registration records and documents provide important biographic information, needed to proof nationality.

Since data sharing and interoperability are critical for enhancing  CRVS processes, privacy and data protection regulations should be strengthened to ensure that CRVS systems digitalization is fully aligned with human rights principles.

## The concept of digitalisation

The present guide assumes the concept of digitalisation as the use of digital technologies to the broader transformation of paper based CRVS systems by reengineering business processes, simplifying operations, providing on-line services and enhancing user's experiences. Digitalisation therefore goes beyond converting analog data into digital format.

On the other hand, digitisation is the practice of converting analog information existent in books and archives into digital form and databases, which can be stored, processed, and transmitted using digital technology. This process involves using digital devices and software to capture, store, and manipulate data.

As part of conceptualisation of your digitalisation project, it is essential to consider whether digital records will fully replace paper records. This is a legal question with enormous practical implications and must be considered. Introducing digital technology in Civil Registries doesn't necessarily mean that paper usage will be eliminated. The paper may still be necessary for specific procedures, particularly physical certificate issuance.

In advanced stages of digitalisation, the CRVS digital system should ensure the authenticity and integrity of digital records, for which a Public Key-Infrastructure (PKI) is necessary. With that, it is possible to adopt use of electronic signatures and digital certification.

### General guidance about CRVS digitalisation projects

Prior to initiating any digitalisation efforts or choosing a digital platform to adopt, a country should undertake a holistic assessment[2] of its CRVS systems to determine the extent to which the current system is achieving its objectives, including identifying any performance issues or bottlenecks in current registration processes. Conducting an assessment will help to identify strategic actions to undertake for further development of the system including the potential for use of technology.

Actions to address key bottlenecks such as weaknesses in legislation, organization, management and infrastructure issues, human resources, weak business processes etc., need to be prioritized prior to embarking on a digitalisation project. The digital solution should be viewed as a tool to facilitate and or enhance realization of the objectives of the CRVS improvement efforts rather than the solution itself. Digitalizing inefficient processes can result in further inefficiencies and wastage of resources. Thus, it is important that the digitalisation exercise be a component of the broader CRVS improvement exercise and be aligned to the vision and strategic objectives of the CRVS system as a whole.

## About this document

### Objectives and target audience

This document is developed to serve as a resource to country stakeholders including those that are involved in decision-making and local and international experts providing technical and policy guidance about designing or adopting of digital solutions to enhance CRVS Systems. Specifically, this document provides information on:

1. Principles for the design and implementation of digital CRVS systems, covered in section I;
2. Key functional and non-functional requirements of digital CRVS systems, covered in section II;

[2] Using the CRVS Systems Improvement Framework (https://getinthepicture.org/resource/crvs-systems-improvement-framework)

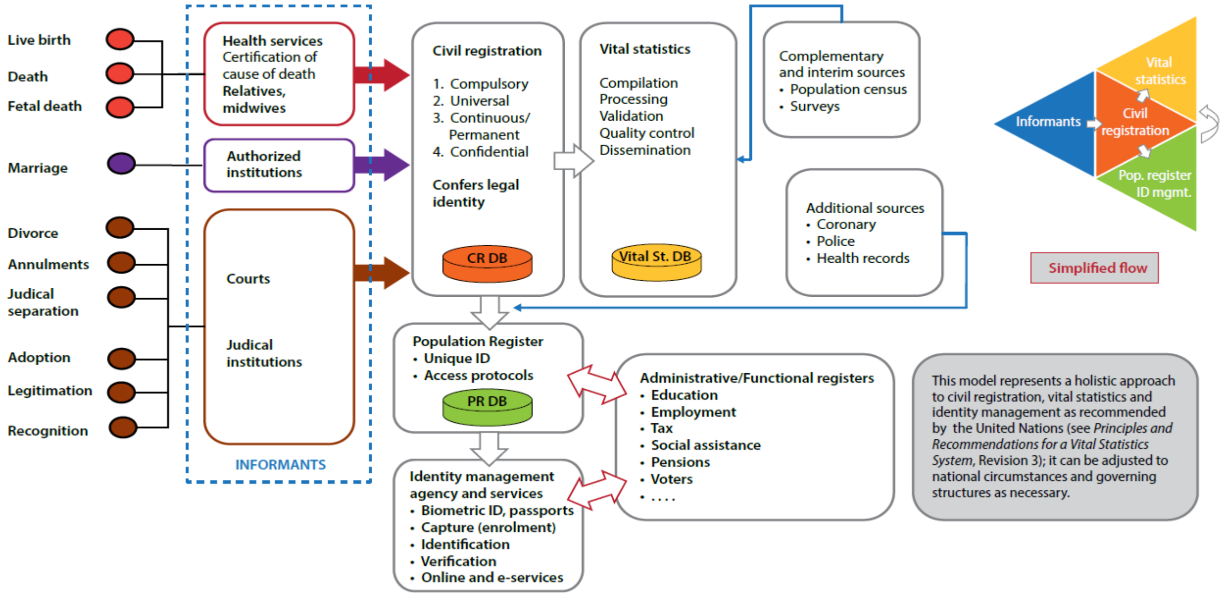
3. Options for licensing of digital CRVS systems and their benefits and risks, covered in section III;
4. Service and hosting options for digital CRVS systems and their benefits and risks, covered in section IV; and
5. Key considerations to make prior, during and when procuring digital CRVS systems, covered in section V.

This document complements and should be read and used alongside the APAI-CRVS digitalisation guidebook which provides comprehensive step-to-step and end-to end guidance on how to undertake a CRVS digitalisation project. Specifically, this document provides information to complement sections 7 & 8 of the APAI-CRVS digitalisation guidebook, which provide guidance on defining the target system architecture and defining system requirements respectively.

## Scope

While this document focuses on key principles for design and implementation of CRVS digital solutions, it is recognised that there are important linkages that CRVS systems should have with other IT platforms within the government e.g., the population register, health information system, voter registry, national identification (ID) system, among others. It is therefore essential that the IT solution adopted be highly interoperable and supports the UN integrated approach to health, civil registration, vital statistics, and identity management as demonstrated by Figure 1.

Figure 1
Model of a civil registration, vital statistics and identity management system



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

The overall goal of this resource is to support countries towards implementation of sustainable, reliable, stable, and secure IT systems for CRVS that facilitate the establishment, verification and authentication of legal identity in compliance with national legislation and international standards and the production of timely and reliable vital statistics.

# Section 1: Principles for design and implementation of Digital CRVS Systems

The principles of a system are the general rules and guidelines that inform and support its objectives. The guiding principles for the design and implementation of digital systems for CRVS are guidelines that support the optimal performance of the system, hence enabling it to achieve its fundamental purpose of universal registration of vital events and the production of vital statistics in line with United Nations principles, standards and recommendations as well as to serve other associated goals.

The 8 principles provided in this document (see Table 1) were initially developed by the member countries and territories of the Pacific Community (SPC) during the Pacific Regional Workshop on Legal Identity and Identity Security, held in July 2019 at SPC headquarters and revised by African member states and experts of the APAI-CRVS digitalisation group.

The principles can help guide countries to adopt robust governance practices and consistent technological design options in their engagement with IT system vendors and other relevant stakeholders.

The order in the list below does not imply relevance or hierarchy, the nature of the principles is being interdependent.

## #1 Principle – Compliance to national and international legal frameworks and standards

Description:

Implementation of digital CRVS system should comply with international principles and standards on CRVS, national legislation including any existing civil registration and IT acts, legislation or policy on privacy, security, data-sharing, auditing and digital government etc., and relevant international treaties.

Rationale:

All other principles and requirements are secondary to delivering a system that complies with international principles and standards on CRVS, specific legislative framework of the country, and relevant international treaties.

Implications:

Documentation on the design and procurement of CRVS IT systems should explicitly state how they will ensure compliance with existing legislation and standards, both nationally and internationally.

### #2 Principle – Sustainability

Description:

A CRVS IT system should be sustainable over the long-term in the following ways:

- technical (support staff to systematically maintain the system, since the IT system will need to be regularly updated and constantly improved);
- instructional (registry and technical support staff should maintain adequate knowledge to manage the IT system effectively);
- administrative (relevant, support contracts, service agreements should be in place for the life of the IT system); and,
- financial (funds should be secured to cover all costs associated with the IT system for its expected lifetime). To the extent possible, countries should adopt a long-term approach and aim to consider these factors as important drivers to sustainability.

It is imperative that a sustainability plan be developed alongside the development of the IT system. Such a plan should incorporate a knowledge-transfer component (and outline modalities for its operationalization) to ensure the country is in possession of all necessary knowledge, information and skills necessary to maintain the system.

Rationale:

A CRVS IT system is a long-term investment for a country. As such, it is imperative to put in place adequate mechanisms to ensure that the systems are sustained over their intended lifetime.

**Implications**:

The technical, instructional, administrative and financial sustainability of the solution (as well as the sustainability of any other areas crucial to its long-term operations) should be addressed explicitly during the planning, procurement, and design phases. Care should be taken when the implementation phase is complete and the system is handed over to be maintained as part of conventional operations. Adequate budgets must be assigned to provide for any maintenance and upgrades required over the expected lifetime of the IT system. In identifying or developing the digital solution of choice which enables sustainability, countries should refrain from disproportional front-loaded investments and rather adopt phase-based/incremental improvement approaches with sustained investments.

## #3 Principle – Cyber Security, Data Protection, and Privacy by design

**Description**:

CRVS IT systems should explicitly address cyber security, data protection, and privacy standards at all stages of the project lifecycle. Relevant considerations that should be made include user management (e.g., deactivation of user log-in after a specified number of unsuccessful login attempts, password expiration, log-in monitoring), backup systems, data encryption, disaster mitigation, management and recovery, among other best practices.

**Rationale**:

CRVS IT systems include significant amounts of personal data which make them attractive targets to malicious actors. Therefore, data security (including in the context of disasters), data protection and privacy are important considerations in the selection and/or design of any IT systems. Data protection standards should be embedded into the design, development process, and operations to build trust with users and stakeholders, reduce the risk of data breaches, and comply with privacy regulations more effectively. Securing the data that the IT systems hold from unauthorized disclosure or modification and respecting the privacy of the persons to whom the data pertains is critical to establishing and maintaining the trust of all stakeholders in the CRVS IT system.

Implications:

A formal risk assessment should be carried out as part of the IT system development. Security requirements should be identified at the same time as functional requirements and should be explicitly included in tender documentation. IT systems with strong cyber security, data protection, and privacy characteristics should be prioritized. The architects of CRVS IT systems should explicitly state how they will deliver on security requirements and which cybersecurity standards they conform to. Plans should be developed to keep the cyber security, data protection, and privacy measures of the CRVS IT system up-to-date for the lifetime of the system.

### #4 Principle – Interoperability and data-sharing

Description:

To harness the full potential of the legal identity data stored in the civil registry, IT systems should be able to share data with other governmental agencies within a country and regionally, as appropriate (based on the legal mandate).

While actual data-sharing will depend on the regulations and agreements of a particular country, the CRVS IT system should have the capability to facilitate secure and easy data-sharing (both automatically and manually) with other organisations entitled to that data. That capability should allow for easy configuration of the key restrictions attached to any data-sharing agreement (e.g., the ability to share only certain types of records). The definition of data standards in terms of data structure and semantics among the stakeholders in the CRVS system and within the CRVS IT system, are necessary to enable interoperability with key sectors such as health, education, social protection etc. Further, Application Programming Interfaces (API) are essential to provide secure interoperability with internal or external services for various clients.

Rationale:

Civil registration data is vital to the processes of private stakeholders (e.g., opening bank accounts, claiming insurance etc) and providers of government services (e.g., social protection, ID management, passports production, elections, health, education and vital statistics production). This capability becomes more important with the development of digital government (e-Government) services and the integration of civil registration as a fundamental component of digital public infrastructure. Data sharing between countries (e.g., to manage cross-border migration or to link events occurring in different countries) may also be a motivating factor to improve the performance of CRVS systems. Overall, interoperability ensures the breakdown of system silos and support for other functions of government to the expected standard.

Implications:

IT systems should support modern data-sharing protocols, and the ability to comply with data-sharing agreements if countries decide to share data internally and regionally. Data-sharing should be easily configurable by CRVS teams and require as little IT expertise as possible. CRVS systems should support multiple mechanisms of data exchange to allow for the differing capabilities of partner organisations or systems. Defining data standards and publicizing them is essential to interoperability. All data-sharing arrangements should be backed by technical documentation detailing who should be allowed to access the data as well as a robust data protection mechanism.

### #5 Principle – Appropriateness to country context

Description:

CRVS IT systems functional requirements should be customized to the country context and ideally not require a greater IT infrastructure, skill sets or capability for implementation or ongoing maintenance than can reasonably be supplied within a national context for the expected lifespan of the system. Where possible, it is strongly recommended[3] that countries adopt a gradual strategy for scale-up and develop ICT capacities within the CR organization's staff and other government institutions to ensure autonomy and avoid vendor lock-in for the expected lifespan of the system.

Rationale:

Countries may have few skilled IT personnel available within governments and in the private sector. In other cases, the number of staff may not be sufficient to handle the existing workload which can lead to significant difficulties in maintaining complex IT solutions over the lifetime of the system. In this regard, it is pertinent that the CRVS IT solution is appropriate to the national context. In addition, it is necessary to continually develop ICT capacities of staff to ensure sustainability in maintaining IT solutions over the lifetime of the system.

Implications:

The implementation of a CRVS IT system should include planning to address capability and knowledge gaps in a country. Countries may consider outsourcing or software-as-a-service (explained in section III) at least in the initial phase, with a longer-term plan to build local capacity on IT-related competencies (hosting, system design and data analytics configuration, etc.). Countries could consider local partnerships with

[3] Except for very small countries that do not have the possibility of maintaining their own team.

incubation hubs or universities (and other relevant institutions of knowledge development and learning) to address the capability gaps.

### #6 Principle – Design with and for the user

Description:

CRVS IT systems should be developed in close collaboration and with critical consideration of the needs of the direct and indirect users, beneficiaries, and overall stakeholders of the system. These include for example, personnel managing civil registration functions, front-line civil registrars, officials dealing with the production of vital statistics, members of the public, and users of civil registration records or data within other government ministries or departments as provided for under the law etc.

Rationale:

Different stakeholders of the CRVS IT system have differing user needs which should all be well documented and accounted for during the system's design.

Implications:

Conducting a thorough stakeholder and user needs analysis is pertinent and a priority for the digitalisation project. This information should be used to guide the design of the digital solution. Furthermore, it is crucial to exhaustively test your designs with users in every social and physical context to maximize their inclusion and adequate consideration of their specific needs. In all cases, the digital CRVS solution should respond to user needs.

### #7 Principle – Country data ownership

Description:

CRVS data should be owned by the country, and the IT system should adhere to the country's sovereignty.

Rationale:

Civil registration data is regarded as nationally significant for a variety of reasons, in particular for countries or other jurisdictions to exert their sovereignty, and the data often has significant cultural, historical and or monetary value.

Implications:

During procurement, country ownership of data should be explicit in any agreement or contract. Contracts should explain how and in what format countries can obtain their data in case a commercial arrangement with a vendor ends or the vendor ceases to operate. Jurisdictional questions about data should also be addressed explicitly in the case of cloud solutions or software-as-a-service. Contracts should state what vendors can access and which uses of the data (if any) vendors are permitted to have. Ideally, the source code should be available to the CRVS organization as well.

### #8 Principle – Adaptability

Description:

CRVS IT systems should be adaptable in their design to handle changes in CRVS processes and government priorities and to respond to ongoing technological changes. This includes allowing direct customization by the administrative user of general functionalities such as user management, reporting, graphic design, among others, without the need of demanding it as a new feature of the solution to the IT staff or the provider.

Rationale:

A CRVS IT system is a long-term investment for a country. As such, it should be able to handle the types of changes that can occur over its lifetime. In addition, the differences between countries are significant, any CRVS IT system that seeks to support multiple countries must take into account those differences.

### Implications:

During procurement or design, it should be made clear how the IT system can manage changes in requirements over the lifetime of the system. Systems that can incorporate change without expensive code modifications (e.g., through configuration) should be favoured.

## Section 2: Key functional and non-functional requirements of digital CRVS Systems

The UN has set out international guidelines and standards on CRVS systems,[4] including key features of CRVS systems, how the systems should be organized and managed to enable them to effectively perform their functions and yield the expected outputs. This chapter discusses key functional and non-functional requirements of digital solutions for CRVS in alignment with UN standards.[5] The functional and non-functional requirements are listed here in no particular order.

### Functional requirements of digital CRVS systems

Functional requirements relate to the operation and functionalities of the system to satisfy the usage requirements. Functional requirements refer to the specifications of the software's functions; i.e., what precisely the software must do (the software's goals). Without meeting these requirements, the CRVS system will not effectively perform its functions and therefore not yield its expected outputs. The requirements outlined align to the UN principles and standards for CRVS that form the basis of widely recognized good practice.

### #1 Functionality: Capacity to register all vital events

**Description:**

The UN outlines 10 vital events that should be registered compulsorily by a civil registration organisation: live births; deaths; foetal deaths; adoptions; legitimations; recognitions; judicial separations; marriages; civil partnerships; and divorces. Live

[4] https://unstats.un.org/unsd/demographic-social/crvs/index.%20cshtml#method

[5] A more comprehensive outline of functional and non-functional requirements for digital CRVS systems is available in UNICEF's publication: "CRVS Platforms: Key findings for practitioners." (https://unstats.un.org/legal-identity-agenda/documents/Paper/CRVS_Key%20Findings_for_Practitioners.pdf)

births, deaths, and foetal deaths are recognised as high priority events and, thus, recommended for priority civil registration by all countries. A CRVS IT system should have the capacity to register all vital events and enable the collection of cause of death information in accordance with international standards.

### Rationale:

While the civil registration law in a country may not require registration of all 10 vital events at the time of design or implementation, as the CRVS system and its related ecosystem evolve, the ability to register the other events should be anticipated. The CRVS IT system should therefore facilitate the inclusion of all events without requiring major structural adjustments or financial investments.

### Implications:

Irrespective of the vital events that a country currently registers, the CRVS IT system should be able to add other event types as needs arise. The functionality for registering these other events should be able to be "turned off" initially with the option to be activated when required.

## #2 Functionality: Inclusion of all CRVS milestones

**Description:** The digital system should facilitate the processing of all milestones of  a civil registration process including the production of vital statistics[6]. These milestones include,: notification; validation and verification; certification; information-sharing; storage and archiving; compilation of vital statistics; quality control of vital statistics; generation of vital statistics and dissemination of vital statistics.

### Rationale:

[6] Daniel Cobos, Carla Abouzhar and Don de Savigny (2018), The 'Ten CRVS Milestones' framework for understanding Civil Registration and Vital Statistics systems https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5873547/.

The full value of civil registration to a country is best realized when all CRVS milestones are captured. While the digital system may not in itself manage the processes for the compilation and generation of vital statistics, it facilitates their production and the necessary sharing of data for the National Statistics Office responsible for the production of the vital statistics report.

**Implications:**

The design of the CRVS IT system should facilitate automation of all milestones. Regarding notification and verification of vital events, adopting dual and separate sources of information/evidence (e.g. validation against the health sector data and ID system) is recommended to ensure the authenticity of the vital events.

### #3 Functionality: Linkage of related records (person-centricity)

**Description:**

CRVS IT systems should be person-centric: all vital events related to an individual (e.g., birth, death, divorce, marriage, etc.) should be linked. In addition, relationships between individuals should also be captured e.g. the individual's spouse for a marriage, parents for a birth, children, etc.).

**Rationale**

Being able to understand which records relate to a particular individual improves the ability of civil registrars to maintain the integrity and consistency of data, and it better supports modern uses of civil registration data such as in the development of a population register, supporting digital government processes etc.

**Implications:**

IT systems with person-centric approaches should be prioritized. Use of record numbers/ unique personal identifiers enable unique identification of individuals' records within the system and enable creation of persons profiles and linkage of related person records. In doing so, protocols for data confidentiality must be observed.

### #4 Functionality: Detection, merging, and removal of duplication records

**Description:**

The entry of more than one record for the same event should be automatically detected and the error removed. The removal of potential duplicate records requires a policy and key process guidelines.

**Rationale:**

CRVS systems face an inherent risk of including more than one record for the same event. This can happen due to fraud as well as unintentionally (e.g. when event registration is undertaken from different localities or at different points in time and/or when there is a slight alteration of the details of an event resulting in an event appearing as not previously registered). A well-designed matching function or feature or algorithm enables the database to be searched for any matching records and, if found, prompts for confirmation of the data.

**Implications:**

The CRVS IT solution should include standard rules and checks applied to each record accepted into the CRVS database in order to detect any duplicates (whether entered by external, third-party systems, by civil registration representatives in regional centres, or by staff at the central civil registration office). If a potential duplicate match is found, it should be brought to the attention of the relevant CRVS staff member and resolved appropriately.

### #5 Functionality: Querying and record searches

**Description:**

Users need to be able to search and retrieve records from the CRVS IT system, using a variety of parameters (e.g. single names, multiple names, diacritics, transliterations, previous names used, geographies, date ranges, etc.).

**Rationale:**

Searching for recent and historical records is a basic functionality of a CRVS IT system. Civil registration offices are often requested to facilitate a genealogical search of records by individuals, families, courts and researchers.

**Implications:**

The IT solution should enable effective and efficient searching of current and historical records, including corrections and amendments made. It is important to leverage name search algorithms that consider: phonetic matching; name language identification; typographic errors and misspellings; orthographic variations; initials matching; optional name tokens; etc. It should also enable easy retrieval of any associated supporting documents.

### #6 Functionality: Correction and amendment of records

**Description:**

Civil registration records should be able to be modified to reflect amendments to records and/or to record recent changes in the civil status of an individual.

**Rationale:**

Civil registration records are dynamic and may require correction and/ or changes (e.g., the addition of a father's information, new documents in cases of adoption, legal name changes, corrections of erroneous information and annotations on the records).

**Implications:**

The CRVS IT solution should have the capacity to facilitate the recording of corrections and amendments to civil registration records, without tampering with the original record. All amendments should be logged in the CRVS IT system with relevant metadata (e.g., information identifying who changed the record, when it was changed, and any supporting documents for the change as applicable).

### #7 Functionality: Certificate management

**Description:**

Users should be able to print all required certificates, based on defined templates. The system should keep records of all certificates printed and provide reliable means of verification of the certificate, as a fraud prevention and audit measure.

### Rationale:

Keeping unique records of individual certificates (as well as the life events that they certify) allows verification of documents, which can help in the detection and prevention of identity fraud or other abuses.

### Implications:

Each instance of a printed certificate should be verifiable. Including a unique number, a QR code or a bar code allow tracing and auditability. Certificates should have version numbering to manage changes over the life of an individual (e.g., for amendments and corrections) and to be verifiable. Certificate records should be searchable based on certificate identifiers and version numbers. The printing function may need to be able to manage secure paper for certain certificate types. However, the use of validation feature such a QR code and bar codes — which removes the need for security paper save costs and provide an efficient and secure way to verify the authenticity of certificates may be considered.

## #8 Functionality: Activity logging capacity

### Description:

The system must log all user actions. Any action taken by a user within the system (to access, create, update or delete a record) must be recorded in a log. Each log entry should include what the action was, who made it, when, and what was changed (e.g. by capturing the record before and after an action was taken to modify the record). The log must be protected against illegal manipulations.

### Rationale:

This function enables active and retrospective auditing of the systems and system users, discovering and investigating security breaches (whether by unauthorized individuals or authorized individuals acting in breach of policy) and assisting in the investigation of incidents. It also provides assurance in demonstrating compliance with privacy and data protection laws and policies.

**Implications:**

It is recommended that three levels of logs i.e., access log, process log and audit log be enabled and that these logs form a permanently recorded part of the CRVS system, in line with user activity. The access log enables documentation of records accessed for enquiry or update purposes. The process log develops a history of all processes used by all users in the system. The audit log maintains a permanent history of all changes made to any record on the system.

All logs are to be made available to system administrators and high-level civil registry staff for enquiry purposes. It is recommended that an alert function be put in place and directed at the CRVS management team to enable active monitoring. Access to the logs should be restricted and the logs should be protected from tampering. The system should have the ability to run reports on activity login.

### #9 Functionality: Interoperability (allowing for data importing and exporting)

**Description:**

The system should adopt interoperable standards to exchange data with other external platforms. Interoperability is an essential characteristic of CRVS applications because it facilitates communication and data-sharing among sectors that need to electronically interact with the CRVS system, such as health system, identity system, and statistics as well as potentially with private sector users and across borders.

**Rationale:**

Importing and exporting data from the system is required for various purposes, namely for data-processing (e.g., for ingesting data from the health system such as birth records or to compare data of two individuals for which there is suspicion of record duplication) and data-sharing (e.g., to provide relevant data to another government sector). A common requirement of a civil registration office is to provide regular (and ad hoc) datasets to approved recipients e.g., identity management system, national statistics office, health departments, electoral commissions, education departments, approved private organisations). The CRVS IT system should be able to accept individual records from other systems (e.g., the health information system), as applicable according to the local process for civil registration. Bulk data-importing – in cases in which data cannot be directly entered into the CRVS IT system (e.g., due to an outage) or in cases where historical data previously stored in other formats needs to be imported – is also an important functionality for the CRVS IT system.

**Implications:**

Countries should ensure that any technical platform under consideration has the relevant functionality (currently required and envisioned for the future) to receive and share data from external platforms.

### #10 Functionality: Role-based user permission

**Description:**

A CRVS IT system should define which users have access to which functions and categories of data. That access should be assigned to the role an individual holds within the CRVS system, rather than to the individual. For example, a “deputy-registrar” role should be created, and a number of permissions assigned to that role. Then, all deputy registrars can be assigned that role and automatically gain related privileges.

**Rationale:**

A civil registration organization employs staff with different responsibilities. Users should only have permissions within the IT system to perform actions and access records to which they are entitled due to their roles. This assists in preventing people from performing actions that they are unauthorized, while enabling others to perform the actions which their role requires. The ‘role-based permissions’ functionality facilitates the management of permissions and helps prevent issues such as permission creep and over-provisioning of permissions from arising.

### Implications:

Each user must have a unique username and associated password. Shared user accounts or usernames should not be allowed. Roles should be created to manage system permissions. Permissions should not be attached directly to user accounts. All user accounts must be associated with roles that reflect the functions and data to which they require access in order to perform their duties. Roles and individual assignments to roles should be regularly audited to ensure access is limited to those requiring it.

## #11 Functionality: Storage and backup

### Description:

Civil registration datasets must be adequately maintained to facilitate their retrieval over extended periods of time. The CRVS IT system must include mechanisms to ensure the availability of data and the ability to restore data in the case of an adverse event (e.g., a natural disaster) or failure (e.g., hardware failure).

### Rationale:

Digitization of civil registration records is an enhanced method of record preservation with critical advantages (e.g., improved speed of storage and retrieval). However, complex IT systems are vulnerable to risks to their stored data e.g., data corruption, data loss, malicious damage, and hardware failure.

### Implications:

As part of a formal risk assessment, Recovery Time Objective[7] and Recovery Point Objective (RPOs)[8] should be captured. These will allow solution providers to determine

[7] Recovery Time Objective (RTO) often refers to the amount of time that an application, system, and process can be down without causing significant damage to the business and the time spent restoring the application and its data to resume normal business operations after a significant incident.

[8] Recovery Point Objective (RPO) generally refers to calculating how much data loss a company can experience within a period most relevant to its business before significant harm occurs, from the point of a disruptive event to the last data backup

the appropriate back-up mechanisms required. Back-up and restore mechanisms and plans should be regularly tested to ensure they remain effective. The records or databases created by a back-up procedure should be located in a different geographical area as a mitigation to the risk of natural disasters. All backups should be given the same level of protection (i.e., the same security measures) as the original.

### #12 Functionality: Disaster mitigation

**Description:**

CRVS IT system should include measures to manage the impacts of natural and manmade disasters. Disaster mitigation measures should include the possibility to export data and metadata and take into consideration: electricity supply to servers/data centres; physical security for premises; support for business continuity; and minimization of Recovery Point Objective (RPOs) to prevent or minimize potential data loss. During implementation of the CRVS IT systems, disaster recovery tools and routines (e.g., daily backup or a mirror site) should be put in place.

**Rationale:**

Many countries are at risk of hazards (both natural and unnatural), which could affect civil registration infrastructure (including CRVS IT systems). Mitigating these risks is crucial to ensuring the sustainability and stability of the CRVS system.

**Implications:**

The implementation of CRVS IT systems should include disaster recovery measures grounded in effective IT management practices (system backup and restore capabilities). It is essential to store backups in another geographic location or in the cloud in order to mitigate for the impact of a disaster.

### #13 Functionality: Security Information and Event Management (SIEM) capability

**Description:**

SIEM is a security solution that helps organizations recognize potential security threats and vulnerabilities before they have a chance to disrupt business operations. It surfaces user behavior anomalies and uses artificial intelligence to automate many of the manual processes associated with threat detection and incident response[9]. The CRVS IT system should be consistent in conducting system audits to facilitate constant monitoring of risks and should also pursue ISO Certifications. All systems should have a robust mechanism of user authentication and authorization. Instead of adopting the typical ID and password method, utilizing two-factor authentication with a secondary verification method through a separate communication channel is desired (out-of-the-box authentication).

### Rationale:

This requirement certifies that the CRVS IT system, business process, service, or documentation procedures have all the requirements for standardization and security assurance. It also helps avert and identify risks that could affect the system.

### Implications:

Both internal and external audits should be envisioned to ensure adherence to international standards and help avert possible system hacks and data manipulation. The system of choice should facilitate implementation of SIEM processes to identify security incidents in near-real time, and to enable action in a timely manner to mitigate or minimise any incidences.

## #14 Functionality: Analytics

### Description:

[9] https://www.ibm.com/topics/siem#:~:text=SIEM%20solutions%20enable%20centralized%20compliance,meeting%20strict%20compliance%20reporting%20standards.

Analytics is an advanced feature of data utilization to produce knowledge for the decision-making process. The analytics platforms are specialized software, and the CRVS IT system should be able to connect to third-party analytics platforms to support the analysis of vital statistics and monitoring and evaluation of public policy.

Rationale:

Analytics facilitate the analysis of vital statistics helps to identify patterns and trends in the data collected during the registration of vital events such as births, deaths, and marriages. By analyzing this data, governments and other stakeholders can gain insights into the health public policies and well-being of their populations, identify areas where interventions are needed, and track progress toward development goals.
Additionally, analytics can help identify errors or inconsistencies in the data and take corrective action to improve its accuracy and completeness.

Implications:

Countries need to incorporate analytics capabilities into their digital CRVS IT systems. There are a variety of platforms available, both open-source and commercial solutions, that can be utilized for this purpose. By leveraging these analytics functions, countries can gain valuable insights from the data collected through CRVS systems, which can inform evidence-based policies and interventions to improve the health and well-being of their populations.

## Non-functional requirements of digital CRVS systems

Non-functional requirements relate to the operating level and performance characteristics of the system. Non-functional requirements are relevant criteria to operational characteristics of a system that should be considered when selecting a product. While functional requirements define the system's fundamental behavior, non-functional requirements set out how the system will carry out this function. Unlike functional requirements, non-functional requirements do not form the backbone of the system but are critical for its efficiency. That means the system will still work if the non-functional requirements are not met. Yet, one should not downplay the role of non-functional requirements[10]. While functional requirements are primarily focused on the client's needs, non-functional requirements are more user oriented. The key nonfunctional requirements for a digital CRVS IT solution are outlined below.

### #1 Functionality: Usability

From a user perspective, the ease of use of the software or platform should be considered e.g., its configurability with a multitude of options, its ability to support local languages, its capacity to support language packages that allow for easy translation into the language of choice and the intuitiveness or user-friendliness of the user interface.

### #2 Functionality: Reliability

Reliability is the ability of an application to run consistently without failure over time. To meet this requirement, the software or platform should allow for and implement regular system and data backups for use in case of failure. In addition, the system should be reviewed to assess how likely/unlikely the technical components will hold up/fail over time, based on internal characteristics and external conditions.

### #3 Functionality: Scalability

Scaling digital solutions that are data-intensive requires the application to maintain consistent performance without crashing or stalling as the number of users and data grows over time. For platforms hosted on local servers, the ability to scale also depends on the infrastructure in place. For solutions hosted remotely, internet connectivity will need to be considered.

### #4 Functionality: Auditability

It is recommended that the system should be auditable to ensure the transparency of the data processing and the consistency of the procedures performed by the users. Also, the source code should be available for special audits.

[10] https://www.uptech.team/blog/functional-vs-non-functional-requirements

### #5 Functionality: Documentation

Regardless of whether the software is developed in-house or outsourced, the software must have detailed documentation of its operations for the users and technical characteristics for the IT support staff.

### #6 Functionality: Security

The system should be protected from unauthorized access, use, disclosure, disruption, modification, or destruction of the data of the CRVS system in order to provide confidentiality and integrity. This can be done by the implementation of cryptographic methods to protect the CRVS system from unauthorized access, prevent malicious adulteration of data, among others.

### #7 Functionality: Optimal Performance

The system should have optimal performance for the most common procedures of the CRVS system such as capture, search and retrieve data from the database, printing certificates, listing of reports, among others, considering the basic characteristics of the IT hardware and networking equipment of the CRVS services.

### #8 Functionality: Relevance to local telecommunications context

Country telecommunications infrastructure needs to be taken into consideration when implementing and developing a CRVS IT system. Net-work capabilities (Wide Area Network or Local Area Network) are a key requirement for data interoperability, data-sharing and data integration.

### #9 Functionality: Online and offline access options

In countries where connectivity to the internet is a challenge, the ability of the CRVS IT system to function in both onlineand offline modes is essential.

### #10 Functionality: Mobile device capabilities

Systems can be designed to work on mobile phones and tablets. A mobile app that works offline and seamlessly connects to remote servers is preferred.

## # 11 Functionality: User alerts

User alerts sent to clients through SMS, USSD, email or other channels like social media (e.g., to notify a client that a certificate requested is available for pick-up) can help improve service delivery in a civil registration organization.

# Section 3: Licensing models for digital CRVS Systems

Once the digitalized civil registration process has been designed, the technical application requirements have been specified based on the fundamental principles, and an agreement has been reached on the main functional and non-functional technical requirements, it is time to choose the appropriate source code licensing model. This decision is crucial for the implementation strategy of the CRVS application.

When choosing a suitable license model is crucial to weigh the benefits and risks of each option and consider the findings of a comprehensive assessment; this will help determine suitable choices for the country's specific needs.

There are (2) two main types of source code licensing models for digital CRVS systems, namely: Proprietary commercial software license and Open-source software license. This section outlines the key benefits and risks/disadvantages that a country would encounter in adopting either licensing option.

## Proprietary commercial software license

A proprietary commercial software license is a legal agreement between the software vendor (company or individual) and the client (organization such as for example the civil registration agency) that grants the client the right to use the software under certain conditions. This type of software is typically sold for a fee and is protected by copyright law.

### Benefits

- Time used to purchase the software is much shorter than time spent developing the same software.
- Often fewer resources in terms of human capital, and money are required.
- In addition to the actual software, the country will also benefit from the company's experience in developing and installing the CRVS IT system, leading to less-risk and a more robust implementation.

- Commercial systems are typically designed to adapt to differing infrastructures and environments and likely will have data exchange and data-sharing facilities already.
- The system is more reliable as commercial software is generally tested for more varied uses and to meet different security requirements.
- The software will continually improve by sharing functions from other jurisdictions where it is utilized.
- System customization can be considerably limited in the case of 'off-the-shelf' solutions.
- The system can be evaluated before purchase.
- The system is maintained by the vendor and often upgraded (usually at a cost).
- The access to source code can be included in the contract, however the clients are not allowed to change it.

## Disadvantages/ Risks

- Often, purchasing a commercial system also means relying on the implementing vendor for ongoing support. There is a risk of the client being dependent on the vendor and of the vendor becoming unable to provide the required support (e.g., if the company goes bankrupt or decides to discontinue a software).
- Commercial software suppliers will want to protect their intellectual property (i.e. the source code, database schemas, instruction manuals). It is important to discuss and understand the intent and scope of this protection, so it is clearly understood by all parties and any risks mitigated. Regardless of the intellectual property of the software, the contract must establish that the country is the owner of the data.
- There may be a need to customize the software to fit individual business functionalities fully, which can be expensive and time-consuming if not initially discussed or understood at the beginning of the project. The business process innovation should be performed before the customization to reduce costs and ensure fully conformity of the CRVS IT system with the country legislation and technical requirements (i.e. the commercial IT solution should not determine the civil registration process of a country).

- Where the software is licensed periodically or for a set number of users, the vendor may charge fees for additional users or usage of the system. It is important to discuss and understand this at the beginning of the project.
- The system is often expensive and sold with unclear, complex fee structures (e.g., a fee-per-user which may be combined with other criteria).
- There are always new requirements to improve the system. Any modification of new implementations would incur additional costs and technical support.
- At the end of the contract, there is a high risk of discontinuity of the CRVS services or strong limitations to migrate to another system. The license must ensure full access to data and tools to migrate it to another database.

### Open-source software license

Open-source licenses allow software to be freely used, modified, and shared[11]. The source code and the software product are freely available. However, the professional services to customize or implement the solution can be paid or free, depending on the developer's business model. The software is usually supported by a community of developers and users[12].

#### Benefits

- There are no upfront costs, but implementation, maintaining or customising it will likely require investment.
- Clients have the right to make changes to the software.
- Clients can engage the local IT industry for customisation, maintenance, and/ or implementation.
- The software benefits from a community of practice and updates/ enhancements of functionalities included in other jurisdictions in which it is implemented.
- Development costs can be shared with other organisations or countries.

#### Disadvantages/ Risks

- A loosely knit community of users/developers might not be able to provide the business

[11] An extensive list of licenses that comply with the Open Source Initiative license definition is available at: https://opensource.org/licenses/

[12] The Pacific Community (SPC) has recently supported Niue to implement OpenCRVS and opensource licensed at a national level.

relationship needed or the liability and accountability considerations but if the community is not sufficiently strong it may not be able to maintain the software.

- While open-source software eliminates the need for licensing fees, allocating resources and budget for the configuration, implementation, and system operations is still necessary.
- Lack of local technical support and local human resources available in the country could jeopardize implementation (e.g. local developers not familiar with the programming languages or underlying technologies involved).
- Free and open-source software often requires integration and/or dependencies with components that are developed and supported by other organisations, adding complexity in the solution.

### In-house software development

The decision between in-house or outsourced software development is a critical choice the CRVS institution faces when digitalizing its CRVS system.

Outsourcing the development of CRVS software involves procuring external software development firms or freelancers to provide the desired software, offering distinct benefits. It can enhance cost-efficiency, particularly for short-term projects, by eliminating the need for in-house technical staff. Speed is another advantage, as experienced outsourcing partners can expedite project timelines through resource leverage. Furthermore, outsourcing permits organizations to scale resources up or down to meet project demands, providing valuable flexibility.

Whether to develop in-house or outsource software depends on various aspects, like budget, staff expertise, and timeline. Ultimately, the decision should be based on the organization's goals and available resources. It's essential to choose an approach that best supports successfully complying with core CRVS digitalization best practices presented in previous sections of this guide.

Many CRVS organizations create their own software with the help of public servants or consultants. A recent study by the African development bank revealed that 72% of African countries use custom-built software for their CRVS data systems[13]. To protect their ownership of the software and source code, it is vital for all professionals involved in the development process to sign a commitment agreement.

Indeed, an in-house software can be tailored specifically to meet the organization's unique requirements. This means that the solution's technology, functionality, and design can be fully controlled and customized according to the preferences. By having an in-house solution, the organization can optimize its operations and ensure that the system works as it needs.

Another advantage of in-house software is its potential for seamless integration with other governmental solutions, such as national ID and population registry, allowing the creation of a fully integrated IT infrastructure across the country.

When the solution is developed by internal staff members who understand the organization's requirements and business processes, they can add significant value by suggesting alternatives and improvements. They can provide valuable IT advice and information based on their knowledge of the organization's operations and objectives. This development experience creates a sense of ownership and accountability within the organization, leading to better sustainability and long-term support for the solution.

Additionally, engaging the local IT industry for development opportunities promotes local capacity.

In contrast, developing in-house software has disadvantages. For example, it may not take advantage of the valuable experience and lessons learned from other jurisdictions that have implemented similar systems. The lack of knowledge transfer can lead to unnecessary challenges and delays in the development and implementation, and it may mean the development of software components that have already been developed in other jurisdictions and may even be available as open-source software.

Developing and testing an entire software poses a higher risk level than utilizing pre-existing commercial or community-supported open-source software. For software developed in-house, the CRVS organization must invest significant effort, resources, and time into thorough testing and quality assurance to minimize the risks associated with potential bugs,

[13] Link to AfDB Assessment

vulnerabilities, or compatibility issues that may arise during the implementation and operational phases.

The financial investment required to develop software from scratch is typically higher than adopting commercial or community-supported open-source software. It needs dedicated resources, including skilled developers and project management expertise, which can increase the overall costs. Additionally, ongoing maintenance, support, and updates may require continued investment, mainly if the organization relies heavily on the developers for support services. The higher costs associated with in-house software development should be carefully considered in terms of budget constraints and long-term sustainability.

If the CRVS organization opts to hire consultants to develop the software, it could be challenging, mainly if there is a lack of internal expertise in maintaining and troubleshooting the system. It can create a dependence on the consultants.

Developing and supporting an in-house CRVS system heavily relies on local technical skills. In regions with a shortage of skilled professionals or limited access to specialized expertise, developing and maintaining an in-house solution may face challenges.

Another disadvantage or risk of an in-house solution is the difficulty in migrating off the technology in the future. If knowledge and technical documentation are primarily held by the developers or not adequately documented, it can pose challenges when transitioning to a different technology or vendor. The organization may depend on the original developers for ongoing support and maintenance, limiting future flexibility and adaptability.

### Software modification and migration of data

It is important to note that the ability to make modifications to the CRVS IT system and to migrate data to another system are key requirements regardless of which type of software is chosen. Countries should endeavour to understand from the vendor, the cost and licensing implications of any required changes to the standard commercial system to enable it to meet the specific requirements of the country and the process for the migration of data. When analysing the potential changes needed and the necessity to eventually migrate to a new system, the following components should be understood:

1. **Cost of change**: the cost to be charged by the implementing vendor to make the changes (including any upfront costs as well as any effects on subsequent maintenance or support fees).
2. **Time to make change**: the time needed to make the changes should be integrated into the greater project plan.
3. **Risks of testing new system**: the number and extent to which various components of the software (i.e., database/business rules/user interface/security/outputs, etc.) need to change and the risks associated with testing the new system, including risks of making other components of the system unstable, which is the greatest challenge to the completion of the project and needs to be considered carefully.
4. **Intellectual property**: ownership of the intellectual property of any changes made, including whether the vendor wants and/or expects the changes to form a part of their standard product made available to other civil registration offices.
5. **Business continuity during migration to a new system**: Every system has a limited lifetime and migration to another solution should be expected and planned. The license and the contract should facilitate the migration to a new system and ensure CRVS's services continuity during this process.

## Section 4: Hosting options

When implementing a digital CRVS system, the infrastructure – that is to say the central hardware that will be running the system and storing the data being collected – that supports its operation is crucial. The choice of hosting services which will provide that infrastructure, significantly impacts adherence to principles like sustainability, data accessibility, security, and privacy. Moreover, deciding where to host and maintain the IT system and the data, requires considering technical and human resource aspects such as server space, power supply, security and privacy protocols, anti-virus software, backup servers, and the need for skilled personnel to manage these systems. As such, it is essential to conduct a thorough analysis to select the most appropriate hosting option.

A recent assessment by APAI-CRVS and AfDB shows that 72% of African countries use the self-hosting model for their civil registration organisation[14]. However, the model of outsourced hosting should be considered when making a decision on this important issue.

While many countries may have concerns about the reliability of hosting with a cloud computing service, there is a growing global trend toward adopting this model[15]. Therefore, it is wise to consider moving for this alternative.

Numerous hosting options exist for systems, but they primarily fall into two main models: self-hosting, where the civil registration organisation retains complete control over the infrastructure, and cloud hosting, where hosting services are outsourced to an external service provider. This section discusses benefits and disadvantages of these two models.

[14] Digitalisation of Civil Registration and Vital Statistics (CRVS) Systems in Africa: An assessment of the level of digitalisation of CRVS systems in African countries. APAI-CRVS, 2023.

[15] New Zealand and Australia have recently adopted cloud storage for their CRVS data

### Self-hosted

The software and data are hosted internally by the civil registration organisation or by another governmental agency responsible for the national ICT datacenter. The model can also be defined as "on-premises hosting" because the IT infrastructure, applications, and data are physically located within the premises of the civil registration organisation. This implies that the agency authority owns and cares for the hardware, software, and infrastructure to host its IT systems and the data. Adopting virtualization[16] technologies is highly recommended even for self-hosted solutions. Moreover, self-hosting can utilize cloud technologies, such as load balancing and containerization[17], called private cloud hosting. In this approach, the hosting continues to be used exclusively by that organization and is not shared with other external users or organizations.

#### Benefits

- The servers and data are completely under the control of the civil registration organisation.
- The civil registration agency can maintain complete control of software, functions and features.
- Software decisions are completely up to civil registration agency.

#### Disadvantages/ Risks

- Servers are subject to the local environment such as: power outages, other accidents, flooding, fires, earthquakes, etc..
- This system requires discipline to maintain backups and procedures for disaster recovery.
- Limited performance and capacity to quickly integrating cutting-edge applications and innovation.
- It is the responsibility of the civil registration agency to maintain the operating system and application software patches and upgrades and add devices, as required.
- There are more demands placed on the local IT staff.
- There are potentially higher total costs associated with ownership.

[16] Virtualization is a technology that allows multiple virtual instances or virtual machines (VMs) to run on a single physical server or host machine. Each virtual instance operates like a separate physical server with its own operating system, applications, and resources.

[17] Containers are software like Docker and Kubernetes that facilitate the packaging and deployment of applications and their dependencies in isolated, portable containers.

- It requires investment in physical security, incident management practices and back-up management, which may be difficult to support.
- It is a high IT investment and generally a significantly large investment for a non-IT/ low-IT government department such as the civil registration authority.

### External hosting, including Cloud Computing

External ,Ecan be with a governmental or a private service provider. In this case, civil registration authority will not control entirely the infrastructure used by its IT system. In this case, its important to implement legal and technical measures to ensure that data ownership remains with the civil registration authority and that changes to the CRVS IT system are possible. Specifically, the retention of complete control over the software and all its functions and features is necessary and should be included as a clause of the contract.

If a civil registration authority switches from a self-hosted to an outsourced model, developing a plan and preparing its IT staff for this change is crucial.

Nowadays, the trend is cloud. In this model, the applications are fully hosted on remote servers, the software is sold (or offered freely) as a service that can be contracted per user and per month/year per record or by volume of records, and the software vendor usually offers it as a package delivered by the Internet.

Hiring a cloud computing service is the most common form of outsourced hosting. Outsourced cloud services are also called off-premise or public cloud and can include well known providers already used by countries such as AWS, Oracle, Microsoft or google.

There may bemaybe concerns about the idea of giving up so much control. Even though employees at reputable cloud hosting vendors undergo background checks, some organizations aren’t comfortable with someone else handling and possibly accessing their data. Some countries legislations address these concerns, which makes the choice of vendor and the geographic location of their datacenters important in terms of applicable law.

It is possible to adopt a hybrid cloud model that includes both public and private cloud services, respecting legal and technical requirements. In this case, sensitive data is hosted in a private cloud. Hybrid solution can balance the benefits and risks of cloud computing.

Benefits

- Outsourcing hosting services can be more cost-effective than hosting the system in-house. It can eliminate the need to procure hardware, software, and the core datacenter infrastructure. Moreover, larger data centers have economies of scale enabling them to reduce operational costs.
- Specialized data centers are often more flexible and can adapt quickly to unexpected demands and new needs without a lengthy procurement process or compromising quality or speed.
- Providers in hosting services have a team of experts highly specialized and dedicated to managing and maintaining their services.
- CRVS organizations can focus on essential activities, including improving the functionalities of their IT system which is then hosted by a dedicated organization.
- Outsourcing providers typically have redundant systems and backup procedures to ensure the system remains available during a disaster or outage.
- Most cloud providers do offer some amount of protection at least at the infrastructure level, such as intrusion detection and protection against denial-of-service attacks.
- Cloud computing adopts high levels of automation of routine tasks, which can help streamline operations and optimize the available resources.

Disadvantages/ Risks

- Maintaining a consistent connection between the practitioner and the data center can be difficult due to challenges in the telecommunications infrastructure. If Internet goes down, remote data stores cannot be accessed – although this can be mitigated by maintaining on premise mirrors.

- Using an external data center, the CRVS organization risks losing total control of its IT system. Measures must be put into place to ensure that data ownership remains with the CRVS authority and that changes to the CRVS IT system are possible. Specifically, the retention of complete control over the software and all its functions and features is necessary and should be included as a clause of the contract.
- A private provider may offer low initial prices but charge additional fees for services you assumed were included. The hidden costs can result in unexpected expenses and administrative problems. As required the CRVS authority may want to seek support during contracting to ensure that such eventualities are considered.CRVS organizations are not often well-positioned to pay a regular service fee.

### Combining models

Adopting a hybrid model, combining self-hosting and cloud hosting is possible. A hybrid cloud combines elements of both self-hosting and cloud hosting. In a hybrid cloud setup, data and workloads can move seamlessly between the two infrastructures, allowing organizations to leverage the benefits of both models.

Although running datacenter often ends up costing higher, except in specific cases of organizations with high technical capabilities and intense resource needs, the advantage of datacenter is that money is spent upfront as a capital expenditure, which in many organizations is easier to sell to upper management or donors. However, a financial analysis including amortization, cost of replacement, and the cost of the required human resources would clearly switch the picture in favor of cloud hosting in most cases.

Most developing countries face difficulties possessing an advanced connectivity infrastructure and have concerns about data sovereignty. These two factors are barriers to the widespread adoption of the cloud hosting model. If a CRVS organization decides to migrate to the cloud hosting model, it is highly recommended to establish a gradual and pragmatic strategy for migration.

## Section 5: Procurement considerations

TheT procurement process entails determining the requirements for the CRVS IT system, communicating with suppliers, administering contracts and assuring quality of the products/services procured.

Procurement of IT systems for CRVS is at the core of the civil registration organization's business as any changes effected can significantly impact on the performance of the organisation (both positively or negatively), including its relationship with other stakeholders with whom civil registration services and products could be linked (e.g., the health system, the identity system, the statistics system, etc).

Procurement processes should therefore be managed carefully and under the leadership of appropriate professionals knowledgeable about the requirements of the solution and the acquisition procedures.

Within the civil registration organisation and/or as a part of the broader government ministry there should be an established model/protocol of IT procurement which provides guidance about managing procurement procedures and tasks and enable collaboration betweenpeople involved in the IT system procurement process. Such a model is important as itserves as a framework used by management teams to make the process of acquiring IT systems easier, transparent, and comprehensive.

A generic procurement process begins by setting up the context and status of the CRVS system, based on the earlier assessment. This includes answering critical questions such as: what performance issue/challenge is the civil registration organisation seeking to address through a new IT system[18][19]? What is the extent of the challenge? What are alternative solutions to addressing the challenge? What are the benefits, costs and risks of engaging in the

[18] A comprehensive analysis of the existing CRVS business processes should be undertaken to identify possible weaknesses and redundancies. Guidance on how to undertake business process analysis is provided in the "CRVS Systems Improvement Framework" (https://www.vitalstrategies.org/resources/crvs-systems-improvement-framework/). This should be followed by a redesign of processes, for which the IT solution would be built on. It should be noted that digitalization of ineffective CRVS processes would result in similarly flowed/ineffective processes. As such, it is imperative that any digitalisation process is preceded by informed analysis.

[19] 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 also found in the CRVS Digitisation Guidebook (CRVS-DGB) published by the United Nations Economic Commission for Africa, developed for the Africa Programme for Accelerated Improvement of Civil Registration and Vital Statistics (APAI-CRVS). http:// www.crvs-dgb.org/en/methodology/.

procurement of a new system?

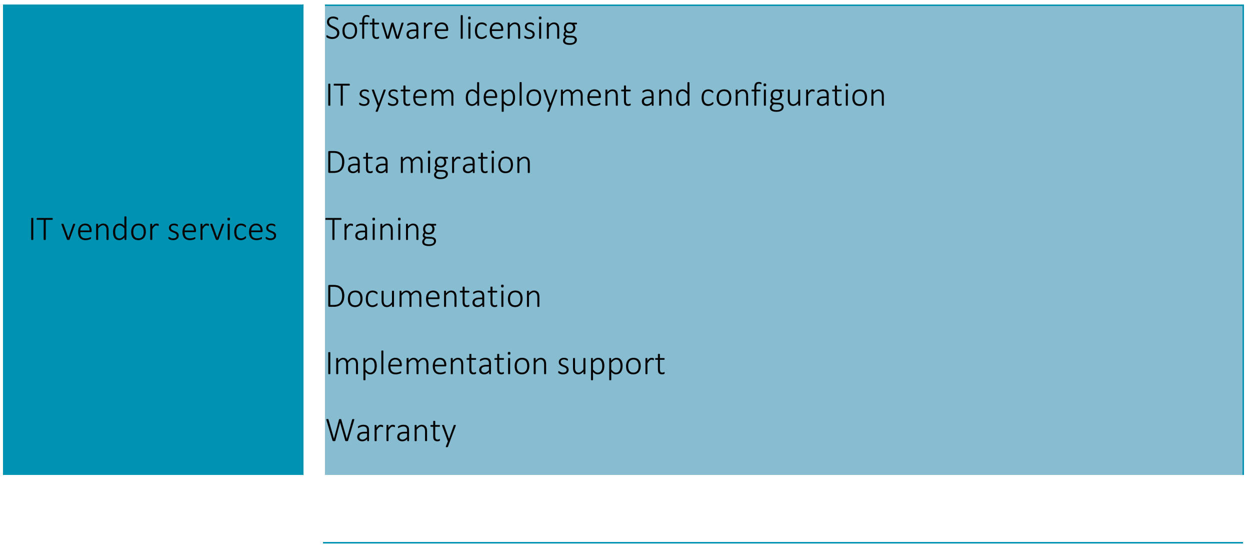
Then requirements are gathered to establish a business case for the IT procurement process in alignment with the vision and goals of the CRVS system and organisation (Section 1 - Principles for design and implementation of Digital CRVS Systems) and the technical requirements (Section 2 - Key functional and non-functional requirements of digital CRVS Systems) of the CRVS system and of the civil registration organisation.

### Total Cost of Ownership

Another important consideration of the procurement team should be the implementation and running costs of the IT system. The cost of implementing and operating a CRVS IT system varies depending on the technologies and systems chosen, as well as the scope and scale of implementation.

While making the choice of the IT solution to procure, it is important to consider the Total Cost of Ownership (TCO), which is composed by (1) the initial costs of implementation and (2) the operational costs. See Figure 1 for initial costs of implementation and Figure 2 for the operational costs.

### Initial costs



IT vendor services

- Software licensing
- IT system deployment and configuration
- Data migration
- Training
- Documentation
- Implementation support
- Warranty

| | |
|---|---|
| IT infrastructure | Servers<br>Data storage devices<br>Computer networking equipment<br>Computers<br>Mobile devices<br>Printers and scanners<br>Third-party software licensing |

**Figure 2. Operational  costs**

| | |
|---|---|
| **IT vendor services** | Software licensing<br>Post-warranty support and maintenance |

| | |
|---|---|
| **Hosting** | Hosting of production IT system<br>Hosting of development, test and training IT systems<br>Hosting of recovery IT system<br>Storage of data backups |

| | |
|---|---|
| **IT infrastructure replacement/ renewal** | Servers<br>Data storage devices<br>Computer networking equipment<br>Computers<br>Mobile devices<br>Printers and scanners<br>Third-party software licensing |

Following acquisition is the contract execution stage which entails managing and coordinating all the activities associated with the fulfilment of the IT procurement contract requirements.

This phase includes acceptance of the products/services provided, installation of systems and management of warranty and maintenance services. During this stage, irrespective of the digital solution that is chosen for implementation, it is essential to ensure that there is sufficient knowledge and information/training provided by the IT software supplier to the national IT and/or CRVS staff to ensure that adequate capacity is built locally for the daily maintenance or operation of the solution. Written protocols of essential features of the software and how it is to be managed should be provided to the country and as much as possible simplified. The national team should also to every extent possible ensure that the terms of contract are met by the supplier and that any matters are addressed in a timely manner. In addition, it is important that any changes made as an outcome of the procurement process be made in a timely way and without impacting business continuity.

Stages of procurement

Following an established 6 stages model will help ensure that the procurement process follows best practices and mitigates any possible risks.

1. Planning the procurement

- Securing financial resources, whether be from national budget or donor fund.
- Define the technical team responsible for the requirements.
- Prepare the Term of Reference (ToR). ( Current system description,  Vision, functional and non-functional requirements)
- Receive authorization to initiate the procurement process.

2. Launch a request for Expressions of Interest

- Calling first for Expressions of Interest (EoI) enables the purchaser to find out what vendors are offering.
- After the EoI, the purchaser can make decisions about which contractual aspects arenot negotiable (hosting, source code rights, etc.).
- Based on the EoI, a shortlist of providers to receive the RfP can be elaborated.

3. Define tender selection criteria and write Request for Proposals

- A RFP for a CRVS IT System should be elaborated based on a consultative process involving relevant stakeholders.

- The RFP should be specific. Tighter criteria will receive targeted responses that can be compared.
- The profile of the type of vendor required should be specified, with vendors that can offer local support in the country favoured.
- Vendor warranty, maintenance and support services after implementation should be included in the procurement package.
- Rather than specify restrictive hardware requirements in the RFP, the vendor should propose the appropriate hardware for the offered IT system, as long as it is compatible with the government IT infrastructure (e.g. the existing data centre where the IT system will be hosted).
- A checklist with recommended content for a RFP is provided in Appendix 1.

### 4. Release RFP and respond to bidders' questions

- The RFP should be released with enough lead time for proposal submission.
- Questions raised by bidders should be discussed and answered in writing.

### 5. Evaluate proposals

- The evaluation should consider Total Cost of Ownership (both initial implementationand operational costs of the IT system).
- Consider sending a list of questions/areas to be clarified to the bidder along with a timeline within which the responses should be provided.
- It is important to ensure that the hardware proposed by the vendor is of good qualityand fits the target IT environment.
- Valuable insights can be gained from reaching out to other countries implementing the IT systems offered by the bidders, to collect feedback on the performance of thespecific vendors' IT systems.

### 6. Award, negotiate and sign the purchase contract

- Writing a purchase contract for an IT system is of utmost importance, as it will legally define the relationship with the vendor and what is expected from the vendor.

- Vendor warranty, maintenance and support services should be well outlined within the contract, along with the delivery of a functional IT system.
- The cost of developing new features for the IT system during its lifetime should be included in the contract.
- Documentation (e.g. manuals, passwords) to be handed over during the IT system implementation should be indicated in the contract.
- In cases in which the software is licensed for a given timeframe, number of sites or number of users, the vendor may charge fees for additional users or usage of the system. It is important that the contract clarify the terms for application of such provisions.
- It should be made clear in the contract that all data is owned by the government (or its citizens, depending on the legal framework), and the vendor can neither claim ownership over data nor withhold access to it.
- The contract should clearly define the legal framework under which the contract is managed, as well as the legal jurisdiction where the data will be stored (advisably the country where the IT system is being implemented).
- There should be a software escrow arrangement in place, so the IT system source code is held by a third party and accessible to the government (and can be further maintained and developed by the government or another vendor) in case the vendor ceases to exist due to bankruptcy.
- Periodic reviews of vendor performance should be included in the contract, as well as provisions on how to handle the transition if the contract is terminated.

A checklist with recommended content for a purchase contract is shown in Appendix 2

| 1. Planning the procurement |
|---|
| • Securing financial resources, whether be from national budget or donor fund.<br>• Define the technical team responsible for the requirements.<br>• Prepare the Term of Reference (ToR). ( Current system description, Vision, functional and non-functional requirements)<br>• Receive authorization to initiate the procurement process. |
| 1. Launch a request for Expressions of Interest |
| • Calling first for Expressions of Interest (EoI) enables the purchaser to find out what vendors are offering.<br>• After the EoI, the purchaser can make decisions about which contractual aspects are not negotiable (hosting, source code rights, etc.).<br>• Based on the EoI, a shortlist of providers to receive the RfP can be elaborated. |
| 2. Define tender selection criteria and write Request for Proposals |

- A RFP for a CRVS IT System should be elaborated based on a consultative process involving relevant stakeholders.
- The RFP should be specific. Tighter criteria will receive targeted responses that can be compared.

- The profile of the type of vendor required should be specified, with vendors that can offer local support in the country (through a local and well qualified partner) favoured.
- Vendor warranty, maintenance and support services after implementation should be included in the procurement package.
- Rather than specify restrictive hardware requirements in the RFP, the vendor should propose the appropriate hardware for the offered IT system, as long as it is compatible with the government IT infrastructure (e.g. the existing data centre where the IT system will be hosted).
- A checklist with recommended content for a RFP is provided in Appendix 1.

3. Release RFP and respond to bidders' questions

- The RFP should be released with enough lead time for proposal submission.
- Questions raised by bidders should be discussed and answered in writing.

4. Evaluate proposals

- The evaluation should consider Total Cost of Ownership (both initial implementation and operational costs of the IT system).
- Consider sending a list of questions/areas to be clarified to the bidder along with a timeline within which the responses should be provided.
- It is important to ensure that the hardware proposed by the vendor is of good quality and fits the target IT environment.
- Valuable insights can be gained from reaching out to other countries implementing the IT systems offered by the bidders, to collect feedback on the performance of the specific vendors' IT systems.

5. Award, negotiate and sign the purchase contract

- Writing a purchase contract for an IT system is of utmost importance, as it will legallydefine the relationship with the vendor and what is expected from the vendor.
- Vendor warranty, maintenance and support services should be well outlined within thecontract, along with the delivery of a functional IT system.
- The cost of developing new features for the IT system during its lifetime should beincluded in the contract.
- Documentation (e.g. manuals, passwords) to be handed over during the IT system implementation should be indicated in the contract.
- In cases in which the software is licensed for a given timeframe, number of sites or number of users, the vendor may charge fees for additional users or usage of the system. It is important that the contract clarify the terms for application of such provisions.
- It should be made clear in the contract that all data is owned by the government (orits citizens, depending on the legal framework), and the vendor can neither claim ownership over data nor withhold access to it.
- The contract should clearly define the legal framework under which the contract is managed, as well as the legal jurisdiction where the data will be stored (advisably thecountry where the IT system is being implemented).
- There should be a software escrow arrangement in place, so the IT system source code is held by a third party and accessible to the government (and can be further maintained and developed by the government or another vendor) in case the vendorceases to exist due to bankruptcy.
- Periodic reviews of vendor performance should be included in the contract, as well asprovisions on how to handle the transition if the contract is terminated.
- A checklist with recommended content for a purchase contract is shown in Appendix 2.

Following execution, a new phase of procurement management entailing the overall governance of IT procurements is initiated. This phase includes management of the vendor/supplier relationship, management of the assets acquired including development of asset management strategies and quality management which entails implementing continuous improvement in the procurement management process, and in all the products and services provided for IT purposes within the organisation.

# References

World Bank. 2008. Supply and Installation of Information Systems – Single-Stage Bidding, December 2008. Available at: https://projects.worldbank.org/ en/projects-operations/products-and-services/brief/procurement-plicies-and-guidance#standarddocuments.

Inter-American Development Bank and UNICEF. 2015. Toward Universal Birth Registration: A Systemic Approach to the Application of ICT. Available at: https://www. unicef.org/protection/files/ICS_CoPUB_Toward_Universal_Birth_Registration.pdf.

United Nations. 2018. Handbook on Civil Registration and Vital Statistics Systems: Management, Operations and Maintenance. Available at: https://unstats.un.org/unsd/ demographic-social/Standards-and-Methods/files/Handbooks/crvs/crvs-mgt-E.pdf.

United Nations. 2014. Principles and recommendations for a vital statistics system. Available at: https://unstats.un.org/unsd/demographic/standmeth/principles/ M19Rev3en.pdf.

Daniel Cobos, Carla Abouzhar and Don de Savigny. 2018. The 'Ten CRVS Milestones' framework for understanding Civil Registration and Vital Statistics systems. Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5873547/.

Brisbane Accord Group. 2015. Regional Standards for Information Technology for Civil Registration and Vital Statistics in the Pacific Islands. (Unpublished )

APAI-CRVS, The civil registration and vital statistics Digitisation guidebook. http://www. crvs-dgb.org/en/

Vital Strategies. CRVS Systems Improvement Framework. Available at : https://www.vitalstrategies.org/resources/crvs-systems-improvement-framework/

## Appendix 1: Procurement checklists: Contents of a Request for Proposals

### 1. General

Scope of Request for Proposal

Request for Proposals process

Eligible bidders

Required qualifications of the bidder

Agency and person in charge of the procurement

### 2. Technical requirements

Functional requirements

Non-functional requirements

Hardware compatibility requirements

Testing requirements

Implementation schedule

Warranty, maintenance and support services required

### 3. Preparation of proposals

Language of the proposal

Documenting process of the proposal

Proposal price and currency

Period of validity of the proposal

### 4. Submission of proposals

Deadline of submission

Late proposals

Withdrawal, substitution and modification of proposals

**5. Evaluation of proposals**

Opening of proposal by purchaser

Clarification of proposals

Criteria for verification of requirements (mandatory and optional)

Evaluation and comparison of proposals

How to contact the purchaser

**6. Contract award**

Award criteria

Notification of award

Write justification for elimination of bidders

Contract negotiation

Signing of contract

## Appendix 2: Procurement checklists: Contents of a Purchase Contract

**1. General**

Definitions

Notices

Governing law

Settlement of disputes

**2. Subject matter of contract**

Scope of the system

Implementation schedule

Supplier’s responsibilities

Purchaser’s responsibilities

**3. Payment**

Contract price

Deliverables and percentage of payments

Terms of payment

Taxes and duties

**4. Intellectual Property**

Copyright

Software license agreements

Confidential information

**5. Supply, installation, testing, commissioning and acceptance of thesystem**

Representatives of contractual parties

Project plan

Design and engineering

Inspections and tests

Installation and configuration

Acceptance

Training of government staff

Handover

**6. Services**

Training

Warranty

Corrective maintenance

Evolutive maintenance

Support

Development of new functionality

**7. Data**

Data privacy

Information security

Legal jurisdiction

Data ownership

**8. Guarantees and liabilities**

Warranty and defect liability

Loss of or damage to property

Accident or injury to workers

Indemnification

Insurances

Force Majeure

Software escrow

## 9. Change in contract elements

Changes to the contract

Changes to the system

Termination