BEST PRACTICE GUIDELINES FOR DIGITAL CRVS SYSTEMS

DRAFT FOR CONSULTATION

Pacific Community
Communauté du Pacifique

Vital Strategies

Swiss TPH
Swiss Tropical and Public Health Institute

Bloomberg Philanthropies

DATA FOR HEALTH INITIATIVE

Pacific CRVS
supported by Brisbane Accord Group

BEST PRACTICE GUIDELINES FOR DIGITAL CRVS SYSTEMS

DRAFT FOR CONSULTATION

Pacific Community
Communauté du Pacifique

Noumea, New Caledonia
2021

Suggested citation: Mathenge G, Newdick D, Castro G, Dwivedi V, Bratschi M, Renner C, (2021). Best practice guidelines for digital CRVS systems. Noumea, New Caledonia: Pacific Community.

Cover icon: Freepik.com
Design and layout: Gaëlle Le Gall Queguineur

Prepared for publication at SPC's Headquarters,
B.P. D5, 98848 Noumea, New Caledonia, 2021
www.spc.int | spc@spc.int

CONTENTS

ABBREVIATIONS

API	Application Programming Interface
APAI-CRVS	Africa Programme on Accelerated Improvement of Civil Registration and Vital Statistics
CRVS	Civil Registration and Vital Statistics
EoI	Expression of Interest
ICT	Information and Communications Technology
ID	Identity/ identifier
IT	Information Technology
PaaS	Platform as a Service
PCRN	Pacific Civil Registrars Network
RfP	Request for Proposals
RPO	Recovery Point Objective
SaaS	Software as a Service
SPC	Pacific Community
Swiss TPH	Swiss Tropical and Public Health Institute
UN	United Nations
USSD	Unstructured Supplementary Service Data
WAN	Wide Area Network

TABLES AND FIGURES

ACKNOWLEDGEMENTS

This report is a joint product of the Pacific Community, Vital Strategies, and the Swiss Tropical and Public Health Institute.

We would like to thank all those who critically reviewed the contents of this report including:

- Jeff Montgomery, New Zealand Department of Internal Affairs
- Hosea Mitala, United Nations Economic Commission for Africa
- Paulo Siqueira, United Nations Development Programme
- Tanja Sejersen, United Nations Economic and social Commission for Asia and the Pacific
- Philip Setel, Vital Strategies
- Rafael Kluender, Swiss Tropical and Public Health Institute
- David Abbott, Pacific Community
- Rajat Goyal, New Zealand Department of Internal Affairs
- John Kananghinis, New Zealand Department of Internal Affairs
- Risa Arai, United Nations Development Programme
- Chahine Hamila, United Nations Development Programme

The development of this report was supported by the Australian Department of Foreign Affairs and Trade (DFAT) as a part of the support provided to SPC to organise the Pacific Regional Workshop on Legal Identity and Identity Security held in 2019.

This report is, in part, a product of the Bloomberg Philanthropies (www.bloomberg.org) Data for Health Initiative. The views expressed are not necessarily those of Bloomberg Philanthropies.

DEFINITIONS

Application Programming Interface (API)	An interface that defines interactions between multiple software intermediaries (i.e. the types of calls or requests that can be made and how to make them, the data formats, etc.). Through information-hiding, APIs enable modular programming, allowing users to use the interface independently of the implementation.
Civil registration organisation	The government organisation responsible for civil registration of vital events, such as births, marriages and deaths, occurring within a particular jurisdiction.
Cloud	A network of servers and the services, software and databases provided over a network connection. Clouds may be limited to a single organisation (private cloud) or available to multiple organisations (public cloud).
Cloud computing	The use of services, software, and databases via the cloud.
Deployment package	A package used to make a software available for use.
Mobile application (mobile app)	A software application designed for a mobile device.
On-premises hosting	The act of hosting a software locally instead of on a cloud.
Open-source software	A software for which source code is accessible and can be modified by a community of users (as opposed to proprietary software).
Proprietary software	A copyrighted software of which the source code is kept secret by the company who developed it (as opposed to open-source software).
Server	A computer program or a device providing resources to other computers over a network.
Software as a Service (SaaS)	A software licensing and delivery model in which a cloud service provides ready-to-use software through the internet on a subscription basis.
Web application	A computer program executed on an internet or intranet server that can be accessed through a web browser.

SUMMARY

Civil registration and vital statistics (CRVS) systems are increasingly implementing information technology (IT) to support data management processes. In many countries, civil registration officials are involved in making decisions about the type of IT system needed to support CRVS operations. Unfortunately, in some countries, these decisions have resulted in inappropriate vendor contracts and/or led to unfavourable outcomes, such as the acquisition of an IT solution that is not fit-for-purpose or that does not align to the needs of the country. This document aims to provide civil registration officials and other national stakeholders that may be involved in decision making around CRVS IT systems with general guidance on requirements for consideration.

Section 1 presents 11 principles that are essential for the effective design, implementation, and operation of any IT system for CRVS (also referred to as IT solution). Derived from discussions between the member countries and territories of the Pacific Community (SPC) at the Pacific Regional Workshop on Legal Identity and Identity Security, held in July 2019 at SPC headquarters, these 11 principles assert that any CRVS IT system should:

1. **comply with local legislation and standards**;
2. be **sustainable** over the long-term for a country;
3. address **security and privacy at the design stage**;
4. enable **disaster mitigation** measures;
5. allow for the development of a **central record of a person** and links to relevant events as well as other people implicated in the events;
6 **share data** with other agencies/departments/ministries within a country and regionally, as appropriate;
7. be **appropriate to the country context** and not require a superior IT skillset or capability than can be accessible to the country;
8. facilitate **access to data**;
9. **limit ownership of all CRVS data held by the IT system to the country**;
10. be **readily customizable** to handle changes in CRVS processes and changing government priorities; and
11. during implementation, allow for adequate training and the **transfer of knowledge** about the system to country staff.

Section 2 provides guidance on 11 key functional requirements of IT systems for CRVS which are needed to enable management of CRVS operations in line with UN recommendations. These include capacity to:

1. **register all 10 vital events** (live birth, death, foetal death, adoption, legitimation, recognition, judicial separation, marriage, civil partnership and divorce)[1] and man-

[1]Live births, foetal and adult deaths should be prioritized over the other 7.

age the related processes and subprocesses;

2. support the processing of **all steps of civil registration and the production of vital statistics** (i.e. notification, validation and verification, registration, certification, sharing of information, storage and archiving, compilation of vital statistics, quality control of vital statistics, generation of vital statistics and dissemination of vital statistics);
3. **log activities** or record changes and/or amendments to records and maintain critical information to track who has changed each data field, when and where (location of the user);
4. **match an individual's events** with respect to other events and family relationships through the assignment of a unique registration number or code for each record;
5. define **role-based user permissions** to authorise specific users access to functions and categories of data;
6. enable automated **detection of duplicate** entries for the same event;
7. include **data importing and exporting** functionalities and API- based data exchange;
8. enable **querying and record searches**;
9. allow for the **correction and amendment of records**; and
10. permit **storage and back-up** to facilitate retrieval of records over extended periods of time.

Section 3 provides information on the advantages and disadvantages of specific types of software licensing options[2], including custom-developed software, commercial off-the-shelf software and Community-supported open-source software, as described below.

1. **Custom-developed software** is a software that is built from scratch for the country, specifically designed for its particular requirements and can be tailored to fit the way the civil registration organisation wishes to operate.
2. **Commercial off-the-shelf software** refers to software that is ready-made and commercially available.
3. **Community-supported open-source software** is a software for which both the source code and the software product are freely available and there is an active community of practice to support use of the open-source software and its development.

Section 4 elaborates on the advantages and disadvantages of three service and hosting options that may be available to governments to host their data and the CRVS system: software as a service; as an outsourced system; and as a self-hosted system.

1. **SaaS** indicates that the database and software are hosted on remote servers, and that the software is sold (or offered freely) as a service that can be contracted monthly or annually per user.
2. **Outsourced system and data storage** indicates that the organisation customises, buys or develops the software and then hosts the system and data at an external

[2]Although outlined distinctly, it should be noted that some software can exist as a combination of these options. For example, commercial software can be custom developed for a country, etc.

centre. As such, the hosting is outsourced (e.g. at the government IT facility or with a private vendor) and payments are made per user/storage or per month/year.

3. **Self-hosted by the civil registration organisation or parent ministry** refers to systems that are hosted independently.

Section 5 provides key considerations during procurement of IT solutions for CRVS.

An outline of the steps and factors that should be considered when procuring an IT solution for CRVS are provided. These include: launch of a request for expressions of interest; defining selection criteria and writing a request for proposals (RfP), release of the RfP and responding to bidders' questions; evaluating proposals; and awarding, negotiating and signing of the purchase contract. A checklist of the contents of a RfP and a checklist of the contents are provided in the annex.

INTRODUCTION

Civil registration is a core and essential function of governments: by recording vital events, such as births and deaths in a country, citizens and residents gain access to basic rights and the government is able to develop more effective public policies and programmes based on the vital statistics data collected. Information technology (IT) systems are critical to establish well-functioning CRVS. The use of IT systems to collect, transmit, store, protect and retrieve data is central to data management of a civil registration organisation in any jurisdiction. At the same time, if an IT system 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 and even have a detrimental impact on a country's governance processes.

This document is developed to serve as a resource to countries in the 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 the production of timely and reliable vital statistics. Specifically, this document provides information on:

1. Principles for implementation of digital CRVS systems;
2. Key functional requirements of digital CRVS systems;
3. Licensing options for digital CRVS systems and their benefits and risks;
4. Service and hosting options for Digital CRVS systems and their benefits and risks;
5. Procurement considerations.

While the focus is on IT systems used to manage the operations of the civil registration organisation, it is recognised that there are important linkages that CRVS systems should have with other IT platforms within the government (e.g. population register, health information systems, voter registry, national identification (ID) system, and the vital statistics system). It is therefore essential that the IT solution adopted supports the UN integrated approach to civil registration, vital statistics and identity management.

SECTION 1: PRINCIPLES FOR 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 development of IT systems for CRVS are guidelines that support the goals of universal registration of vital events (including the establishment of a legal identity for all persons) and the production of vital statistics.

The **11 principles** provided in this document (see Table 1) are designed to help countries develop and/or procure IT solutions to support civil registration and the production of civil registration based vital statistics. 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, these principles can help guide countries in their engagement with IT system vendors.

Table 1. Principles for implementation of digital CRVS systems

#1 Principle	Legal compliance
Description	Implementation of digital CRVS systems should **comply with National legislation** on CRVS as well as with any additional related legislation or policy (e.g. privacy, security, data-sharing, and digital government).
Rationale	All other principles and requirements are secondary to delivering a system that complies with the specific legislative framework of the country.[3]
Implications	Procurement and design (and the respective planning) for CRVS IT systems should explicitly state how they will ensure compliance with existing legislation, both nationally and internationally, if the data is stored overseas.

#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 current); **instructional** (registry and technical support staff should maintain adequate knowledge to manage the IT system effectively); **commercial** (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 aim to minimise the total cost of ownership of the solution.
Rationale	CRVS IT systems are expected to be a long-term investment for a country. As such, it is imperative to sustain them over their intended lifetime system.

[3]In many countries' legal/regulatory frameworks surrounding digital development are inadequate/incomplete. In such cases IT systems should aim for international standards while waiting for national frameworks to align accordingly.

Implications	The technical, instructional, commercial 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. It is imperative that a sustainability plan be developed alongside the development of the IT system.

#3 Principle	**Privacy and security by design**
Description	CRVS IT systems should explicitly address security and privacy from the initial stages of development or procurement throughout the entire lifecycle of the system (through retirement) to ensure that information security procedures can be implemented on a routine basis. Relevant considerations include deactivation of user log-in after a specified number of unsuccessful login attempts, password expiration and the encrypted storage and transfer of data.
Rationale	CRVS IT systems include significant amounts of personal data which make them attractive targets to malicious actors. Therefore, data security and privacy are important considerations in the selection and/or design of any IT systems. Securing the data that the IT systems hold from unauthorised 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.
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 security and privacy characteristics should be prioritised. Designs 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 security measures of the CRVS IT system up-to-date for the lifetime of the system.

#4 Principle	**Disaster mitigation**
Description	CRVS IT systems should include measures to manage the impacts of natural 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 minimisation of Recovery Point Objective (RPOs) to prevent or minimise potential data loss. During implementation of the 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 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 location in case of a disaster.

#5 Principle	**Person-centricity**
Description	CRVS IT systems should be person-centric: every individual's vital event record (e.g. birth, death, divorce, marriage, etc.) should be connected. 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 prioritised.

#6 Principle	**Interoperability and data-sharing**
Description	CRVS IT systems should be able to share data with other agencies/departments/ministries 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 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). Application Programming Interfaces (API) are essential to provide secure interoperability with internal or external services for various clients (internal or external).
Rationale	Civil registration data is vital to the processes of other CRVS stakeholders and providers of government services (e.g. passports, elections, health, education and vital statistics production). This capability becomes more important with the development of digital government (e-Government) services. Data sharing between countries (e.g. to manage cross-border migration) may further be crucial to improve the performance of CRVS systems. Interoperability ensures the breakdown of 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 formats of data exchange to allow for the differing capabilities of partner organisations or systems. All data-sharing arrangements should be backed by technical documentation detailing who should be allowed to access to the data as well as a robust data protection mechanism.

#7 Principle	Appropriateness to country context, in particular its human resource capacity
Description	CRVS IT systems should not require a greater IT skillset or capability (for implementation or ongoing maintenance) than can reasonably be supplied within a national context 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. This can lead to significant difficulties in maintaining complex IT solutions over the lifetime of the system.
Implications	The implementation of a system should include planning to address capability and knowledge gaps in a country. Countries may consider outsourcing or software-as-a-service (explained below) 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 incubation hubs or universities (and other relevant institutions of knowledge development and learning) to address the capability gaps.

#8 Principle	Easy access to data
Description	CRVS IT systems should make it easy to access data for reporting, discovery and analytical purposes, within applicable legal or personal data protection constraints.
Rationale	Registrars need to be able to access data in a number of ways to meet the requirements of their clients (i.e. the general public) as well as legislative requirements (e.g. reports to the national statistics office) and ad hoc requests which could emerge during special situations (e.g. disasters).
Implications	IT systems that include capabilities for reporting and analysis, provide data in standardised formats for reporting, and use non-proprietary formats to store data should be favoured. Reporting capabilities should include robust security mechanisms, especially robust access control. Modern data analysis and reporting methods (e.g. dashboards and visualisations) should be provided by the system or it should allow easy integration to separate capabilities. Reporting and analytics requirements should be explicitly included in tender documentation.

#9 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. Contracts should state what access vendors and ideally, the source code may have to CRVS data, and which uses of the data (if any) vendors are permitted to have.

#10 Principle	Flexibility
Description	CRVS IT systems should be flexible in their design to handle changes in CRVS processes and government priorities and to respond to ongoing technological changes.
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 IT system that seeks to support multiple countries must take into account those differences.
Implications	During procurement or design, vendors should explain 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.

#11 Principle	Knowledge transfer to countries
Description	Part of the process of acquiring (whether procuring or building) a CRVS IT system should include the transfer of knowledge about the system to country staff as well as adequate training of teams that will use and manage it. This should include business knowledge (i.e. training and knowledge transfer for civil registry staff) and technical knowledge (i.e. training and knowledge transfer for technical IT staff) sufficient to ensure continued operation of the IT system after implementation. Where possible, ownership of the system source code should be included as a requirement. This would provide the possibility for system development/update by local specialists.
Rationale	A CRVS IT system is a long-term investment for a country. As such, it should be able to be managed and supported by staff within the government (civil registry staff or technical staff) to enable full return on the investment over its lifetime.
Implications	The effort, duration and cost of training and knowledge transfer for both civil registry and technical staff should be cited in any plan or proposal to implement a CRVS IT system.

SECTION 2: KEY FUNCTIONAL REQUIREMENTS OF DIGITAL CRVS SYSTEMS

The UN has set out several principles and standards on CRVS through related handbooks and guidelines (https://unstats.un.org/unsd/demographic-social/crvs/index.cshtml#method), which depict a well-functioning CRVS system. It is imperative that any CRVS IT system be designed to meet these principles and standards. Further, the IT system should be tailored to the country's context and be designed to meet both the current and future needs of other stakeholders that may interact with the system (health ministries and departments, national identity agencies, etc.). This chapter provides functional requirements of digital solutions for CRVS, needed in order to manage civil registration operations, in line with UN principles and standards, and that form the basis of widely recognised good practice.

Table 2. Key functional requirements of digital systems for CRVS

#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 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 evolves, the ability to register the other events is anticipated to become a requirement. The CRVS IT system should facilitate the inclusion of all events without requiring major structural adjustments or financial investments.
Implications	Irrespective of the number of 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 processing of vital events should if possible accommodate all milestones of civil registration and the production of vital statistics[4], as indicated in the list below. • notification • validation and verification

[4] 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/.

	• registration • 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	The full value of civil registration to a country is best realised when all CRVS milestones are realised.
Implications	The design of the CRVS IT system should automate all milestones. Regarding notification and verification of vital events, adopting dual and separate sources of information/evidence (e.g. validation of collected information with health datasets) is recommended to ensure the authenticity of the vital events.

#3 Functionality	**Detection, Merging, and Removal of Duplicate Records**
Description	The entry of more than one record for the same event should be automatically detected and the error resolved.
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 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 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.

#4 Functionality	**Querying and record searches**
Description	Users need to be able to search and retrieve records from the 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.

#5 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 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 and when it was changed).

#6 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, including images of the printed template, 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 uniquely numbered to 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. Ideally the printing function should be able to manage secure paper for certain certificate types.

#7 Functionality	Activity logging capabilities
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).
Rationale	This function enables active and retrospective auditing of the systems and system users, discovering and investigating security breaches (whether by unauthorised individuals or authorised 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.

#8 Functionality	Data importing and exporting
Description	The system should be able to receive and send data electronically to other, external platforms.
Rationale	Exporting data from the system is required for various purposes, namely for data-processing (e.g. 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. national statistics office, health departments, electoral commissions, education departments). 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.

#9 Functionality	Role-based user permissions
Description	A CRVS IT system should define which users have access to the 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 organisation 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 not authorised to perform, while enabling others to perform the actions which their role requires. The use of role-based permissions facilitates the management of permissions and helps prevent issues (e.g. 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.

#10 Functionality	Storage and backup
Description	Civil registration datasets must be adequately maintained to facilitate their retrieval over extended periods of time. The 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	The computerisation 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 and RPOs should be captured. These will allow solution providers to determine 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.

#11 Functionality	Consistency in monitoring of risks and improvement
Description	The IT system should be consistent in conducting system audits to facilitate constant monitoring of risks and should also pursue ISO Certifications.
Rationale	This certifies that the IT system, business process, service, or documentation procedure has all the requirements for standardisation and quality assurance. It also helps avert and identify risks that could affect the system.
Implications	Both internal and external system audits should be envisioned to ensure adherence to international standards and help avert possible system hacks and data manipulation. Security Information and Event Management (SIEM) processes should be implemented to identify security incidents in near-real time, and to enable action in a timely manner to mitigate or minimise any incidences.

Depending on the country context and the availability of resources, additional advanced functionalities, listed below, may be relevant.

a. **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 online and offline modes is essential.
b. **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.
c. **Fraud detection capabilities**: IT systems can incorporate mechanisms for fraud detection, which can be useful to detect fraud attempts (e.g. document forgery) in the context of civil registration operations.
d. **User alerts**: User alerts sent to clients (through SMS, USSD, email or other channels (e.g. social media)) can help improve service delivery in a civil registry

organisation (e.g. to notify a client that a certificate requested is available for pick-up).

In addition to the features and functional requirements described above, the criteria outlined below should also be considered when selecting a product.

- **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.
- **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.
- **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.
- **SIEM capability and processes**: All systems should have out-of-the-box authentication, authorisation, and data encryption mechanisms.
- **Analytics**: Understanding the analytical features of the system will be helpful to improve decision-making. For example: Does the software offer online/offline functionality, visualisations and the ability to connect to third party analytics platforms and data warehouses for natural language processing and predictive analytics?
- **Telecommunications**: Country telecommunications infrastructure needs to be taken into consideration when implementing and developing a CRVS system. Network capabilities (Wide Area Network or Local Area Network) are a key requirement for data interoperability, data-sharing and data integration.

© ADB

SECTION 3: LICENSING OPTIONS FOR DIGITAL CRVS SYSTEMS AND THEIR BENEFITS AND RISKS

There are 3 main types of licensing options for Digital CRVS systems namely: (i) custom-developed software, whereby the software is built from scratch to suit the prescribed needs of the users; (ii) commercial off-the-shelf software, whereby the products are ready-made and are readily available for purchase from the commercial market; and (iii) community-supported open-source software in which the source code and the software product are freely available and there is an active community of practice to support their continued development. Table 3 outlines these options as well as their key benefits and risks. Although presented as distinct it is important to note that the three overlap. For example, open-source software can be adapted and then sold as commercial off-the-shelf software.

Table 3. Licensing options for digital CRVS systems and their benefits and risks

Custom-developed software: A software system is built from scratch	
BENEFITS	**RISKS**
• It is specifically designed for your requirements and can be tailored to fit exactly how the organisation wishes to operate. You control the technology, functionality and design. • It can be customised to interface with other software that you operate and potentially provide a fully integrated IT infrastructure across your entire organisation. • If the developers are staff members, they can add significant value to your company by suggesting alternatives and improvements and by providing IT advice and information. • The development experience creates ownership and improves sustainability. • It is possible to engage the local IT industry and, therefore, promote local businesses. • It creates an opportunity to productise the solution and leverage jurisdictions with similar laws creating further economic opportunity.	• It does not necessarily take advantage of CRVS experience in other jurisdictions. • There is higher risk in testing and producing an optimal and secure functioning system. • The investment required is usually higher than with commercial or community-supported open-source software. • A significant investment of time is required during the development process and a custom- made application takes longer to implement. • It can be difficult to obtain support for custom-made software, unless the developers offer support services. • Control over design does not guarantee satisfaction with the end product, as that depends on the capabilities of the technical team and the ability of product owners and end users to accurately express their needs and preferences. • A lack of local technical skills can undermine the development and support for the CRVS system. • It can be difficult to migrate off the technology as knowledge and intellectual property are held by the developer and there are risks of vendor lock-in.

	• Continuous innovation funding is required by the government to enhance the system in order to keep up with the changing technology landscape (often resulting in missed benefits that are otherwise available with commercial products and Community-supported open-source software).
Commercial off-the-shelf software: A commercially available product can be purchased	
BENEFITS	**RISKS**
• Time used to purchase 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, you are also paying for the company's experience in development and installing the CRVS system with the aim of a less-risk and higher-accuracy implementation. • Commercial systems are typically designed to adapt to differing infrastructures and environments and likely will have data exchange and data-sharing facilities already.[5] • 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. • System development costs can be shared. • The system can be evaluated before purchase. • The product is maintained and often upgraded (usually at a cost).	• Often, purchasing a commercial system also means relying on the implementing vendor for ongoing support. There is a risk of the vendor becoming unable to provide the required support. • 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. • There may be a need to customise 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. • 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.

[5]It should be noted that readiness of data exchange also depends on what kind of software one needs to interface with.

Community-supported open-source software: The source code as well as the software product are freely available and there is an active community of practice to support the software	
BENEFITS	**RISKS**
• There are no upfront costs (but maintaining or customising it will likely require investment). • You have the right to make changes to the software. • You 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.	• A loosely knit community might not be able to provide the business relationship needed or the liability and accountability considerations and if the community is not sufficiently strong it may not be able to maintain the software. • Configuration, implementation and system operations still require investment. • A lack of local technical support and local human resources available in the country could jeopardise 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.

It is important to note that modifications will be required to all systems, regardless of which type of software is chosen. Countries should endeavour to understand from the vendor the cost implications of any required changes to the standard commercial system to enable it to meet the specific requirements of the country. When analysing the potential changes needed, the following components should be understood:

a. **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);
b. **Time to make change**: the time needed to make the changes should be integrated into the greater project plan;
c. **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. The potential effect that these changes may have on the system and whether these changes would result in a special version of the CRVS software, outside the vendor's mainstream clients; and
d. **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.

SECTION 4: SERVICE AND HOSTING OPTIONS FOR DIGITAL CRVS SYSTEMS AND THEIR BENEFITS AND RISKS

When adopting digital solution for CRVS functionalities, countries need to select the service and hosting options (i.e. where the IT system and data will be hosted, maintained and accessed). A range of technical and human resource aspects will need to be considered before making a final decision, including: server space; uninterrupted power supply; security and privacy protocols; anti-virus software; back-up servers; and skilled personnel to manage these systems.

This section provides three main options that are available for services and hosting. Table 4 provides the benefits and risks related to each option.

Table 4. Benefits and risks of different service and hosting options for digital CRVS systems

Software as a service: The database and application are 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.	
BENEFITS	**RISKS**
• The software is relatively easy to implement and its maintenance is managed by the SaaS provider. • Implementation and operation costs are clear. • Investment in improved software can easily be shared among customers. • Subscriptions (typically monthly) are available in lieu of a software license; software maintenance or upgrades are addressed by the vendor. • Minimal hardware is needed; only what is needed to access the software over the internet is required. • The country does not need to invest in servers.	• Data is hosted on remote servers and may not always be in agreement with national legal framework and policy. • Ministries are not often well-positioned to pay a regular service fee. • High-quality internet access is required; there can be local cache/data/code that will help SaaS software run more smoothly (while online) or in offline mode (e.g. Google Docs). • There may be limited customisation options. • This system is dependent on vendor support. • There is a need to account and plan for responsibilities and approaches in case of a breach or leak of personal information.
Outsourced system and data storage: The organisation customises, buys or develops the software and then hosts the system and data at an external centre and pays per user/ storage or per month/year.	
BENEFITS	**RISKS**
• The servers are safely located in a secure data centre. • Control over software and its functions and features is retained. • There are multiple options for support.	• This requires continuous connectivity between the practitioner and data centre. • The software and operating system licenses still need to be purchased and the hardware and software may still need to be supplied or for an additional monthly fee to be paid.

	• Telecommunications infrastructure can present challenges.
Self-hosted: The software and data are hosted internally by the organisation or ministry.	
BENEFITS	**RISKS**
• The servers and data are completely under your control. • You maintain complete control of software, functions and features. • Software decisions are completely up to you.	• 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. • It is your responsibility 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. • 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.

SECTION 5: PROCUREMENT CONSIDERATIONS

Procurement of IT systems for CRVS refers to the series of activities and procedures followed to acquire all necessary hardware, software and networks needed to establish and make functional a CRVS IT solution. The process entails determining the requirements for the CRVS IT system, communicating with suppliers, administering procuring contracts, managing IT assets 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 population register, health system etc). Procurement processes should therefore be managed carefully and under the leadership of an appropriate technical team that is well knowledgeable about the requirements of the project.

Within the civil registration organisation and/or as a part of the broader government ministry within which the civil registration agency sits, there should be an established model/protocol of IT procurement which should provide guidance about managing procurement procedures and tasks and enable maintenance of collaboration between people involved in the IT system procurement process. Such a model is important as it serves as a framework used by management teams to make the process of acquiring IT systems easier yet comprehensive. Following an established model will help ensure that the procurement process follows best practices and mitigates any possible risks.

A generic procurement process begins by setting up the requirements of the CRVS system and of the civil registration organisation. Requirements gathering entails establishing a business case for the IT procurement process in alignment with the vision and goals of the CRVS system and organisation. This includes answering to critical questions such as: what performance issue/challenge is the civil registration organisation seeking to address through a new IT system? 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 procurement of a new system?

Once a clear business case is established, a comprehensive analysis of the existing CRVS business processes should be undertaken to identify possible weaknesses and/or redundancies. Guidance on how to undertake business process analysis is provided in the "CRVS Systems Improvement Framework" (https://sdd.spc.int/digital_library/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 digitisation of flawed/ineffective CRVS processes would result in similarly flowed/ineffective processes. As such, it is imperative that any digitisation process is preceded by informed analysis. 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 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). Figure 1 provides key steps outlined in the guideline. The guideline is available from: http://www.crvs-dgb.org/en/methodology/

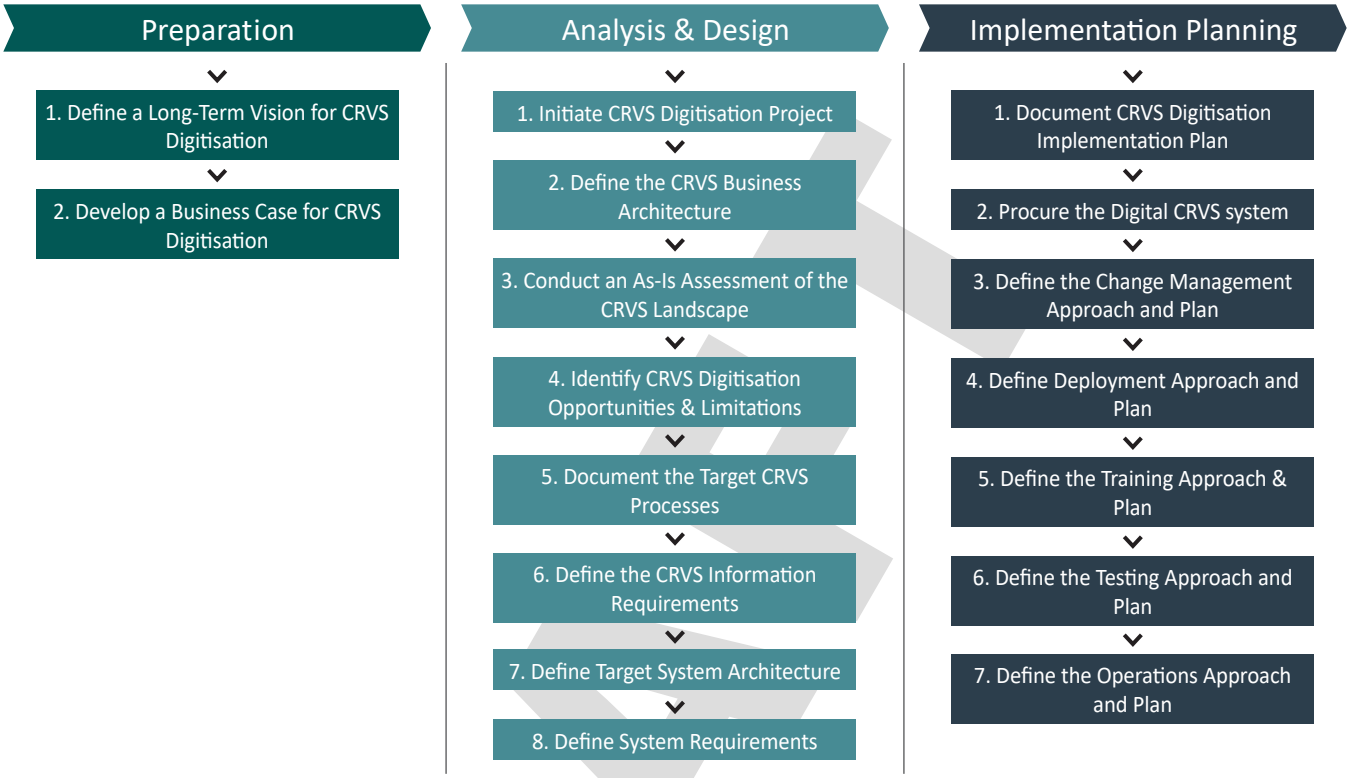

Figure 1. Phases and activities of the CRVS digitisation project

Once the requirements are set up and approval obtained to proceed with the procurement process, the procurement team should be able to proceed to the next stage of **acquisition**. Acquistion refers to engaging the relevant IT procurement managers/ team in evaluating and selecting appropriate suppliers and signing IT procurement contracts and purchase orders for the necessary products/services. Acquisition includes a range of activities including identifying potential solutions that align to the country requirements, establishing communication channels with the suppliers, evaluating proposals submitted and negotiating on the best terms of procurement. As described in the previous sections, there are three key types of CRVS IT systems namely: (i) Custom developed software i.e., where a software is built from scratch and specifically designed for the country requirements; (ii) Commercial off-the shelf software where a commercially available product can be purchased and modified to specific country requirements if needed and; (iii) Community-supported open-source software whereby the source code as well as the software product are freely available and there is an active community of practice to support the software.

In the CRVS domain, commonly, commercial off-the-shelf options are preferred over custom-developed software. This is because the functionalities required for IT systems for CRVS (despite country specificities) are broadly standardised across jurisdictions. Generally-speaking, it is in principle, more appropriate to procure an IT system that is already available and tested by other civil registration organisations (and therefore of a

certain maturity). Further, there is the guarantee that the supplier has experience in the civil registration domain, having supported previous implementations.

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 largely 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, which extends well beyond the costs of implementing the IT system (see Figure 2 for initial costs of implementation and Figure 3 for the operational costs).

IT vendor services	• Software licensing • IT system deployment and configuration • Data migration • Training • Documentation • Implementation support • Warranty
IT infrastructure	• Servers • Data storage devices • Computer networking equipment • Computers • Mobile devices • Printers and scanners • Third-party software licensing

Figure 2. Implementation costs

IT vendor services	• Software licensing • Post-warranty support and maintenance
Hosting	• Hosting of production IT system • Hosting of development, test and training IT systems • Hosting of recovery IT system • Storage of data backups
IT infrastructure replacement/ renewal	• Servers • Data storage devices • Computer networking equipment • Computers • Mobile devices • Printers and scanners • Third-party software licensing

Figure 3. Operational costs

Following acquisition is the contract execution stage which entails managing and coordinating all the activities associated with the fulfillment 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. Table 5 provides a summary of some of the steps that a country may follow leading to the execution stage.

Table 5. Key considerations for procurement

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. • After the EoI, the purchaser can make decisions about which contractual aspects are not negotiable (hosting, source code rights, etc.). • 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 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 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.

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.

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

APPENDIXES

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

1. General	2. Technical requirements
☐ Scope of Request for Proposal	☐ Functional requirements
☐ Request for Proposals process	☐ Non-functional requirements
☐ Eligible bidders	☐ Hardware compatibility requirements
☐ Required qualifications of the bidder	☐ Testing requirements
☐ Possibility for site visit	☐ Implementation schedule
	☐ Warranty, maintenance and support services required

3. Preparation of proposals	4. Submission of proposals
☐ Language of proposals	☐ Deadline for submission
☐ Documents comprising the proposals	☐ Late proposals
☐ Proposal price and currency	☐ Withdrawal, substitution and modification of proposals
☐ Period of validity of proposals	
☐ Format and signing of proposal	

5. Evaluation of proposals	6. Contract award
☐ Opening of proposals by purchaser	☐ Award criteria
☐ Clarification of proposals	☐ Notification of award
☐ Evaluation and comparison of proposals	☐ Contract negotiations
☐ How to contact the purchaser	☐ 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
- ☐ Periodic performance reviews
- ☐ Supplier's responsibilities
- ☐ Purchaser's responsibilities

3. Payment

- ☐ Contract price
- ☐ Terms of payment
- ☐ Taxes and duties

4. Intellectual Property

- ☐ Copyright
- ☐ Software license agreements
- ☐ Confidential information

5. Supply, installation, testing, commissioning and acceptance of the system

- ☐ Representatives of contractual parties
- ☐ Project plan
- ☐ Subcontracting
- ☐ Design and engineering
- ☐ Hardware delivery and transport
- ☐ Inspections and tests
- ☐ Installation and configuration
- ☐ Acceptance
- ☐ Handover

6. Services

- ☐ Training
- ☐ Warranty
- ☐ 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

Pacific Community (SPC)
B. P. D5 – 98848 Noumea Cedex, New Caledonia
Telephone: + 687 26 20 00
Email: sdd@spc.int
Website: http://www.spc.int – https://sdd.spc.int