Toward Universal Birth Registration

A Systemic Approach to the Application of ICT

EDITORS

Mia Harbitz and Kendra Gregson

unicef

IDB

Toward Universal Birth Registration

A Systemic Approach to the Application of ICT

Editors

Mia Harbitz and Kendra Gregson

unicef

IDB

Suggestion citation: Inter-American Development Bank and UNICEF. 2015. *Toward Universal Birth Registration: A Systemic Approach to the Application of ICT. Washington, DC:* Inter-American Development Bank and UNICEF.

Photo: © UNICEF/UGDA201400367/Vassie
Uganda, 2014
Mother of four, Mantume Christine holds her newborn baby girl outside the family home in Mityana District, Central Uganda. Her newborn daughter will today receive her birth certificate issued by the district hospital. With the help of a new Mobile Vital Records System (mobileVRS) scheme, initiated by UNICEF, Uganda has seen an increase of 18% in birth registrations within the last two years allowing children the right to basic health care services.

The Institutions for Development Sector of the Inter-American Development Bank was responsible for the production of this publication.

Production Editor: Sarah Schineller (A&S Information Specialists, LLC)
Editor: Margie Peters-Fawcett
Design: Word Express, Inc.
Proofreader: Sue Debowski

Contents

Acknowledgements

This publication is the result of the technical and financial collaboration of the Instituto para el Desarrollo Social Argentina (IDESA) under the leadership of Kendra Gregson from the United Nations Children's Fund (UNICEF), and Mia Harbitz, formerly working with the Inter-American Development Bank (IDB). The publication benefited from the expertise of Jorge Avelino Colina, Santiago Gastelu, and Liliana Alejandra del Carmen Torres of IDESA, as well as Sebastian Rohr and Silvia Knittl from accessec GmbH, who elaborated the technological framework.

A technical meeting on the topic identified the key areas to consider when developing the civil registry and using new tools and resources to enhance its effectiveness, thereby being the basis for this publication. The success of the meeting would not have been possible without the sincere commitment of all its participants to share their working knowledge and experience to improve birth registration. These were, in alphabetical order, Dieh Mandiaye Ba (Ministry of Local Governance and Development and Urban Planning, Senegal), Susan Bissell (UNICEF), Atif Ikram Butt (UNICEF), A.K.M. Saiful Islam Chowdhury (Local Government Division, Bangladesh), Edward Duffus (Plan International), Rudy Rosales Gallardo (Registro Nacional de las Personas, Guatemala), Luca Guanziroli (United Nations High Commissioner for Refugees), Abdelhak Harrak (Ministry of Interior, Morocco), Lourdes Hufana (Philippine Statistical Authority, the Philippines), Svetlana Ilescu (Civil Status Service Ministry of Justice, Moldova), Lukas Iseli (Federal Department of Justice, Switzerland), Neo Corneliah Lepang (Ministry of Labour and Home Affairs, Botswana), Zainab Mahmoud (National Population Commission, Nigeria), Dragan Mioković (Federal Ministry of Internal Affairs, Bosnia and Herzegovina), Chantal Nast (International Commission on Civil Status, France), Alex Njihia (Civil Registration Department, Kenya), James P'Okidi Okello (Kitgum District Local Government, Uganda), Rebeca Omaña (Organization of American States), Javier Ortega-Garcia (Universidad Autónoma de Madrid, Spain), Keiko Osaki-Tomita (United

Nations Statistics Division), Matthew Perkins (United Nations Economic and Social Commission for Asia and the Pacific), Ettienne Ravo (Civil Registry Office, Vanuatu), Carlos Reyna (Registro Nacional de Identificación y Estado Civil, Peru), Alexandra Rohrer (Etat Civil de Lausanne, Switzerland), and Anneke Schmider (World Health Organization). Many thanks go to Vivian Beetle, Peg Fraser, and Rebecca Gribble for diligently documenting the discussions during the consultation. This technical meeting would not have been the success it was without the tireless support of Sophie Flynn of UNICEF, and Tamara Menzi, Fleur Jaccard, and Ursula Eichenberger of Switzerland's National Committee for UNICEF.

This publication was further enhanced by the review of a distinguished group with specialized knowledge. Anette Forsingdal Bayer from the Namibian Ministry of Home Affairs and Immigration contributed her extensive operational knowledge in introducing information and communication technologies (ICT) into a civil registry. From UNICEF, Milen Kidane's work, supporting civil registrars, provided a practical application lens to the publication, and Kerry Neal contributed to the understanding of the legal implications of this technology. Robert Palacios from the World Bank contributed his unique expertise on ID-management. Finally, the IDB's Miguel Angel Porrua Vigon provided reflections on the application of ICT in civil registries.

Finally, the technical meeting and it contributions to this publication would not have been possible without the support of Switzerland's National Committee for UNICEF and the Anne Frank Fonds. Many thanks go to Elsbeth Müller, Executive Director of the Swiss National Committee, for her vision on the importance of birth registration to protect children. Buddy Elias, Chair of the Anne Frank Fonds, reminds us to 'hold out hope for our children' as we move forward to register the births of all.

Objective and Purpose

The objective of this publication is to analyze the legal, administrative, and technological requirements for the use of information and communications technology (ICT) for birth registration. The intended audience includes civil registry agencies or those countries that are considering the introduction of ICT, as well as those that already have the system in place. While many countries have already updated their civil registry frameworks to include ICT and while many are taking it into consideration, it is the authors' hope that the guidelines can also serve as a means to review current arrangements.

Guidelines and recommendations are lacking in terms of the use of ICT in civil registration, as well as its use in other information produced by the civil registries. This publication, however, will focus only on the registration of births, given the pivotal role that registration has in establishing the legal identity of an individual for the issuance of a birth certificate as a breeder document. While it is recognized that civil registration interacts with other branches of government, the focus of this document rests only on civil registries.

The Inter-American Development Bank (IDB) and United Nations Children's Fund (UNICEF) have identified a knowledge gap between the need and the capacity to design, develop, install, and operate ICT systems that will make the birth registration process more efficient and secure. This publication will identify and examine the potentials of ICT to support the birth registration process more efficiently, accurately, securely, and in a timely manner.

Civil registries should be based on a robust framework that includes definitions, governance, organizational structure, and the roles and responsibilities of those involved. Shifting from a paper-based to a digital registration environment can provide the opportunity to review the three basic institutional framework elements: the legal, administrative, and technological aspects.

A civil registry is not only responsible for birth registrations, but is also responsible for the registration of all other civil events such as adoptions, marriages, divorces, and deaths, including the issuance of certificates for each of these instances. This publication does not address the frameworks for efficient management of these other civil events.

This joint IDB–UNICEF publication provides the background analysis and a practical checklist for civil registries that are considering the implementation of an ICT system or are reviewing an existing system for the registration of births. It is expected to contribute to improve the efficiency of the registration procedures, as well as reduce the time it takes between (i) the birth and the legal registration of the child, and (ii) the legal registration of the child and the delivery of the certificate.

It is hoped that these guidelines will strengthen the right to immediate birth registration (United Nations Convention on the Rights of the Child, Article 7), as well as the right to be recognized as a person before the law (The Universal Declaration of Human Rights, Article 6).

Abbreviations

AES	Advanced Encryption Standard
API	Application programming interface
BCP	Business continuity plan
CA	Certifying Authority
CISA	Certified Information Systems Auditor
CMDB	Configuration Management Database
CMMI	Capability Maturity Model Integration
CRL	Certificate revocation list
CRUD	Creating, reading, updating, deleting
dba	Database administrator
dbo	Database operator
DRP	Disaster response plan
ERP	Emergency response plan
EU	European Union
FAT	Factory accepted test
GPS	Global Positioning System
GSM	Global System for Mobile Communication
GUI	Graphical user interface
http	Hypertext transfer protocol
ICAO	International Civil Aviation Organization
ICT	Information and communications technology
ID	Identification
IDB	Inter-American Development Bank
IDESA	Instituto para el Desarrollo Social Argentina
IEC	International Electrotechnical Commission
IMEI	International Mobile Equipment device ID
IPsec	Internet protocol security

ISO	International Organization for Standardization
ISP	Internet service provider
ITU	International Telecommunications Union
L2TP	Layer 2 Tunneling Protocol
MNO	Mobile Network Operator
MPLS	Multiprotocol Label Switching
MSISDN	Mobile Station International Subscriber Directory Number
OCSP	Online Certificate Status Protocol
PC	Personal computer
PIN	Personally identifiable information
PKI	Public key infrastructure
SAT	Site Acceptance Test
SIM	Subscriber identity model
SIT	Systems Integration Test
SMS	Short message service
SP	Service provider
SSL	Secure Sockets Layer
TLS	Transport Layer Security
UAT	User Acceptance Test
UN	United Nations
UNICEF	United Nations Children's Fund
USB	Universal Serial Bus (memory stick)
WAN	Wide Area Network
WORM	"Read once read many"
WPA2	WiFi Protected Access
WWW	World Wide Web

Chapter 1

Institutional Framework and Linkages for the Civil Registry

The steadily increasing recognition of and interest in the right to identity, as laid out in international treaties and operational issues pertaining to legal identity, is encouraging. A growing number of countries have invested, or will invest, in information and communications technology (ICT) systems for civil registration and identification, but the speed at which technologies for such purposes are evolving represents a challenge to many countries. The lack of recruiting and retaining the technical expertise and hence the capacity to adequately assess the different aspects that are required to upgrade, modernize, and maintain digital registration system can be particularly daunting for many countries.

In many developing countries, a considerable portion of the population is not registered at birth or otherwise recorded in the civil registry—often a prerequisite to be included in a civil identification registry and obtain a national identification card. Keeping in mind that new technology and policies are often geared towards e-ID methods, it is worth taking a closer look at the population's ability to obtain the necessary breeder documents, such as a birth certificate issued through civil registration, in order to obtain other identity cards and be able to access and manage online information and services. While civil registration systems capture the vital and civil events of a person's life, including death, marriage, divorce and adoptions, it begins with birth registration. ICT can be an enormously helpful tool to support more timely, accurate, and efficient birth registrations, as long as it is considered in light of the national policy environment, social and cultural norms, and other aspects of the civil registry.

The institutional location of civil registry and identification agencies varies from country to country. Common institutional homes for a civil registry are the Ministry of the Interior, the Ministry of Justice or the Electoral Tribunal, although they can also be autonomous (or semi-autonomous, such as Uganda's Registration Services Bureau) institutions, or be located in the Ministry of Education or Finance. Whatever

the institutional arrangement, countries need to establish clear legal boundaries for the identification, registration, verification, certification, enrollment, storage, transmission, and authentication of personal identity. At the same time, the institutions and administrations need to be strengthened to permit equal access to formal institutions, for example through the introduction of clear, built in control and monitoring mechanisms.

Under the umbrella of ICT, there are many possible options and devices, such as radio, mobile phones, satellite systems, and computer networks, as well as applications that can be useful for the timely registration of births. This publication will focus on the back-office considerations that can be applied to any of these ICT systems. The choice of system depends on the needs and environment of each country, and should be locally appropriate. In areas where there is scant or no electricity, it will make more sense to continue processing registrations and records in a paper-based environment. In areas with unreliable Internet connectivity, the solution may be to transfer information to CDs or memory sticks (USB), although this is not necessarily recommended.

Regardless of whether it relates to ICT and electronic records, the conversion from paper-based to electronic records may require legal changes and financial requirements to ensure smooth transition. Old paper records should be maintained for a specific period of time. Moreover, the issue of digital record storage (cloud or proprietary servers) should be addressed to ensure that a back-up system is in place for maintenance or in the event of a disaster.

Switching from a paper-based environment to electronic records will require financial commitment and investment. The determination of the investment and maintenance needs depends on a thorough understanding of the ICT specifications and operational obligations and necessities. However, the expected savings and efficiency that derives from this switch will have a positive impact on a civil registry's performance. It will also improve customer satisfaction. This publication will focus more on the needs relating to birth registration in a national context than on the financial investment of ICT.

Chapter 2

Legal Framework

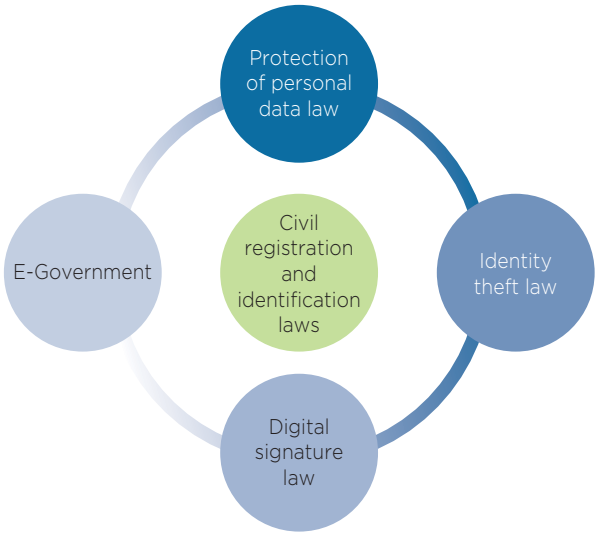
2.1 Introduction

National constitutions are based on a set of fundamental principles, according to which a country is governed, that limits the power of the state and protects the rights of its people. The objective of this section is to inform the development of a strong legal framework for civil registration that is efficient in terms of resources and is adaptable to societal and technological changes. The framework should build on a combination of international laws, standards, and principles that relate to civil registration, as well as national constitutions, laws, and regulations of the respective country. Although the principles and obligations may be generic, it is the laws and regulations therein that enable the establishment of a civil registry and its identification instruments (Harbitz and Arcos, 2011).

It is essential that the legal frameworks of civil registries comply with ratified international conventions, such as The Universal Declaration of Human Rights and the United Nations Convention on the Rights of the Child. National decrees are also relevant, such as those that relate to the protection of personal data and the application of e-government processes. Issues that relate to digital signature fraud, privacy, and identity theft should also be taken into account if they are not already addressed within the context of the law. Figure 2.1 illustrates the elemental structure of the legal framework for a civil registry. Civil registration law, itself, should center on the individual, since it fulfills the state's obligation to register and establish the identity of a child. The four basic legal instruments are the laws that pertain to the protection of personal and confidential information, electronic signature, electronic governance, and identity theft.

Before ICT is introduced for birth registration and civil registration in general, it is important to revise and, if necessary, upgrade the legal framework to support the use of ICT. For instance, older legislation may not have considered digital storage

FIGURE 2.1: Elemental Legal Framework for the Civil Registry



or electronic transmission of personal data. In many countries, ICT is on track to replace the tedious and obsolete processing and archiving of paper-based documentation relating to birth registrations. The affordability of ICT and the availability of modern broadband/wireless network coverage (including remote and rural areas) have influenced many countries to analyze new and more efficient methods to register birth events. ICT has the potential to provide fast data access and accelerate processing, and with the right applications in place, it will create a more secure environment to authenticate ID documents.

The process of registering births will need to be redesigned—or in some cases, reformulated—to ensure greater efficiency and accuracy when introducing ICT. The redesign should include the entire process of registration, from the birth event (point of delivery) to the point where it is archived at the civil registry. Although not a focus of this publication, all other civil registration processes should be redesigned or reformulated when an agency invests in ICT.

2.2 Legal Foundation

2.2.1 Establishment of a Registration System

While also reflecting the political structure, history, and traditions of a country, the legal basis for a civil registry must include the normative definitions, as well as those of the registration instruments. The law should incorporate the elements of the structure, as well as its functions and institutional characteristics, such as funding sources and the selection and appointment of appropriate authorities. The framework, as a whole, should allow for the flow of information, relationships between entities, and technical requirements. Elements of the registry structure should be consistent and include:

a. objectives of the registration system and the civil registry;
b. function of the civil registry: to record vital events (excludes registration procedures);
c. relationship with other organizations: the exchange of information (excludes directional flow or details of information);
d. electronic storage and transmission of personal data; (for storage, it must define whether to store the personal data on servers or within a proprietary cloud)

e. funding: alternative sources and procedures to obtain funding, in addition to the current (regular) funding structure;
f. methods of selection and appointment of chief executive;
g. responsibilities of civil registry personnel; and
h. sanctions system and adjudication process.

Establishing appropriate systems will differ from country to country. It is important to develop a legal structure that will adapt to emerging cultural changes, such as the increasing occurrence of extramarital births, same-sex relationships, in vitro fertilization, and surrogacy, as well as the particular naming customs of ethnic and minority groups. The introduction of technological changes can be challenging, especially when these classifications were not included in the original framework and when the framework has been written in such a way that it limits the materials used for registration. Examples include the stipulation that registrations be carried out "by means of an entry in a record composed of individual numbered pages" or that the "production of the birth certificate be done by hand in clear and legible handwriting."

2.2.2 Protection of Personal Data

Personal data is defined as the set of biographical information that is contained in a person's record. In the case of birth registration, it is noted that the minimal information required (United Nations, 1998) is the mother's identification and the date and place of birth, along with supporting documents (see Section 2.3). Additional information, as in the case of some countries (Botswana, Chile, Norway, among others), may include a unique identification code, personal number, and/or copy of the birth certificate, as well as the biometric data of the individual and/or his or her parent(s) (e.g., mother's fingerprint, fingerprint of an adolescent or adult registrant, as is the case in Uruguay).

It is crucial to ensure the protection of personal information that is collected through appropriate applications, whether it is in electronic form or paper-based, in order to prevent criminal offenses. When printing the copy of the registration, it is recommended that there is minimal information on it to protect the individual when presenting this document as identification. It is also recommended that the base material include a security substrate image using secure printing techniques and with a unique record number (UNICEF, 2013).

Unlawfully manipulating or falsifying official documents is common, worldwide. Fraudulent practices in relation to identification cards, passports, and other official documents (e.g., birth certificates) pose a risk to the individual and society as a whole. An array of methods and technologies, however, are available to prevent the counterfeiting of documents and to facilitate the identification of fraudulent documents. This, however, requires a significant amount of funding to prevent such practices from taking place and to be able to detect whether or not documents are legitimate. To ensure a sustainably secure environment, it is essential that due diligence is carried out and that careful planning and strictly audited implementation procedures are executed.

A civil registry collects and stores a vital set of people's personal data, which can be shared with third parties, such as other government ministries. One of the responsibilities of the civil registry is to validate and verify the identity of the individual when providing public services, such as healthcare, education, and social and municipal services. In some countries (e.g., Mexico) it is legal to share such information with private entities (e.g., banks, insurance companies, credit card institutions, telephone services), whereas other countries (e.g., Peru) limit this interaction to a binary verification of the information provided or collected by the third party. The law, therefore, must specify the procedures by which third parties can request information and what information can be shared, verified, or authenticated on line. The law to protect such data, unfortunately, is outdated, obsolete, or nonexistent in some countries. The essential principles of the protection of personal or confidential data that should be taken into account when introducing ICT for birth registrations include the following:

a. **Aim:** The flow of data information should legally protect the individual's private data and its ultimate use. In other words, the law must protect what is personal and confidential and is maintained in files, registers, databases, and other technical means for data processing—whether in the public or private domain—in order to guarantee the individuals' right against its unwarranted use.
b. **Purpose:** Data can be shared only with an authorized third party and only if it relates to the purpose for which the data is collected. The law should clearly establish who can access it and the purposes and limitations for which the civil registry gathers the data.
c. **Appropriateness:** The request for data should be according to legal established procedures.
d. **Legality:** The communication and storage of data must be securely managed to avoid misuse or fraudulent practices.
e. **Veracity:** Data must be protected against unauthorized tampering; secure procedures should be in place for the updating of information (e.g., data should be inputted correctly and errors should be amended) and all necessary changes should be recorded. Only authorized individuals should be empowered to make changes to information that is held, following the instruction in the legal framework.
f. **Previous consent:** In general, the processing of an individual's record requires the individual's consent. It should be stipulated in the laws of the civil registry, therefore, that the information of an individual that is shared with a third party has the prior consent of the individual, and that it is shared for legitimate purposes. If a mechanism to opt out of information sharing is considered within the law, it must be made clear to the individual.
g. **Security:** The organizational and technical requirements to safeguard the confidentiality, integrity, and access to civil registries should be taken into account (see Section 4.6).
h. **Rights:** The individual should be entitled to act against any unlawful management or misuse of his/her personal data. (S/he

should be assured of his/her right to privacy); transparency of data; and ability to petition for the rectification or destruction of incorrect or unreliable data. Furthermore, a constitutional remedy, known as *Habeas Data*, should provide the individual with the knowledge of what information is being held by what party.

i. **Data management responsibilities:** Data users must adhere to the purpose for which the data has been requested. For instance, only identity data must be used to verify an individual with whom the requesting third party has a relationship.
j. **Controls:** Systems must be in place to detect any deviation or fraud in the management and use of personal data or records.
k. **Sanctions:** Misconduct must be documented and administrative or criminal sanctions must be defined for those who violate these principles.

2.2.3 Digital Signature

A digital signature is a mathematical technique that validates the authenticity and integrity of a document that is sent electronically. It has the same power as a written signature. The technical characteristics of digital signatures are discussed in Chapter 4 (Sections 4.11–4.13) while, in the meantime, this can be described as an asymmetric key operation that encrypts the private key that is used to digitally sign an electronic document at one end and the public key that is used to verify the signature at the other end.

An ICT network can improve the security of birth registrations, particularly in the event that a third party reports a birth (e.g., a birth attendant). A digital signature can capture the identity of the reporting party and his/her authorization to notify the civil registry of a birth event. Laws that permit third-party digital signatures must ensure the identity of the parties, and include the following:

a. The legal weight given to a digital signature should be the same as that of a handwritten one.
b. The issuance and validity (life span) of a personal digital certificate with private information (known only to the signatory as a private key) should be regulated. The digital certificate, itself, is an electronic document that is issued and digitally signed by a Certifying Authority (CA) that links the owner to the third party requesting the certificate.
c. The CA acts as the Trusted Third Party and should be managed by a legal entity that has a license to issue and maintain the certificates, so that the CA acts as the validation link between the two parties. The guarantee of the CA is essential in the case of both parties.
d. A procedure should be developed to validate a digital signature in cases where the individual is not able to register, as in the case of a mother delivering a baby. This can be achieved by adding a Trust Anchor (e.g., birth attendant), known as a Root CA, to the list of trusted certificates.

There may be no requirement for government-operated civil registries to issue CAs. Given the high cost and effort that is involved in establishing and maintaining the necessary security infrastructure for CAs, it

may be more cost effective to procure the services of a qualified provider.

2.2.4 Characteristics of Identity Theft

Identity theft is defined as the unlawful appropriation of the identity of an individual. An individual or organization can use this appropriation (public or private) to commit proprietary crimes and assume control over assets and property. It can also be used to cause moral harm to the person whose identity was stolen.

Identity theft is most often associated with online transactions, although it can also occur in the scope of paper-based registers and documents. The increase in such crime, however, is due to the advancement of technology and the growing use of social networks and electronic retail, banking, and credit/debit card transactions. The more digital transactions there are, the more opportunities there are for this type of crime.

There are four key elements that characterize this crime: (i) **commodity:** information of the stolen identity; (ii) **offence:** means by which the information is obtained; (iii) **purpose:** intention of the offence; and (iv) **authorization:** the victim's lack of it. The laws of a civil registry should define identify theft and include the necessary interventions or penalties:

a. **Definition of identity:** A unique set of features and characteristics that individualize an individual, including the name and other biographical data (IDB, 2015). In contrast, a digital identity is defined as a set of attributes that form the digital representation of a person in an ICT network environment, which can be converted to an alphanumerical string.
b. **Stages:** The stages that lead to the offence need to be determined. According to literature, there are four stages:
   - Stage 1: Preparation of methods to capture personal information for the intended identity theft (e.g., design of an illegal software that will enable the seizure of passwords);
   - Stage 2: Capture of information that is related to the identity;
   - Stage 3: Transfer of the stolen information; and
   - Stage 4: Actualization of the fraud (the harm).
c. **Victim's informed consent**: The criminal acts without the informed consent of the individual(s) concerned.
d. **Dishonesty:** The intention of the person to steal the identify information as a means to cause harm.
e. **Sanctions:** These must be defined and should be incorporated into the legal framework or within the confines of current penal regulations, according to the type of offence(s) committed.

ICT networks now provide applications to improve data storage and the processing of personal records. Without appropriate safeguards in place, the risk of data hacking and abuse can be extremely high, especially within systems that can process millions of identity records in a split second and when conducting mass-data analyses (Big Data) on public and private datasets. Protecting the digital identification of an individual is

crucial, since inappropriate use of online identifications (ID) can lead to severe financial and personal damage to the individual. Appropriate legislation, therefore, should protect a person's ability to use online services and his/her digital identification.

The legislation must also result in guidelines and manuals to mitigate risk of identity theft or misuse of personal information. The mitigation procedures must range from authorized access to civil registry records; and the use of passwords or other techniques to authorize access to system protection protocols and firewalls.

2.3 Procedural Framework

2.3.1 Registration of Vital Events

The normative framework defines the registration process, those responsible for it, and the documents required. The procedural framework, usually detailed in an operation manual, describes the process for the practical application of the law. Each process should contain the (a) name of the process, (b) purpose or event, (c) authorized person(s) to report the event, (d) documents to be submitted by the registrant, (e) officer(s) responsible for the process, (f) authorizing offices of the civil registry, (g) content of a birth record; (h) document to be issued, and (i) documents for archiving. In the case of a birth event, the process would include the following:

a. **Name of the process**: birth registration.
b. **Purpose:** registration of the identity of the individual and issuance of a birth certificate.
c. **Person responsible for the process:** legal guardian(s), as defined in the national legal framework (mother, mother and father, etc.).
d. **Required documents** (including the registration submission):[1]
   - ID of the mother or other legal guardian and
   - medical certificate of live birth.
e. **Officers responsible for the process:** those who are authorized to process registrations.
f. **Authorizing office of the civil registry:** the officer of the civil registry—legally authorized to approve or authorize.
g. **Content of a birth record:** name of child, date of birth, place of birth, name of parent(s) (or legal guardian), sex. A folio/registration number is allocated by the civil registry and entered into the record and a unique identification number may be assigned at this stage.
h. **Document to be issued:** first birth certificate, with unique registration number, free of charge.
i. **Documents to archive:** supporting documents of the mother, father (if identified), and the medical certificate of live birth, record of foundling, as described by the law.

[1] Optional documents, which may be collected but should not deter the registration of the child:
- ID of the father or individual named as co-parent (if s/he is identified);
- marriage certificate if parents are married; or record of civil union contract;
- a third person with an accepted ID is permitted to act as a witness in the event the birth has taken place outside the formal healthcare system.

Additionally, the normative framework to amend names, surnames, and sex should be considered, and the ICT system must be designed such that there is a record of change in the individual's record. The recording of an event must be designed so that notes can be made in the event information cannot be provided. For instance, if the father is unknown, the record should indicate that, rather than be left with a blank field.

There are many vital events for which civil registries can collect related information. Some of this information may directly support the identification of familial relationships. These events include:

a. birth of children (given names, surname);
b. marriage and/or civil union contract (with or without surname changes);
c. divorce or dissolution of civil union contract (with or without surname changes);
d. adoption (given name and/or surname changes); and
e. sex change (gender identification)

The following additional activities are optional and may be carried out by an authorized agency (e.g., civil registry, civil identification agency, ministry, police, or other, as specified by national decree). These include:

a. issuance of a unique identification number;
b. issuance of a national identity card;
c. issuance of a national/regional identity (usually together with an ID card);
d. issuance of a passport that is compliant with the biometric features stipulated by the International Civil Aviation Organization; and
e. change of address.

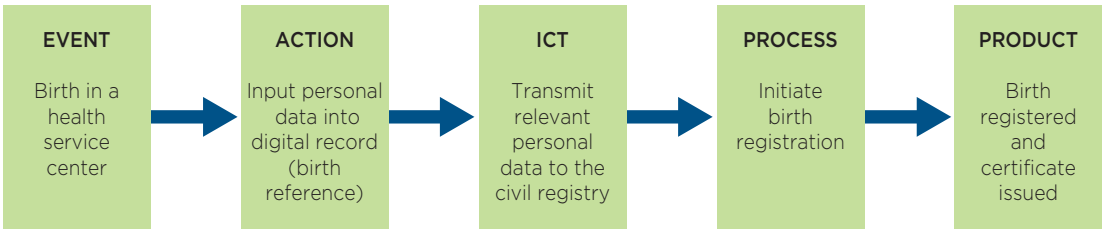
2.3.2 Registration upon Birth Delivery

Ideally, a birth should be registered the moment a baby is born. ICT can support the registration of children born in public or private healthcare centers (as illustrated in Figure 2.2), as well as those born outside of these centers (e.g., directly online or by mobile phone). The information that can be transmitted can include, at a minimum, the following data: time, date, place of birth, and sex. This set of data is known as a "birth reference".

In remote areas, when the delivery occurs, the person in charge (obstetrician, midwife) or some official close to the point of delivery (social worker) could use a mobile phone to alert the registration authorities by sending a clearly structured (predefined) message to a Registry Address including at least the following data: time, date, place of birth and sex of the newborn. This set of data is known as a "birth reference".

The birth information can be transmitted online, offline, or by mobile application. Online transmission requires sufficient national technology infrastructure that allows for high speed Internet connection. Where this is not possible, offline registration can be done by submitting the information in batches as and when Internet access is possible. Submitting the records in paper format or on electronic storage devices, such as USBs or an external hard drive, that are transferred to a central unit are less desirable and more precarious

FIGURE 2.2: Application of ICT with Regard to Birth Registrations in Health Service Centers



methods. (See Section 4.14 for the technical aspects of a mobile phone.)

In using a mobile phone, one methodology is to use a unique directory number that identifies a subscription to a mobile telephone network (MSISDN). The notification of birth can be transmitted by mobile phone by an authorized person on a pre-formatted template, followed by submission in person of the paper medical certificate of birth at the civil registry. In the absence of this document, the authorized person can simply state the date, time, and place of the birth, at which point the mobile message is identified by the registry, where it is transferred into digital form. Additional information relating to the name of the newborn and the authorized person is also entered at this point, preferably with evidence of an ID card or similar. The relevant dataset is then automatically updated or amended and the authorized registrant is provided with a reference number relating to the digital birth certificate that can be issued to the family (see Section 4.14).

It is essential to take into account some key factors. First, the reference of the digital birth certificate, issued by the civil registry, does not replace the medical certificate of live birth, which the midwife or healthcare professional must complete. In fact, the birth reference substantiates the medical certificate of live birth. Second, the person transmitting the notification alert by mobile phone must be an authorized agent, registered at the civil registry and supervised for proper use of the mechanism.

2.3.3 ICT Implementation in a Civil Registry

The application of ICT within the civil registry will enhance the process of registrations, include the following: registry address including, at least, the time, date, place of birth and sex of the newborn. This set of data is referred to as a "birth reference".[2]

a. **Name of the process:** electronic birth registration;

[2] A birth reference is defined as a set of data used to report a birth that occurred outside of an authorized healthcare facility, such as place, time, date of the birth and sex, along—if possible—with the identity of the parent(s), reported by a third party who possess a legal identity.

b. **Purpose:** to generate a digital record of the identity of the individual and of the birth certificate;
c. **Authorized applicant to start the process:** the authorized agent as defined in the national legal framework (mother, mother and father, legal guardian, etc.);
d. **Documents required**, including the registration submission:
    - mother's ID (electronic authentication);
    - birth notification (already registered at the registry);
    - father's ID (if he is identified) (electronic authentication); and
    - marriage certificate of parents (electronic authentication).
e. **Responsible officer:** only the officer(s) authorized to process the registration;
f. **Registration approval:** the registration process of a birth event begins and ends in the office of the approving officer;
g. **Registration information:** validation of mother's and child's name, date of birth, place of birth, and sex; addition of father's name. At this point, a unique identification number may be assigned;
h. **Document to be issued:** an original birth certificate in paper form and a digital print of the birth certificate; and
i. **Archive:** supporting documents to be filed (e.g., those of the mother and father (if he is identified) and birth reference data.

To facilitate ICT processing, the laws governing the structure and organization of a registry must not obligate the institution to only store documentation in paper form. It should be sufficiently flexible to enable digital storage.

2.3.4 Corrections to and Amendments of Data

The normative framework should include the necessary procedures to correct registration errors and rectify omissions. Generally, there are two types of procedures to do this within a database: administratively, by order within the civil registry; and judicially, whereby the judge intervenes and compels the civil registry to make the correction.

The administrative order should be speedy, flexible, and less bureaucratic, especially designed to allow for swift and easy correction—within appropriate procedures—of minor and easy-to-prove errors or omissions that emerge within a record or as a result of a comparison with other public records. The norm should allow for the correction to be made by an authorized individual, either as part of the processing of data or as a request from the interested party, the latter of which should be addressed to the registry's highest authority with supportive documentation. An opinion from the legal department of the civil registry should be sought, followed by an administrative decision that permits the change to be made to the registration. When the correction is deemed structural (i.e., a request to change a name, affiliation, place, or date of birth), the decision must be made by judicial procedure, which is more comprehensive, since it requires a greater comparison of documents, evidence, testimonial assessments, and a resolution by the court. In both cases, the corrections are usually processed on a hard copy. By applying ICT, the efficiency of the procedures can be increased by digitalizing the processes.

BOX 2.1

ICT Support for Correction and Modification of Records

A digital record enables a registered individual or person to access, by way of an e-government application, his/her personal data that is stored on a civil registry database—either for validation purposes or for use by a third party agency. Should the individual discover that the corresponding dataset is incorrect or there is missing information, an update or amendment can be requested online through an electronic self-service mechanism. The individual will be asked to provide personal identification by way of a unique identification number or authenticate himself/herself by providing a password or a digital certificate (if the latter has been provided with a Personal Identification Number (PIN)). The online request transmits to the civil registry for processing, and a new certificate can be emitted.

2.3.5 Exchange of Information

The exchange of information should be defined within the framework and the practice should be implemented in order to use, verify, and improve the quality of data. The term is usually associated with mitigating the risk of loss of information. Implementing institutional interoperability depends not only on the technology itself; it also depends on having a sound legal framework that is secure, private, and accountable.

E-government allows for three types of interactions. ICT design considerations for these are further discussed in Annex A. What should be noted is that for a government registry to function electronically, it must be based on interconnected registries that have a secure level of authentication (i.e., features on identity cards), including a legal framework to support the management of people's identities. E-government is usually open only to citizens of a country, yet the civil registry is responsible for all the vital events that take place within its territory, regardless if it is an event of a citizen or not. Sometimes the e-government system does connect with the civil registry specific for a country's citizens.

1. **G2C (government to citizen):** when one of the parties of the exchange is the citizen;
2. **G2G (government to government):** when both parties of the exchange are government bodies;
3. **G2B (government to business):** when one of the parties of the exchange is a private legal entity.

In order to exchange information effectively and beyond technological means, it is essential to have a sound legal framework. Within this, the following characteristics should be defined:

a. objectives of the information exchange
b. form of the exchange
c. parties with which the civil registry is authorized to initiate the exchanges
d. definition of the data that can be exchanged between the parties
e. understanding by the user of the difference between the request and the service provided

f. obligation of the civil registry to act, by virtue of office, when a user reports an inconsistency or a missing registration
g. obligation of the civil registry to charge an appropriate fee for the service provided (see Section 3.1.3)
h. obligation of all parties to comply with the foremost principles of privacy, good faith, and accountability

Prior to exchanging information with an entity, the civil registry should assess the entitlement of the entity to request the information. In order to make the exchange, there should be a mutual understanding by the registry and the party of the following:

a. semantics of the information with respect to language and the software used
b. precise details of the data that will be exchanged, as well as the required frequency
c. method of exchange
d. assurance of technical compatibility between security systems and measures to preserve the authenticity, integrity, and confidentiality of the transmission
e. hardware conditions and monitoring routines
f. procedures to follow should there be an instance of inconsistency in the registers or the discovery of no record
g. conflict resolution process
h. payment for services
i. acquisition description to make the exchange between the parties possible
j. validity period of the exchange agreement
k. revision procedures
l. annex describing the institutional interoperability (see Annex A).

2.3.6 Communication Strategy

Using ICT for birth registration will require the acceptance of all stakeholders. This includes those who implement the new technology as well as those who will use the service. There may be reluctance to use an unfamiliar tool, leading to a lack of trust in the technology and in the use of captured data. Photography may not be welcome in a community, for instance. There may also be some hesitation if the profile of the job is changed, raising concerns that it may jeopardize a person's chance of employment. It is, therefore, important that all personnel are informed and are provided with the capacity building that is necessary for this technology. Stakeholders also need to understand that ICT will enable people to access the registration process and provide them with the services and benefits for which they are eligible. They will need to recognize that ICT will improve the registration process. Some countries, therefore, have developed a communication and information strategy that has been adapted to reach those communities where underregistration is common.

In Peru, information has been widely shared on the importance of and the need for identity documents. The information has been translated into various indigenous languages and is disseminated among communities in coordination with other public agencies that provide social services. The law requires that anyone receiving government benefits have the right to

a government-issued identity document. On market days, the National Agency for Identification and Civil Registration (Registro Nacional de Identificación y Estado Civil (RENIEC)) offers real-time, online registration services, together with legal advice in the case of late registration, where an identity needs to be (re) established. Birth certificates are issued immediately when the parent has an ID card.

Legal Framework Checklist

Have the following issues been considered?

- **Adaptability**: generate a legal framework that can introduce cultural, societal and technological changes as soon as they appear.
- **Compliance with ratified international conventions:** the Universal Declaration of Human Rights and the Convention on the Rights of the Child must be taken into account in every legal framework.
- **Legal foundation:** a framework that incorporates the registry structure.
- **Protection of personal data:** birth registration data is sensitive information and should be guarded. With the inclusion of ICTs in the process, emphasis has to be made on the need for security, which includes consideration for confidentiality, integrity, and availability (see Chapter 4 herein).
- **E-government–digital signature:** if the government chooses to provide information and services through ICTs, a regulation of the digital signature in order to provide legal validity to e-procedures should be provided.
- **Characterization of identity theft:** to mitigate risk of misuse of personal information.
- **Birth registration procedures:** definition and classification of all the procedures that take place in the registration offices. These regulations make it possible to answer the questions of what, who, when, where, and how procedures are made.

Chapter 3

Administrative Framework

The registration process depends on the consistent application of standards and procedures, qualified humans resources, adequate infrastructure, and sufficient financial resources. It can be particularly challenging when the civil registry is linked to political cycles and officials may be transferred at random intervals, given that the operation and management depends substantially on specialized training and knowledge.

This chapter will identify and provide a listing of the minimum administrative requirements for the sound management and supervision of a civil registry. The considerations relate to the interconnection and interoperability between local civil registry offices with their headquarters, as well as to the interoperability with other public agencies.

3.1 Management Capacity

The introduction of ICT can facilitate the birth registration process, although the training and knowledge required to use and operate the system will demand more specialization. The management capacity must be clearly defined, as must the potential risks associated with running and supervision of the registry, both at the central and local levels.

3.1.1 Profile of Human Resources

To ensure that an ICT environment will offer a high quality of service, an organizational chart that defines the roles and responsibilities of staff should be developed. This should be supported by a manual that includes a detailed description of the position and the required skills and experience. Qualified employees should be recruited within the rules and regulations of human resource management.

To maintain a talented pool of employees, civil registry wages should compete with those in the labor market and staff should be offered stability and opportunities of job mobility.

Job descriptions can strengthen management practices and guide managers who are in a supervisory capacity. Each job description should outline the responsibilities of the employee and the tasks of the position. A performance evaluation process with appropriate criteria should be established to provide staff with the opportunity for promotion and job mobility. The job descriptions should include:

- Identification:
  - name of the position
  - location
  - immediate supervisor
  - subordinate positions
- Definition of the position: objective and nature of the job
- Functions and expected outputs
- Requirements of the position
  - education—academic level
  - certificates (ICT, security, project manager, accounting, procurement, etc.)
  - work experience
  - specific knowledge
  - other requirements
- Working conditions
  - facilities
  - technical tools for the position
  - level of responsibility
  - working hours
- Relationships with others
  - internal suppliers
  - external suppliers.

On the basis of this description, the civil registry will be able to define the administrative requirements of the human resources department as follows:

a. Selection of personnel
b. Career planning
c. Performance evaluation
d. Training
e. Remuneration.

The manual should include the concept of professionalism and ensure that each job is commensurate with the academic requirements of the position. Some positions (e.g., registration, analytical, and ICT management) will require a technical or university degree. To develop a pool of talent will require continuous and, sometimes, extensive training. This is possible through technical and personal development programs that overlap or intersect in terms of their objectives. Personal development can have an impact on the development of the civil registry.

With regard to technical development programs, by enhancing the competencies of employees and incorporating new procedures and technological changes, civil registries will increase their efficiency and be able to develop new services. To employ an ICT system will require continuous training—approximately 50 to 60 hours a year for each employee—in order to maintain a high standard of efficiency. By investing in the training of staff through technology and personal development programs, civil registries will be able to maintain professional, up-to-date, and motivated staff.

In terms of ICT personnel, the role of Service Manager should be highlighted. The

Service Manager is the professional who is responsible for organizing and supervising the IT department or for liaising and monitoring in the case of outsourcing. The Service Manager should be a highly qualified professional who understands the entire structure and each process of the civil registry.

3.1.2 Back-Office and Front-Office Infrastructure

The design of the infrastructure of a civil registry must take into consideration the following three aspects:

- employees should be offered the necessary requirements to enable them to comply with back-office procedures;
- individuals/users in the front office should be offered privacy and be made to feel welcomed and comfortable; and
- individuals should be able to access the civil registry, especially those with a physical disability, and may use a wheelchair, as well as those who are blind.

The back-office infrastructure requires:

- adequate space for furniture, hardware and equipment, human resources, and archives;
- adequate working conditions (climate control and staff security);[3]
- a business continuity plan (BCP), disaster recovery plan (DRP), and an emergency response plan in terms of risk analysis and mitigation; and
- an in-house primary operational data center and a secure backup center in a remote location for ICT infrastructure.

The front-office infrastructure requires:

- sufficient space for the public and customer service employees;
- a feeling of comfort by the public in the waiting area and by customer service employees;
- BCP, DRP, and emergency response plan (ERP) in terms of risk and mitigation.

To ensure that the front and back offices remain fully operational, at least 10 percent of the annual budget should be put towards maintenance and repairs, according to a 10-country survey.[4] A civil registry should have within its structure a department that is responsible for the daily routine of monitoring and maintenance. This service can also be outsourced.

So that individuals and families have access to the services of a civil registry, it is recommended that there is at least one permanent office with a personal or digital service (e.g., ATM, electronic kiosk) for every 100,000 inhabitants.[5] The offices should be geographically distributed so that the largest regions of the country are

[3] An example includes locks or electronic access control systems on doors to protect valuable documents and papers. A policy relating to who has access should be in place.

[4] IDB project RG-T2020, Good Practices in Civil Registries, recommends a minimum requirement, based on the interviews of 42 registrars at the national and subnational levels.

[5] To establish an optimal quantity of offices in order to efficiently fulfill the services of a Civil Registry may prove inaccurate. Thus, a minimum number of customer service offices is indicated. In the last decade, there has been substantial implementation of ICT systems in the public sector so as to

included, with strategic ones placed where there is a likelihood of nonregistration. They should also be located near hospitals with maternity wards, schools (for those children who are not yet registered), and social assistance centers (i.e., areas where families and their children congregate).

Mobile offices may be set up in those small or isolated towns where the cost of a permanent office may not be justified or, alternatively, virtual registration can be offered. The latter solution can relate to registrations within the healthcare and educational systems, or in the case of isolated groups, such as refugee camps, or where ethnic groups or immigrant populations reside due to integration issues.

3.1.3 Financing Arrangements

The cost of transitioning from a paper-based environment will require additional resources, financially and administratively. To introduce, upgrade, and maintain ICT will require resources. It may also require an adjustment to the distribution of funds within the budget. As with other public and private institutions, a civil registry requires resources to fulfil its mandate, improve the quality of existing services, and/or provide new services. The introduction of ICT for civil registration requires substantial financial investment. However, a detailed discussion of the financing arrangements and structure is beyond the scope of this publication given that it would prove difficult to address only the financing requirements for birth registration.

The fact that a registry does not have the characteristics of a conventional public good will prove challenging in the search for resources, despite it being a state service *par excellence* (only the state can certify a person's identity). Conversely, since the services it offers to the individual or third party entity must be prevented by the registry from being used by other individuals or third parties, the registry can impose fees, thus reflecting the characteristics of private goods. Furthermore, the exclusion principle that applies when one individual or entity prevents the other from using the information enforces that the registry can be viewed as a private good. These two characteristics illustrate that the civil registry is, indeed, able to charge fees for services and thus generate its own resources.

Civil registries, therefore, have three financing alternatives: (i) own resources; (ii) resources from the government budget; and (iii) resources from international organizations. Each of these sources may or may not be available to a civil registry, depending on the economic, administrative, and legal conditions of each country, province, or municipality. The advantages and disadvantages of each alternative are evaluated below, and a summary of options and considerations is provided in relation to financing mechanisms that are appropriate for a civil registry.

make it easier for society to access the services for which they are eligible without having to physically access the relevant offices. A practical distribution of registration offices can be one per 100,000 inhabitants. The calculation is based on a rate of about 20 birth registration on average per office per week. According to the World Bank (2015), the highest birth rate in 2013 was nearly 50 births for every 1,000 inhabitants over an estimated average of 250 working days.

The folllowing focuses on the financial implications and mechanisms in relation to birth registrations and the provision of relevant certificates. At the same time, the recommendation for providing the service for free will be borne in mind.[6]

3.1.3.1 *Own resources*

The generation of own resources signifies that the civil registry must calculate a fee for each service that it provides. The rate is calculated by estimating the sum of all the expenses (current and capital) that the civil registry makes to produce a quantity of services, divided by the number of services, thus resulting in a per unit cost (fee).

The services that can be priced include the vital event registrations (including the issuance of event certificates) and the provision of information to public and private organizations. Both require a separate analysis.

With regard to vital event registrations, the civil registry must ensure the registration of all births, with the issuance of birth certificates. Given its importance, birth registration is a procedure that should be free of charge to the public. If the cost is charged to a public entity, the amount should be calculated by basing it on the quantity of procedures carried out, multiplied by the unit cost. This will avoid the need for an ad hoc budget and the civil registry will have its own source of income and will still be able to provide the service free of charge to the public. This rate scheme can also be applied in the case of divorce and death registrations. In cases where individuals, themselves, seek the services of a civil registry, such as requesting additional copies of certificates of any event, a fee can be charged for each process.

In sum, each service should be priced. A fee may be charged to the public if they request duplicate certificates. Alternatively, the cost should be charged to another public organization when the recording of events is in the interest of the state, as is the case for births and deaths.

Some countries (e.g., Chile, Rwanda, Brazil) have worked out a system of "cross-subsidies" from other agencies or registries to be able to provide free birth registration and a free first birth certificate.[7]

In terms of providing information at the request of other public or private organizations, the stipulation should be to charge the third party for the amount of the data received. Public organizations may represent healthcare, education, social security, police, migration, and electoral services, while private entities can be banks, financial institutions, insurers, utility services, and real estate companies, among others.

Furthermore, it should be taken into account that the fee charged for providing

[6] Human Rights Council, Resolution A/HRC/28/L.23, unanimously adopted in March 2015 (United Nations General Assembly, Human Rights Council, 2015). "Further calls on States to ensure free birth registration, including free or low-fee late birth registration, by means of universal, accessible, simple, expeditious and effective registration procedures, without discrimination of any kind." The *Implementation Handbook for the Convention on the Rights of the Child* (UNICEF, 2007) states that birth registration should be free. It also states that fines or charges for late registration are counterproductive and a hindrance to birth registration.

[7] The "Convention on the Rights of the Child" (UN, 1989) states that birth registration should be free. It also states that fines or charges for late registration are counterproductive and a hindrance to birth registration.

information is different from that applied to the registration of vital events. To calculate the information fee, the sum of the current and capital expenses that the civil registry must have in order to provide a service of high quality to those seeking identification data is divided by the amount of data provided. The more demand there is from the public and private organizations that seek that data, the less the fee will be.

The fee charged for releasing information may cover the cost of registration processes. As such, the third parties (public and private organizations) that seek to verify vital events would co-fund the registration service.

The advantages of civil registries having their own resources include:

- ability to maintain stable financial resources, increasing at the same rate as expenses;
- bonus schemes for personnel can be implemented, dependent on the number of services and the volume provided;
- potential for financial independence by not having to rely on the political decisions of ministries or higher levels of government;
- potential for a yearly budget and the ability to estimate costs and investments with more accuracy.

The disadvantages are:

- the resulting fee may result too high for certain procedures, especially for low-income citizens;
- a more complex, electronic accounting system may be needed;
- a highly trained staff will be required in all relevant positions; and
- there may be a need to cover possible deficits.

3.1.3.2 *Resources from national or subnational budget*

The central or subnational government budget is an alternative funding source for a civil registry, whereby the civil registry would have its own budget, approved by parliament each year. The budget would be based on estimates calculated by the civil registry and would be dependent on the budget of the state treasury.

For transparency and governance purposes, the civil registry must prepare, each year, a proposed plan of activities with an estimate of the resources required. The transfer of funds depends on the governing economic authority—usually the ministry of finance or budget secretary—and whether there are available resources for the registry. The advantages of this type of financing are:

- there is no need for a complex accounting system, since the budget does not depend on production;
- there is income stability, since funding is automatically transferred each year; and
- free-of-charge services can be applied, given that the resources originate from a third party.

The disadvantages are:

- lack of incentives for employees, as the income flow is not related to efficiency or volume of services provided;

- risks of underfinancing due to:
  - political differences between civil registry and other authorities;
  - low capacity to lobby within the confines of the public sector budget;
  - potential for a government fiscal crisis; and
  - rising inflation, leading to a shortfall in resources.
- potential loss of efficiency and effectiveness on the part of the registry due to lack of incentives and risk of underfinancing.

Civil registries in many countries depend on another government agency for their funding resources. While there are no further advantages to those listed above, there is one additional disadvantage: the potential for struggles between the funding body and the civil registry.

3.1.3.3 *Funds from international agencies*

The lack of resources, low institutional capacity, disinvestment and/or a drop in the quality of the services may offer an opportunity for civil registries to access special funding through international development organizations—usually classified as technical cooperation (nonrefundable)—or from government debt under favorable conditions. These avenues are generally considered unusual and more appropriate for institutional investments and improvements, rather than running costs. The advantages of external financing are the following:

- ideal for long-term investments, as they involve large amounts which can be repaid under favorable conditions;
- financing can be combined with technical capacity building and logistical support; and
- provides political independence, since funds are specifically allocated to the civil registry.

The disadvantages are the following:

- not all civil registries can access this type of funding, since countries may face resource challenges or may prioritize other types of investments;
- approval from other government bodies (e.g., ministry of finance, Office of the President) may be required, despite the fact that there is no political risk; and
- funding is complementary due to their extraordinary nature.

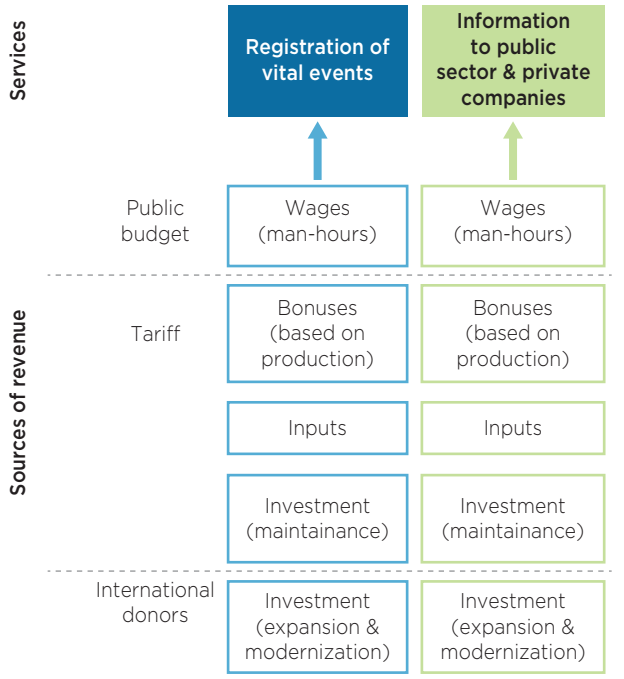
3.1.3.4 *Summary of financing options*

The previous analysis suggests that the disadvantages and advantages of the three sources of funding can complement each other rather than act on their own. Based on this, a funding scheme can be structured as follows:

a. **Fees:** finance based on production, with the capacity to compensate employees for their work;
b. **State budget:** provides revenue stability;
c. **Funding from international development organizations:** ability to access loans for technical capacity and improvements under favorable conditions.

The ideal financing scheme should be structured in such a way as to take

FIGURE 3.1: How to Organize the Financing Scheme for the Civil Registries



advantage of the benefits. Figure 3.1 illustrates civil registry services and the funding needed to carry them out.

With this financing structure, wages would be stable, since the funding would originate from the public budget, providing the appropriate legal framework corresponding with public employment policies, which tend to remain constant (e.g. productivity incentives through a bonus scheme, investment in inputs and maintenance by way of fees). Furthermore, the favorable conditions and potential technical capacity offered by international development agencies would enable the implementation of new systems.

3.1.4 Strategic Business Plan

The importance of having a strategic business plan is often underestimated. It should be a part of the operational plan, providing the basis for future planning and serving as a tool to monitor activities taking place. It also takes into account the deviations that have occurred and the reasons for them.

One of the activities that falls within the responsibilities of a strategic business planning office is the development of indicators for monitoring purposes. With the introduction of ICT, the impact of this on the registration process is important to manage and to monitor. Examples of queries that may help develop the plan include:

a. How is the civil registry operating as a whole?
b. What processes are required to detect potential issues?

The business plan would also be clear on the introduction of ICT. It is proposed that the transformation process should start by introducing each new component within the system while, at the same time, piloting the required staff training program so that it can be gradually extended to the rest of the civil registry. This approach will require sufficient technical knowledge and careful monitoring to ensure that each new process has a positive impact on workload.

3.1.5 Indicators

Indicators are a key element in managing performance. Selected with care, they will identify the disparities between current

and future situations and help resolve them. The results should produce incentives that will improve the efficiency of staff. Caution, however, is required so as not to distort the measurements, which could lead to false results. In order to prevent the possible distortion of results, the following tips can help:

a. Ensure that staff is involved in the development, application, and improvement of indicators.
b. Raise awareness of the fact that the indicator will not be used as a measure for disciplinary action but, rather, for the improvement of performance.
c. The time to develop an improvement plan is when productivity is low.
d. The improvement plan should define the responsibilities and achievements of the individual.
e. Measure compliance of the improvement plan with the indicator results.
f. If the indicators do not improve, review the improvement plan.

The characteristics that an indicator must include are:

a. objectivity
b. accuracy
c. comparability
d. relevance to decision-making
e. user-friendliness
f. reliability (must be independently verifiable)
g. measurability
h. specificity.

To develop the indicators, the following questions should be posed:

a. What will be measured?
b. Who will carry out the measuring?
c. Which measuring method will be used?
d. How often will the measuring be undertaken?
e. Who is interested in the result?
f. What are the outcomes of the results?

The indicators can be divided into four types:

a. Indicators to measure resources: to quantify available resources (human, material, and financial) that the civil registry needs to carry out its activities.
b. Indicators to measure internal processes: operational indicators for management and internal controls, used to quantify an intermediate objective (input) for other processes, which when evaluated together, will serve the population (outcome).
c. Indicators to measure products: to quantify the goods created and the services provided by the civil registry office.
d. Indicators to measure results: to quantify the effectiveness of the services provided.

These indicators influence the operational dynamic of the civil registry. They are illustrated in Figure 3.2.

The most important elements to measure within each set of indicators—relevant to the national context and civil registry responsibilities—are the following:

a. Indicators to measure resources:
   - geographical coverage
   - infrastructure

FIGURE 3.2: Operational Dynamics of a Civil Registry

- human resources
- legal framework
- current spending
- investment spending.

b. Indicators to measure internal processes:
   - management capacity
     - procedures: times and costs
     - ease in accessing services
   - introduction of ICT system on processes
   - use of nonconventional registration methods
   - relations with social services
     - education
     - healthcare
     - social security

c. Indicators to measure products:
   - vital event registration
   - certificate issued
   - information
     - vital events
     - Unique ID and passport.

d. Indicators to measure results:
   - actual registration rate
   - time required to complete a registration
   - timely reporting of vital statistics.

The final result will produce two outcomes: one to benefit the individual and the other to benefit the policy plan. Monitoring the impact of ICT on these indicators, as each component is introduced, provides a guide on the adjustments to be made, whether the structure and process is recognized as beneficial for national application or whether it is having an impact on the efficiency and effectiveness of registration. When organizing the indicators, a catalogue should be made with the following aspects:

- Indicator code: number assigned to the indicator with respect to its place within the catalog, taking into consideration the sub-category.
- Type: distinction that is assigned to the indicator with respect to the typology adopted in the development of indicators (resources, process, product, results).
- Definition of the formula: the components and the relationships for the indicator calculus.
- Disaggregation: indicates the levels at which the indicator will be arranged.
- Baseline: the value at the initial date, established to carry out the measuring; it is used as a reference to measure the progress toward the achievement of objectives.
- Objective: the value that the indicator must reach.

- Term for achievement of the objective: date at which it is expected to reach the proposed value as the objective of the indicator.
- Measurement frequency: time at which the measuring is carried out (daily, weekly, quarterly, biannually, annually).
- Sources: offices that will provide necessary data to calculate the indicator.
- Office responsible for the indicator: office in charge of supervising and reviewing the necessary data to calculate the indicator, according to the formula established in the technical data sheet.
- Monotoring of the indicator: the progress or setbacks of the indicator from the measurements completed on the established dates.

3.2 Internal Controls

3.2.1 Type of Audit and Timing

The functions and responsibilities of a civil registry involve not only the registration of vital events, but also the generation of information about the events. It is, therefore, important to guarantee the reliability of data, especially in view of increasing accountability on behalf of the State. The State, as well as the civil registry, must assume responsibility for their actions, decisions, and the services they provide to civil society. It is essential to undertake an audit to ensure that the activities carried out by the registry are in accordance with economic and legal principles and that they are effective and reliable.

Audits are carried out internally and externally. The internal audit will verify compliance of procedures, review achievements, and inform the management of developments. The external audit is an independent technical assessment of the work, authenticity, and integrity of the civil registry. The objective of an external audit is to inform government authorities and civil society about the quality of data that is generated from the civil registry. Other types of audits include:

a. **Financial.** The financial audit evaluates financial statements, ensuring that the results are factual and comply with required accounting standards. It is the responsibility of the civil registry to prepare quarterly financial statements and annual balances for review.
b. **Systems and procedures**. The systems and procedures audit assesses the appropriateness of procedures and operating systems and the extent to which they conform to the institution in achieving its objectives. Manuals of operations and ICT also are examined, including the security measures that are in place to prevent the unauthorized use of data (see Section 4.6). An audit of security measures, in particular, is important given that it can detect vulnerable areas for potential corruption or economic loss within the institution and will highlight the behaviors or actions that do not conform to the principles of transparency and governance.
c. **Efficiency**. The efficiency audit is similar to a systems and procedure audit, except that is more sophisticated. It establishes whether the management of the civil registry complies with economic and effec-

tiveness principles; that is, whether the institution achieves its results by the least possible means in terms of resources. In addition to assessing the compliance of systems and procedures, the efficiency audit will evaluate whether:

i the institution has acquired the appropriate amount of resources in terms of quality and cost effectiveness;
ii it protects and properly maintains its resources;
iii it avoids the duplication of tasks and the execution of activities that do not add value to its procedures;
iv it prevents idleness and an excessive number of staff;
v it has an appropriate system of management indicators to measure, inform, and assess the financial stability of the institution and be able to achieve results; and
vi it has an internal control system to prevent fraud.

When applying ICT, therefore, one question is whether its introduction has an impact on the efficiency of the organization.

d. **Project**. The project audit is a special appraisal to ensure the appropriate management of a specific project or plan of action. It is only applied when high-level authorities of the registry or government wish to learn about the operation of the project (e.g., special initiative to reduce under-registration, digitalization of files, implementation of ICT system and network.). The evaluation would seek whether:

i the objectives of the program are appropriate, realistic, and practical;
ii the project achieves the desired results;
iii there are elements that may prevent satisfactory outcomes or impacts;
iv it complies with the established procedural regulations of the project; and
v the project complies with the economic principles and effectiveness.

e. **ICT system and network**. There should be an internal and external auditing process of the ICT system (i.e., system, network, application, processes, among others). The internal audit should be continuous and is carried out by a team from the civil registry. The senior management can adjust the system or specifications to respond to the needs of the registration procedures, as well as the need for upgrades. The external audit is carried out by experts who do not have the authority to introduce changes; only to report on their findings. An audit *should* concentrate on the existence of and adhere to good ICT (security) management practice (which may include checking drivespace capacity); it *must* address such things as Internal Identity & Access Management capabilities of and for the ICT system itself (who has which access, granted by whom, when, etc.). This includes privacy and "segregation of duty" issues.

ICT operations quality (regular updates of operating systems and applications are performed; antivirus updates are regular; firewalls are active and rule set clear; access logs are checked and investigated for fraud/compromise). The server capacity and the

privacy settings, as well as the IT security audit, are key to address any vulnerabilities.

The frequency of the audits depends on the type applied. Internal audits are advised on at least a quarterly or biannual basis due to their purpose as an internal management control. An external audit may take place once a year, since it is a testimony of the accuracy of the documents issued by the institution. Systems and procedures audits and efficiency audits should take place regularly to prevent any deviation from management regulations. Financial audits can be done annually, while the project audit is at the request of interested parties to review the appropriateness and the results of the project.

3.2.2 Quality Management Principles

In order to meet the needs of civil society and stakeholders, a set of international standards (set by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)) should be applied: ISO/IEC 9001 (ISO/IEC, 2008). This tool assesses the quality of information provided by the appropriately certified auditors, thus guaranteeing the integrity of the information. The application of these standards sends the message that the civil registry aims to achieve efficiency and effectiveness in the execution of its tasks.

3.2.3 Routine Crosschecking for Consistency

The practice of crosschecking databases for consistency is essential in terms of internal monitoring and auditing, in order to ensure the credibility and reliability of data. Users of data expect consistency; if, however, they should find any inconsistency, doubts as to the quality of the data will arise. The application of methods to ensure consistency of data is vital to the credibility of the civil registry.

The database of a civil registry is a legal one that provides documents that may facilitate an individual's ability to access social benefits, healthcare, and education, among others, while other private and public sector organizations have administrative databases in place to operate their business. Cross-checking the data that is exchanged can ensure consistency in both databases. For example, the biographic data of individuals in an administrative database within a government ministry (third party) can be cross-checked against that held at the registry and vice versa. Feedback of any inconsistencies found would be provided to the third party who will contact the individual whose data it is for correction or for supplemental information.[8] This does not entail full sharing of all information (see Annex A). This will improve the quality of data in both institutions.

Data errors occur during uploading. Typical errors can be classified as follows:

a. No application of electronic systems (ICT): the main source of errors is handwritten documents by front- and back-office employees who make mistakes or are unable to read the handwriting of others.

[8] Should the civil registry not issue unique registration numbers, the inconsistency will need to be corrected by the institution responsible for its issuance so that, ultimately, the data from the birth registry matches the the data in the other institution.

b. Inappropriate application of ICT: this can occur frequently when a handwritten document is digitized and the technical revision (digitizing) is not carried out appropriately.
c. Inappropriate processing when electronically uploading. The uploading of the data may not be adequately monitored, thus affecting its quality. This can be prevented by ICT applications, which incorporate algorithms to detect inconsistent data and alert the processor to check it.
d. Length of intervals between collection of data and electronic uploading. The longer the time span between having gathered the data and its electronic upload, the more potential for errors and the challenges to correct them (e.g., staff turnover, difficult access to civil registry by families living far away).

To establish the consistency of aggregated data, it may be necessary to seek expert assistance (e.g., demographers, experts in sanitation, statisticians) who are able to analyze behavioral patterns and carry out causality analyses of birth rate data in specific populations (poor people, ethnic groups, immigrants). It is also possible to resort to categorizing the data in the following way:

a. Acceptable data: conform to the standards suggested by specialists, the majority of which cannot be suspect, despite the fact that not all the registration data may be accurate.
b. Suspect data: presence of an inconsistency, based on the projections done by a specialist and requiring an examination of the source or contact with the affected individual.
c. Erroneous data: There is no coherence.

In sum, to implement credible databases can be a costly and long-term process. The presence of inconsistencies can immediately impact the credibility of an institution and, therefore, the constant practice of data crosschecks is essential.

3.2.5 Routine Processes to Prevent Errors

The carrying out of error analyses is essential to ensure the adequate operation of a civil registry. The objective is not only to correct the errors but also to learn from them, so as to improve procedures. Routine analyses are a best practice for any organization that seeks to achieve efficiency and effectiveness.

An error should be assumed to have been the result of an involuntary human act rather than one that is inexcusable. Routine checks should be made on a weekly or fortnightly basis (no longer than a month). Should errors be detected, emphasis should be placed on identifying the type of error, frequency, suspected cause, result, and suggested means of preventing reoccurrence. Blame should not be held against the staff member believed to be responsible for the error; in fact, it is important to ensure anonymity in the error detection process. The type of error can include those that relate to electronic uploading, procedures, documentation, loss of information, inconsistencies, among others. The nature of an error is classified as follows:

a. Error of a random nature: hard to detect, suggesting that it was hardly avoidable; presented randomly.
b. Error of a particular nature: Failure is consistent and, therefore, the cause can be identified; once the cause is identified, it is possible to create a rule to prevent it from re-occurring by incorporating it into a specific practice and training plan, in addition—if necessary—to infrastructure development and the strategy of necessary inputs.

All organizations are prone to errors. Those, however, which are close to achieving efficiency, will make errors mostly of a random nature. Those that need improvement will experience errors of a particular nature.

Once the nature of the errors is established, the causes should be examined as follows:

a. Human error: generally caused during manual procedures due to involuntary distraction or repetitive actions that can be prevented by automation (i.e., ICT system applications). In nonautomated procedures, training should be provided so that relevant personnel are aware that this part of the procedure must be checked whenever it is applied.
b. Ignorance: the procedure should be improved and training should be provided to relevant staff.
c. Errors of interpretation: an agreement should be made with respect to which is the best way to carry out the procedure. Rules should be updated as a result, and relevant staff should be retrained.
d. Lack of engagement: Cause is detected when the error is repeated and the other causes are dismissed, especially in relation to ignorance and interpretation. In this case, lack of motivation may be the cause, generally as a result of weak departmental leadership or the lack of resources. The lack of responsibility on the part of a staff member may also be the cause, prompting possible dismissal from the organization—a last resort after eliminating all other causes for error.

Errors can be corrected by providing training and improving procedures. Since automation can prevent human error and facilitate the correction of data more effectively, having an ICT system and network in place is essential. For example, the use of a computer can correct a procedure by way of a parameter within a program without the influence of management and staff. In contrast, a human being requires motivation, training, supervision, and an assessment of the action.

Not all procedures can be automated, however. Many will still depend on human activity. It is important, therefore, to reduce the stages of electronic data transference. By first uploading data electronically, it provides the opportunity to establish filters in the fields to prevent the most common errors. These fields can only be completed with letters or numbers, specific formats for the dates, auto-filling, filters and/or drop-down menus for addresses, sex, etc. With an ICT system in place, errors will be reduced and alerts can be incorporated, should the data input deviate from previous registers.

A fully automated system will not totally exclude error, however, and frequent checks for errors are essential. A systems correction can be more damaging than one that is made in a manual environment.

The occurrence of errors should be viewed as an opportunity to learn, rather than a mistake that requires disciplinary action. To improve performance, staff members need to learn from their own mistakes and those of others. It is therefore important to set a routine to hold weekly or fortnightly departmental meetings as a means to examine the errors.

3.3 Outcome Measurement

3.3.1 Overcoming the Barriers to Timely Birth Registration with ICT

Birth registries provide a country with the number of births that take place within a specific geographic area and within a particular year. They also provide information relating to the number of births that have been registered within the same period. There are a number of socio-cultural, economic, and institutional challenges to overcome in order to reach universal birth registration. The responsibility of timely registration to overcome under-registration lies not only with the civil registry, but also with the family. The introduction of ICT can be an important tool to overcome some of the barriers, particularly by facilitating access by reaching out and bringing the registration services to the communities.

The main challenges can be categorized as follows:

A. Challenges relating to population/registrant include:
   a. Accessibility to the civil registry: long distances, lack of roads, transportation costs, or any other access issues.
   b. Lack of knowledge: lack of awareness of the existence or importance of a civil registry and its mandate; lack of awareness of the importance of registering a birth for the child's future.
   c. Lack of documentation: medical certificate of live birth and/or the mother's ID card
   d. Family structure: lack of collaboration on the part of the partner to carry out the process, absence of the father, discrimination against a single mother.
   e. Socio-cultural issues: language barrier, tradition, social exclusion.
   f. Health problems: mother or newborn.

B. Challenges relating to the civil registry include:
   a. Passive attitude: expect people to register in person with the appropriate documentation.
   b. Logistical problems: lack of resources to operate adequately.
   c. Management problems: poor leadership and organization, leading to inefficiency (loss of resources); unable to reach certain populations (e.g., refugees).
   d. Low and/or poor interrelationship with third parties: lack of a feedback system when collaborating with other public entities and private users to verify identities.

e. Communication: lack of outreach and awareness raising.
f. Legislative issues: not able to register all children born in the territory,

"Only what can be measured can be changed,"[9] and to establish a baseline to measure improvement it is crucial to establish certain criteria.

3.3 Client Satisfaction

The civil registry provides an important service to individuals as well as to other parts of government. ICT may support this service by providing quicker and more accurate data in a timely manner. It is important to monitor the quality of the services, and in this, user surveys may assist.

3.4.1 Satisfaction of the Beneficiary

The civil registry can improve its processing practices within two principal time frames: (i) the period between the birth and the legal registration of the child, and (ii) the period between the legal registration of the child and the delivery of the certificate. The first relies on the responsibility of the parent(s) of the child while the second has the direct influence of the civil registry.

The time it takes from registration to the issuance of the certificate should be as short as possible so that the individual holds an authentic hardcopy document as proof of registration, especially in the case of database damage, assuming that the procedure is not done online. Furthermore, given the challenges for some people to physically access the civil registry, it is recommended that the original/first birth certificate be issued on the first visit. An ICT system will enable certificates to be issued immediately and ensure that copies are always available online.

For the person, the birth registration may be required to access services, and it is also the basis on which other documentation is provided to an individual by the civil registry. These enable the individual to travel outside of the country (passport) and request other documentation, such as a driver's license or credit card (ID card). Furthermore, such documentation may provide the authority for the individual to take part in state and national elections.

The use of ICT may increase customer satisfaction by reducing the time it takes to process the birth certificate. An individual will interact with the civil registry at various stages of his/her life (e.g., birth of a child, marriage), as well as to request copies of vital event certificates. As with any organization, the quality of service is of prime consideration, especially with regard to the issuance of birth certificates. A warm, welcoming atmosphere and the courteous and speedy attention of staff is important. In particular, when interfacing with vulnerable populations e.g., (the poor, ethnic minorities, undocumented migrants, and refugees), efficiency is key to ensure that processes are adequately carried out and that there is no risk of rejection of these populations on the part of third-party users.

To respond to the expectations of the population, the civil registry should

[9] Attributed to Sir Isaac Newton.

undertake a public survey as a means to evaluate the registry's strengths and weaknesses before and after introducing ICT. The research can be done internally or externally. Surveys are useful to gauge the degree of public satisfaction with respect to the processes carried out and the behavior of staff towards the customer. Surveys are indicative of areas for improvement as well as whether other services are needed.

The following criteria relates to customer service feedback:

a. Profile of the client: sex, age, educational level, profession, ethnic group, nationality, distance to the civil registry office, among others.
b. Quality of the process on the part of the client: waiting time, duration of the process, resolution of issues, satisfaction.
c. Quality of the service area: atmosphere and comfort of the service office.
d. Opinions and suggestions.
e. Comparison of the civil registry service with other public or private organizations.

Based on the characteristics of the individual, the information is disaggregated by user profile to detect weaknesses in the service. These are critical to the birth registration process, taking into account the educational level, ethnic group, nationality, distance from the registry, among others.

There are three types of satisfaction surveys:

a. Written feedback is obtained from the individual at the end of each visit to the registry.
b. Sample feedback is obtained from people who visit the registry (exit poll).
c. Surveys are placed at the disposal of the client.

The first type will capture the feedback of all clients. While some may try to avoid the survey or refuse to provide feedback, the majority will do so, providing a sufficient basis for a comprehensive and accurate analysis. The benefits are the following:

a. Quality of service.
b. Quality of the responses will be good, given the proximity of the service.
c. The results can be evaluated by the customer service desk.

On the other hand, the following limitations need to be considered:

a. High cost, since it involves an administrative process that includes staff, infrastructure, ICT applications, and processing.
b. Surveys are not extensive (i.e., few questions are posed to enable the feedback of every client).

The second kind of survey is similar to the first, except that it captures only a sample of the clientele. The benefits, however, of this method over the previous are:

a. Survey is voluntary and can be lengthened to include various other aspects for a more in-depth analysis.
b. Cost effectiveness is achieved, given that there are a lower number of respondents.

The disadvantages are the following:

a. The results may not be significant to some offices.
b. The survey may not provide the customer service desk with sufficient feedback.

A third alternative is to place the satisfaction survey at the disposal of the user. This option, however, is not recommended as it has no statistical value. The self-selection process for obtaining the inputs may be a biased group of users. The reason for this is that people, in general, are skeptical as to the rationale of such surveys and are unwilling to take the time to complete them, unless they have had a strong positive or negative experience.

The results of these surveys complement the activities of those public and private institutions that defend the rights of citizens (e.g., ombudsman, consumer protection companies). The results of the surveys can be compared with the results of external assessments.

Finally, satisfaction surveys must also be carried out to capture the feedback of third-party users—those private and public organizations that require personal identity validation (e.g., schools, hospitals, social welfare entities, banks, insurance companies, service companies, credit card companies). This is essential, since the financing of the civil registry relies on the contributions of these entities (see Section 3.1.3.).

3.4.2 Technical Analysis

Technical analysis refers to an assessment of the quality of information provided by third-party users (e.g., healthcare, education and social security agencies; banks; insurance and utility companies). Similar to satisfaction surveys, they target the feedback of (i) users of the system, (ii) potential users, and (iii) experts.

Since the volume of third-party users is much less than that representing the population, the survey results that target third-party users will be of a higher quality and more accurate. These parties are more able to elaborate on the access and quality of the data held by the registry, the speed in which the requests are processed, the usefulness of the information, and the accuracy of the instructions. These surveys should be carried out periodically, perhaps once or twice a year. Since third-party users request the services of the registry on a regular basis, all users should be asked to complete the survey.

Information should be captured from potential third-party users who may be able to identify issues of access or qualify the information received. Addressing the issues will ensure the long-term relationship between the registry and the user, and increase the potential for more clients.

Experts can also make assessments, similar to a peer review assessment of a scientific publication. In this case, a committee of regional experts is established, whereby each civil registry, together with the relevant nongovernmental organization, can propose an expert. The consultant will analyze the quality of data that is issued by each registry and will provide observations and recommendations, which can be shared with other countries.

Administrative Framework Checklist

Have the following issues been considered?

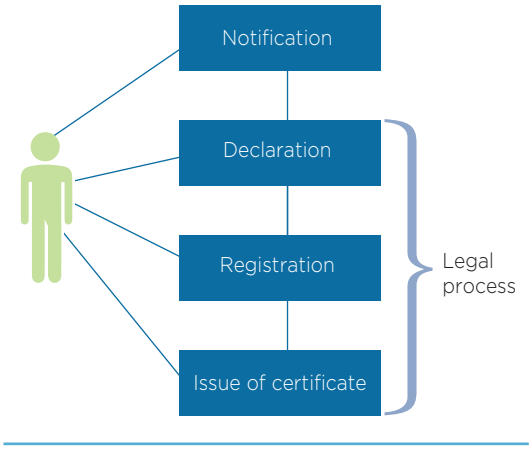
- Organizational chart
- Manual of job descriptions
- Adequate infrastructure in terms of space, comfort, conditions (climate control and security) for the user, risk analysis and mitigation plan, and in-house primary ICT data center with a back-up database at a remote secure location
- Financing regulations
- Designation of authority and terms of office regulations
- Planning department, reporting to chief executive
- Audits
- Crosschecks for consistency analysis
- Routine for analysis of errors
- Outcome measurement: satisfaction of beneficiaries and technical analysis by third parties

Chapter 4

Technological Framework

4.1 Introducing ICT for Birth Registration

FIGURE 4.1: Birth Registration Steps



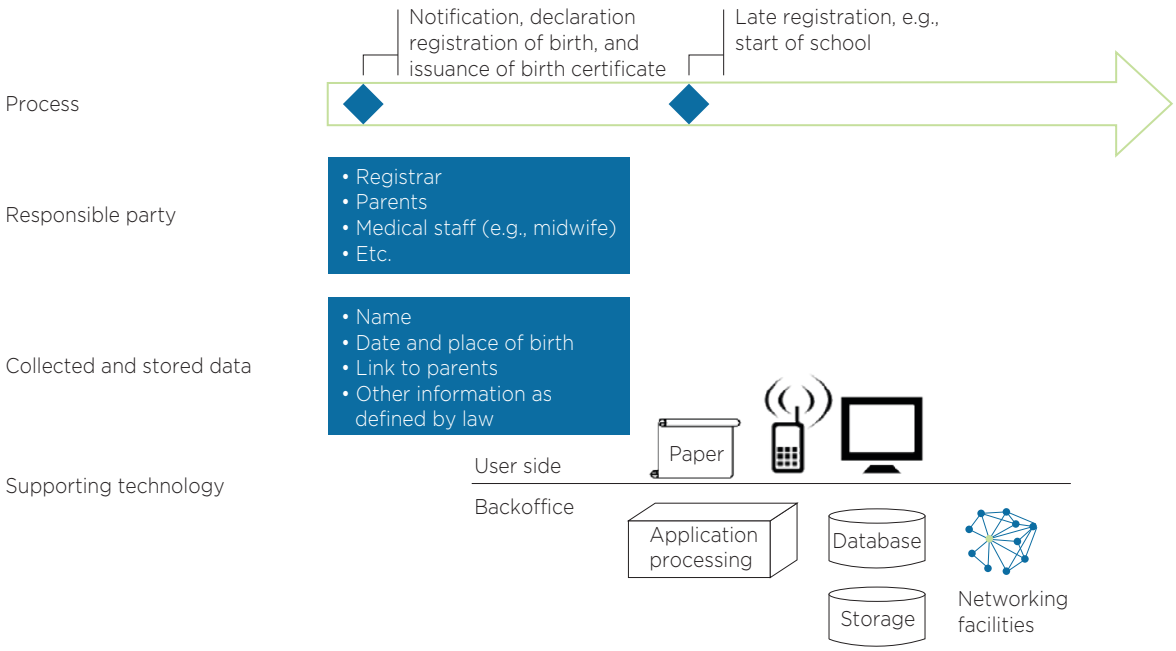
There are three steps to a birth registration process: (i) declaration of a birth by presentation of a hard copy of the medical certificate of birth—or one received by electronic means (computer, mobile phone) along with other required data; (ii) actual registration in the civil registry of the newborn; and (iii) issuance of an official birth certificate, as well as a digital copy where this applies.

The roles and responsibilities of the people involved in the process from birth to certification also need to be defined clearly. These people include the (i) healthcare professional (e.g., midwife, doctor, obstetrician, or witness) who helps deliver the child and signs the medical certificate of birth; (ii) the person registering the birth (e.g., guardian, parent, grandparent); and (iii) the trained and authorized registry official (registrar) who executes the actual registration and issues the official birth certificate. The possible variants (e.g., foundlings, still births, late registration) should also be defined.

The above information will determine who has the authority to engage in the registration. In general, these can be (i) the legal guardian, (ii) the witness or healthcare professional who writes the certificate of live birth, and/or (iii) the registry official (registrar).

The datasets and attributes that need to be presented, collected, and stored should be established within the legal framework (see Section 2.2). These will influence who gathers which data, when, and for what purpose. The structure of the

FIGURE 4.2: Overview of Components, Datasets and Roles in a Civil Registry ICT System



database and the storage methods must be agreed by consensus.

This section will describe the fundamental requirements for the implementation of an ICT system and network in the case of birth registrations, the basis of which should be included in the legal framework of the civil registry. Figure 4.2 illustrates the reliance that ICT has on birth registration requirements, roles and responsibilities of relevant staff, collection and storage of data, and technical support required. Despite the available technology today, many ICT projects have failed to deliver expected results, simply due to inadequate planning, especially with regard to human input. Relevant staff should be made aware of any proposed change to an established process, with an explanation of how ICT system applications can be used effectively to streamline the process. Although the healthcare professionals do not register births, it would make the process more integrated and with less room for error if they were to be equipped with communication devices and connectivity to report on the occurrence of a birth. The agreement between the ministry and health and the civil registry must be negotiated and signed at the highest political level.

The training of registry officials is vital to the successful implementation of ICT applications. In addition, healthcare practitioners and midwifes need to be informed of the appropriate documentation required to enable the entry into the civil registration

system of a child or how to create acceptable digital evidence of a live birth.

4.2 ICT System and Network: The Basic Requirements

4.2.1 Procurement

A civil registry is, in itself, a large organization that may have a number of IT systems that support the implementation of ICT, such as word processing, data storage, online access, internal back-end systems and IT-specific systems management tools. An internal or external IT Help Desk is usually available, with its own established procedures, to provide technical assistance when required. These procedures should be according to the international standards for IT service management, ISO/IEC 20000 (ISO/IEC, 2011), using IT management applications, such as trouble ticket software or configuration management database software to resolve issues more speedily.

The wide variety of already existing IT software systems may create what is known as a brownfield development environment—where it is complex to integrate new systems with those already present. It is easier to start from scratch, in what is known as a greenfield. In a brownfield environment, it is especially essential to have an ICT plan in place that is relevant to a civil registry.

It is this brownfield environment that makes the architectural planning for the introduction of ICT at a civil registry especially necessary. A registry cannot be bought, installed, deployed, and run; rather, ICT support must be carefully integrated within existing systems by way of a process known as an ICT network architecture design (Federal Adminstration of Switzerland, undated). Once the basic ICT architecture has been defined and documented, the software selection process can begin.

4.2.2 Civil Registry Requirements

As part of the architectural design, a needs assessment should be made. This assessment should review the civil registration system, as a whole, and its operation. Before ICT is introduced, as a prerequisite, the registration process should be effectively understood and implemented at all levels of the civil registry and by all involved in its implementation. If these criteria are met, a review—possibly using the earlier noted tools for customer satisfaction and system audits—may identify areas where ICT could be introduced to improve the process.

4.3 ICT System Architecture Planning and Deployment Processes

The overall ICT system architecture for a civil registry should involve the designer (who may be a selected vendor or, alternatively, a body within the government) and other relevant IT staff. Close communication and direction with the personnel who are to use the new ICT process is required at all stages. Taking the environment in which the ICT system will be deployed and used, the system can be divided into several categories, depending on how many layers or tiers it has. It could be a one-tier

(or standalone) system that works independently on a personal computer (PC). Client/Server systems have a component that is installed on each PC (often known as a "fat client" or the "front end") and one component that sits on a server (usually referred to as a "back end"). Some of these front-end systems are able to be used offline and synchronized later, while some require direct connectivity to the back-end.

Another category relates to three-tier or multi-tier systems, which are most commonly used today. Instead of a fat-client graphical user interface (GUI), they require a browser (e.g., Chrome, Internet Explorer, FireFox) as the client side interface and a Web (Application) server as the middle tier (or front-end server). The business (or domain) logic is located in the back-end on another server, which can also hold the database. Very large systems with a significantly high number of datasets (e.g., civil registry ICT systems) usually rely on a dedicated database system. For a highly distributed system that is operated and used at many locations simultaneously, the key is a local, independent operational function. The system, therefore, must be designed in such a way to allow the basic operation of a remote registry site without a wide area network to connect to the central registry infrastructure—an operation usually achieved by deploying a local proxy or cache server on each site that allows for resynchronization and updating once network availability is restored.

This planning process involves the layout and design of the ICT system and includes several considerations. It is very difficult to make changes to the components (front-end server, back-end server, database) of large ICT systems due to their complexity. It is essential, therefore, to provide systems developers, administrators and operators with dedicated environments to test the changes. Specific technical experts can do the design in four stages:

a. Development stage: systems developers only)
b. Testing stage: test engineers only, although systems developers may be granted access on request
c. Integration stage (optional): test engineers and systems production operators only
d. Production stage: systems production operators and users only

At the development stage, systems developers are able to test the varieties of codes and patches to ensure that they operate as they should. At the testing phase, basic integration within the surrounding systems is made available or simulated, allowing the test engineers to ensure that the newly developed changes operate as intended. Integration, representing the third stage, is similar to production and will mimic how the system should operate under production conditions. The live system is only updated once the integration stage has been completed.

4.3.1 Pilot, Rollout, and Operation

Close collaboration between the vendor/systems integrator and the internal civil registry specialists is essential during the planning and buildup phases of an ICT expansion. To ensure that the new registry system fits into

the brownfield environment, it requires significant customization and adjusting.

A large and complex ICT system, such as that of a registry, requires constant support, maintenance and improvement. Since this does not fall within the role of registry personnel, an operations service provider (SP) should be procured through a bidding process to ensure the availability of qualified IT operations specialists.

Once the basic operational Terms of Reference have been agreed upon and a Factory Acceptance Test (FAT) has been conducted and approved, a minor pilot can be put in place to gauge the performance. This strategy contrasts with implementing an ICT system on a clean slate or greenfield environment.

The pilot should take place where there are highly skilled internal and external specialists and it should only involve those processes that have been identified for ICT support. Based on the four stages of architecture previously listed, the test phase should be carried out and include a Site Acceptance Test (SAT). The integration stage follows under production conditions, and the application of a User Acceptance Test (UAT) is made, which includes a number of key users. Based on the satisfaction of the users, the process moves to the production stage where it is implemented. It is at this moment that the team begins to learn how the system operates, how users will react to certain process changes, and how issues can be resolved with minimal impact to operations.

Rollout of the new software should be conducted gradually once the core functionality has been sufficiently tested and a significant number of key users (registry officers at other locations) have been trained to use it. The selection of branch offices should be based on those serving a large segment of the population and which have the sufficient resources to achieve their objective in a short time. The problems that may be experienced by the larger sites can be mitigated more easily than in smaller offices. Only when the majority of the population has been registered should upgrades or major changes to the system take place.

The staff needed for such a rollout should include a dedicated project rollout manager who will remain in place until full deployment is completed, a local rollout coordinator, and at least one key user for each site. For technical expertise, a number of consultants can be recruited for each site prior to implementation, as well as a group of trainers who can ensure that all registry officers are trained to properly use the ICT system.

4.3.2 Documentation, Handover, Service, and Maintenance

Once the system has been completely rolled out at all locations on a national level, the external team (vendor and systems integrator) should ensure that the comprehensive documentation relating to the new system is delivered to the client, including the key parameters, configuration, technical users, administrative users and their respective passwords. During the handover period, the systems integrator should introduce the civil registry ICT specialists and selected SP experts to the management and deliver the administration details of the system, as well as the procedures that relate to troubleshooting and other issues that may arise. The

documentation should be reviewed for completeness and error information should be tested, at which point final payment is made to the vendor/systems integrator.

Extensive licenses are required for non-open-source ICT systems. Vendors usually charge approximately 20 percent of the license fee per annum to provide software updates and support services, excluding services that are essential to the implementation of these. These facilities need to be procured separately or should be included in the agreement with the operational SP.

4.3.3 Operational Support and Personnel

The ICT system may have technical issues or simply have glitches and operational problems. These will need to be addressed by an on-site IT Help Desk that will record the problems that arise. If issues persist or they are beyond the expertise of onsite staff, they should be handed to a civil registry ICT systems specialist to resolve. In cases where the specialist has no solution, the vendor needs to be informed, especially if there is a need for a change or patch. With each new patch and update, the processes need a FAT, Site Acceptance Test (SAT), Systems Integration Test (SIT), and UAT, each with quality control and sign-off actions.

4.3.4 Components

The ICT system is largely responsible for safeguarding the operational efficiency of the civil registry. It will be impossible to carry out the tasks of the civil registry in the event that the core ICT system fails to operate. For this reason, the ICT system should be designed to meet the needs of each of its components, especially the databases that hold the information of those registered. A calculation, therefore, should be made by dividing the hours the system is expected to be in operation by the hours it is supposed to be used. This does not mean that it should be operational 24 hours seven days a week. Normal work hours usually total 40 out of 168 hours a week. Therefore, in theory, it would be acceptable to ensure operation of the system 99 percent of the time during normal work hours; that is 7.92 hours each workday (or an acceptable outage of approximately five minutes each work day).

While this may appear low, the acceptable outage time totals nearly 25 minutes a business week and up to 30 hours a year—a loss of productivity equal to almost one work week. It is recommended, therefore, to task the technical experts with calculating the cost of adding another 0.5 percent, so as to reduce the outage to 15 hours a year cost effectively. They would have to evaluate whether it is reasonable to calculate the (lost) opportunity cost of registry personnel not being able to work 15 hours a year (average number of outage hours x number of registry officials using the system x average hourly wage). The investment may be worth the effort at 99 percent.[10]

[10] Overall systems availability is a challenge to increase, as several weak links may influence the cost factor. Each component (client, access network, core network, front-end servers, back-end servers, database servers) has its own network "sub-system availability" and the calculation is a multiplication factor. At 99 percent availability for each sub-system, the figures would be: .99*.99*.99*.99*.99)=(.99)^5 = .95 overall 95 percent availability.

Systems maintenance, updates, patches, and changes are excluded from this calculated network availability, which means that the processing of these must be done outside of business hours. This is especially important, if the operation of the system is outsourced to an IT SP, as defined in the legal agreement with the SP.

4.4 Client Server Network Availability

Access to the network by individual client servers (officers in the field) should not be a primary concern, given that the software used can be safely updated and reconfigured as necessary through a central asset management and systems software distribution solution.[11] Overall input from local offices, therefore, should not be affected. It is recommended to patch and update client servers outside of business hours (e.g., a weekly patch on Monday afternoons between 5.00 p.m. and 6.00 p.m.).

4.4.1 Local Sub-system Network

Closely linked to the client network is the local sub-system network in remote sites. Only a fully connected ICT system and network can be used to its full extent. If there is no access to the wide area network, say, in a largely populated remote location (e.g., a regional capital), civil registry experts should still be able to conduct basic registration without a back-end server, perhaps at the expense of background or online checks of ID card validity, referred to as "graceful degradation". To enable this, there should be a local proxy server in the larger populated areas to enable basic processing, using user interface functions to cache all birth registries processed during the network outage. Through the "message queuing" or other integrity protection mechanisms, a full synchronization process will be possible with the back-end systems once the network is restored. Depending on the relevance of the site, the local proxy server may be designed with a local failover or may run in parallel twice within a "high availability" mode.

4.4.2 Database and Back-End Server Availability

In order to prevent a complete loss of the ICT systems data, it is imperative to operate the system from at least two independent data center sites, separated one from the other.[12,13] In case of a natural disaster or force majeure, the second data center would back up the first. The details of this provision should be included in the business continuity plan (BCP) and disaster recovery plan (DRP), (see Section 3.1.2)

Back-end servers and databases should be located in a secured and well-maintained data center where ICT experts are able to design, implement, and operate

[11] While this is not a part of the specific ICT solution, the registry should have an efficient software and patch management solution in place, provided through a vendor.

[12] Distance should depend on geographic conditions (e.g., likelihood of earthquakes, flooding).

[13] To further increase availability in case of a DRP, there should be additional backups (e.g., stored on external hard drives, USBs, or tapes) stored in a secure location.

in a network back-end system environment. The installation of similarly configured servers has become standard, given the availability of virtualization technology provided by VMware (ESX Server), Microsoft (HyperV) and the open source project XEN, among others. The front-end and back-end servers should have a user interface, based on a clustered configuration. This means that there are multiple identical servers to form a group (cluster) that shares the workload of the client servers. The advantage of clustering is the ability to add or subtract instances from the cluster "on demand"—a technology that has become popular in the cloud model of ICT operations. Basically, the civil registry ICT system will run in its own dedicated cloud, although the registry will need its own specialists in this environment, as this is a basic ICT service that many ICT SPs can provide at a local level inside their data centers. The SPs should be selected on the basis of security certification, such as ISO 27000 series (ISO, 2013) and a data center certification, such as SSAE 16 (formerly SAS 70).

4.5 Databases

The ICT database of a civil registry is the most important component, holding all the personal information of citizens. Without the database, birth registrations would not be able to be processed efficiently, detracting from the 99.99 percent objective assumed. In order to process large sets of data (such as big data analyses or the validation of voters during regional or national elections, which may take place on weekends or after work hours), the network baseline needs to be set to 24 hours and 7 days a week, which will affect the downtime of 5 minutes each year. In other words, the database may be unavailable.

4.6 Data Protection and ICT Network Security

As a government agency, the civil registry needs to ensure that it will act responsibly and ensure the security and safety of all its operations and records. By developing a core ICT infrastructure, the civil registry provides not only its staff administrative documents, but especially important, the entitlement of those registered to access their personal information and vital records. With this, though, comes the challenge of data abuse and theft, since it is easier for a flawed network to be compromised than for paper documentation to be stolen.

As with protecting paper documentation by way of locks, security alarms, and other methods, an ICT system must be safeguarded. The principles of design are described below.

4.6.1 Disaster Recovery and Business Continuity

As stated in Section 3.1.2, a complex registry ICT system is contingent on the BCP and DRP. First and foremost, registry data records need to be secured for the long term. A data availability plan usually takes into consideration standard operational issues without contingency planning in the case of a catastrophe. It is strongly

recommended, therefore, to include the ICT system and network into the BCP and DRP.

A team of qualified staff should operate and maintain the ICT system. The challenge, however, is that unless budgeting includes the appropriate physical and electronic security measures that are necessary over the long term, it will be difficult to protect the back-end servers and the databases, especially with a remote backup data center. A solution, therefore, is to outsource—at least—the secondary data center to a local SP. This can be combined with the maintenance and operations service of the primary and backup servers.

It is essential that energy sources and internet connectivity be maintained—at least for the core data center and its backup. An uninterrupted power supply is essential, such as a diesel generator, a flywheel, or a battery-based system. Each location should have two separate connections to the electrical grid and two independent lines to the wireless internet, served by two independent service providers within or outside the building.

4.6.2 Protection Targets and Security Design Principles

As stated in Section 2.2.2, every effort should be made to protect personal identity information against theft and abuse. Basic legislation on the protection of personal data should be established as a baseline to secure the ICT system and network used to collect, process, and store vital information at a civil registry. The key objectives to secure data include the following:

a. Confidentiality: data must be protected against unauthorized access.
b. Integrity: data must be protected against unauthorized modification or deletion.
c. Availability: data must be kept available at all times for its intended use.

There are three bases, known as the CIA Triad model (confidentiality, integrity, and availability), which should be incorporated into the design and architecture of civil registry ICT systems. They may be amended accordingly to enable comprehension. These are the following:

a. "Need to know" basis: The civil registry ICT system should be designed to only allow those attributes and datasets that are necessary to fulfill the responsibility of a registry officer to be available. That is, a registry clerk should be able to view the basic attributes of a person, such as the family name, but not be able to conduct a search based on ethnicity or religion of a segment of the population.
b. "Need to have" basis: The ICT system of a civil registry should only collect those datasets and attributes to fulfill its function. For example, to process the birth registration of a newborn, the employment status of the mother or father is irrelevant, although in some countries it may be necessary based on traditional or religious beliefs. The "Need to have" basis is significantly important, since the aggregation of data could be misused to conduct big data analyses to enable abusive schemes, such as ethnic cleansing.
c. "Need to do" basis: A civil registry with an ICT system in place requires specific

job descriptions for its staff. The role of a registry clerk should be only to access the ICT activity that registers the children born in the country, but he or she should be prevented from being able to print or issue new ID cards or passports. Additional boundaries can be set for the registry user, such as limiting the number of results based on a certain query or the number of times a certain query can be issued by the same user within a specific timeframe.

4.6.3 General Security Recommendations

To install an overarching ICT system for civil registration (that may also support the recording of other vital events) that follows a multi-tier architecture will require a fully networked infrastructure. Assuming that the civil registry already has several basic ICT components in use and that the client PCs are running various applications, some proposals are described below.

4.7 Management of Client Users, User-IDs, and Software

It is essential to appropriately manage all client users of the network to ensure the security of operations. Strict overview of the network clients and their user accounts should be constant. It is essential, therefore, to install an integrated internal identity and access management solution. This will enable new users to access their resources quickly while, at the same time, keep low the number of orphan accounts (i.e., accounts belonging to registry personnel no longer with the registry).

4.8 Internal Identity and Access Management

To control IT assets in the face of staff turnover and to reduce the risk of unauthorized IT access, the standard processing of joiners, movers, and leavers in the case of external consultants/contractors and internal staff should be complemented by an IT identity and access management solution. This will automatically generate a new account and enable access to the internal email system and the registry ICT system within the parameters of the role of the staff member. The human resources department may enter the staff member into the system for either a regular employee or a contractor. When the employment term or contract ends, IT access must be denied immediately.

4.9 Authentication, Authorization, and Accounting

Each access to the ICT infrastructure of a civil registry—and especially the birth registry—needs protection through user identification, authentication, and authorization. Each employee should be assigned a dedicated user account (with no access to group-shared accounts), a secret password, and the person's job title with regard to the ICT system. With adequate accounting principles and surveillance technology, only then will it be possible to track and

manage access to ICT resources to ensure security and prevent abuse. In sum, those who have access to the ICT infrastructure should be issued the following:

a. Unique record: established by the civil registry.
b. Unique individual identification number: established by authorized agency.
c. Dedicated individual user account for the directory: this will allow logging on to a network.
d. Dedicated individual user account for the ICT system: in this case, only for birth registration, which is assigned to 4.9.1(d) below.
e. Specific user role of the employee within the ICT system for birth registration.

All log-on events, whether they are successful or unsuccessful, should be collected and stored for a specific time. This will enable an investigation into suspected abuse or fraud.

4.9.1 Limiting Database Administrator Access to Registry Data

Each database should be managed rigorously in terms of who can do what, where, and how—as long as the responsibility rests on a single person, such as a technical expert. Given that many databases and their underlying database management systems do not limit the number of administrative users ("dbo" for database operator and "dba" for database administrator), applications can be set to use both. This opens up an entire database to the potential of illicit manipulation or minor changes—sometimes with disastrous consequences. The following, therefore, are strongly recommended:

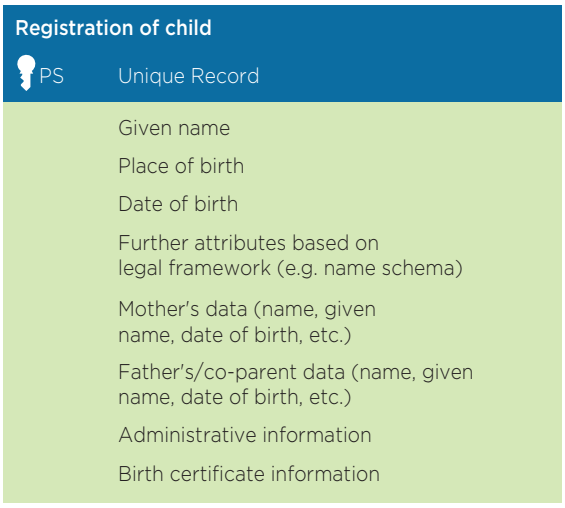
a. Create a team of key technical users who have the minimum access privilege required to achieve their tasks.
b. Document these users and include the purpose and conditions for which they have been granted access privileges.
c. Assign each group of database transactions with a designated database user and document who has made the assignment under which preconditions and for which purpose.
d. Usage of the dbo/dba accounts should be limited to tasks involving maintenance of the database management system and related databases.
e. When possible, limit the use of dbo/dba to access, view, copy, or manipulate the contents of specific database tables. The addition of a layer of encryption is essential.

To ensure best practices in terms of the rights to access the database, rules and regulations should be defined for each technical user, depending on the tasks they need to carry out. An access matrix should be included, defining the level of access rights of each user according to the CRUD scheme (creating, reading, updating, and deleting data). To keep track of these access rules and how they are implemented requires a Privileged Access Management solution.

4.9.2 Database Structure and Semantics

Despite the fact that most civil registry ICT systems that are available carry their own

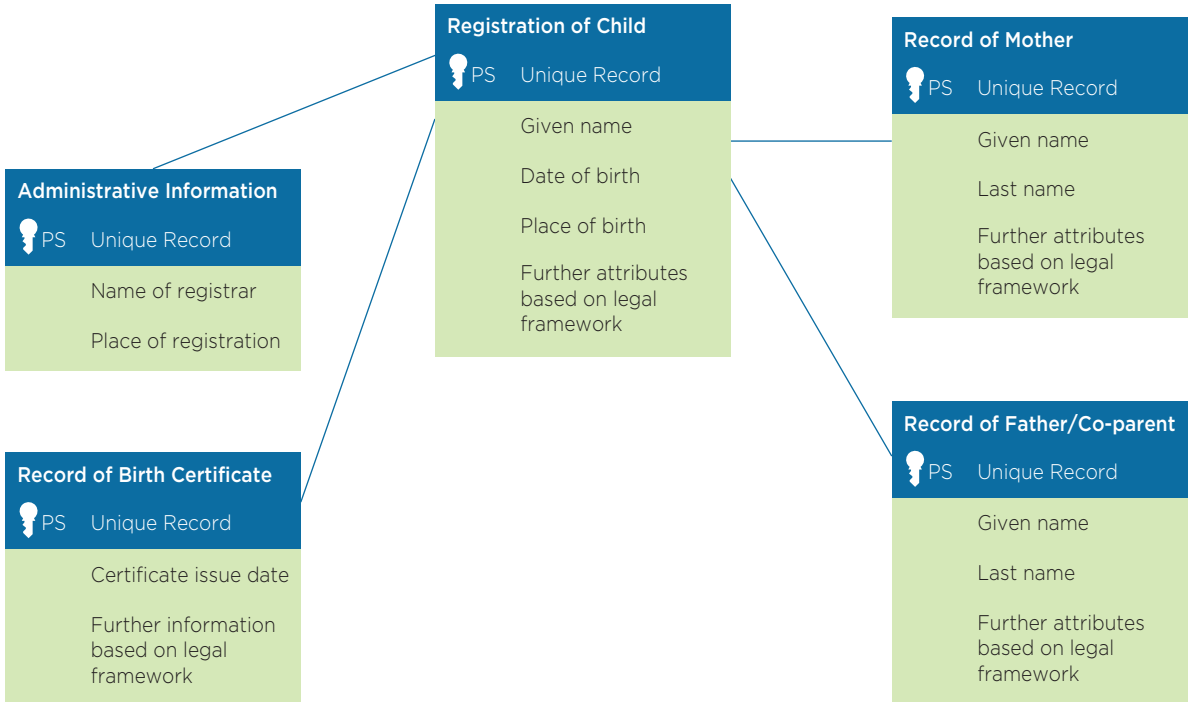
FIGURE 4.3: Single Database Record for All Information



internal data-model and database structures, it is important to define and document how the information will be modeled in terms of their relationship. As the actual implementation will differ significantly, based on the datasets that are needed, gathered, and stored, there are two potential alternatives: (i) one record for all data (Figure 4.3), or (ii) multiple records for different kinds of datasets (Figure 4.4).

A database specialist team and a registry ICT systems specialist must review the database design, given that not all organizational data models are suitable. Special consideration should be made of the computational efficiency of the models, since databases can become significantly slow

FIGURE 4.4: Multiple Database Records



in certain configurations or dataset organizations, especially if there are millions of searchable datasets.

In general, it will reduce the processing effort if all entries are made within one record, compared to the alternative where each entry will need to be made in various records. For example, by inputting an entry change into one record, the system will automatically update the other entries within the one record. This, however, is dependent on whether this more complex network activity can be defined in the procedural tables.

In terms of the governance of the civil registry, all changes within the datasets should not be made by simply overwriting existing entries. Rather, the changes should be entered with the name of the person entering the data and the old data should be clearly marked as overwritten.

4.10 Systems Backup, Data Backup, and Long-term Archiving

While network planning should aim to prevent systems failure, it is possible that an ICT system could crash, creating significant data loss (similar to registry archives burning, despite the presence of smoke detectors and fire extinguishers). It is vital, therefore, to establish and maintain various backups to re-establish operations. The conditions are usually defined as (i) Recovery Time Objective and (ii) Recovery Point Objective. The Recovery Time Objective relates to how long a certain system or sub-system is acceptably unavailable. The Recovery Point Objective relates to how many dataset updates are lost, depending on how often the datasets are backed up.

In the case of birth registrations, a systems crash will have no impact as long as there is a means in place that caches changes, updates, and corrections to existing records. New registrations, however, will be delayed until the system is fully restored. This significantly relaxes the Recovery Time Objective.

The Recovery Point Objective, in contrast, is critical, as any update or change made between the last backup and the crash will be lost and will require manual input. It will be worth investing to ensure that the database network is backed up adequately and that checking methods are in place. There also should be a restoration plan in place. The cost for external hard drives and USBs has dropped significantly to enable a backup exercise each day and maintain a log of backups over three days.

The ICT system will require a few changes in order to keep it functional over long periods of time. Taking into account the front-end, back-end and database servers, a daily backup of the cluster should be made and relocated to a secondary site in case of any changes. As changes will occur infrequently, a one-day backlog will be sufficient. The dataset and server backups can be archived once a month, although there should be a data retention policy in place that defines up to when and how the archived content shall be stored.

More important to regular backup operations is the long-term longevity of these backups. The last two decades have seen a dramatic change relating not only to the

technology, but also to storage devices for large amounts of data. Backing data with tapes, a common method since the 1990s, has become obsolete. So has the magneto-optic and optic "read once read many" (WORM) system. Local ZIP-disks and compact disks are also becoming inefficient ways to back up data due to possible damage, especially in the case of the latter which is affected by bright ultraviolet light. Furthermore, previously used data formatting for files is changing and becoming more incompatible. To be able to save data safely, tape libraries are the most preferable and should be designed to enable the copying of data to new technological storage methods so that the data continues to be retrievable.

The approach to long-term archiving is complex when datasets, records, and digital documents or transactions are digitally signed. Digital signatures are based on digital certificates that have a limited life span of one to 30 years. A user certificate is valid for one to five years, and a root CA up to 30 years. Expired datasets require a new signature with a valid certificate. In this case, the archiving system should be able to automate this process.

4.11 Specific Security Requirements

4.11.1 Integrity

Maintaining the integrity of the data is as important as ensuring the integrity of the dataset and personal records that are on file in the registry ICT system. While some of this functionality may be elementary in terms of security, there are a number of requirements to maximize this.

While encryption of the database will help conceal its contents from those staff processing the data, there must be a way to monitor the integrity of information that is input. One approach is to add check digits to each record, a set of records, or entire database tables, which would be hash object keys that are stored in an additional table.

This approach will mitigate the risk of a system's internal errors that can cause loss of integrity, but it does not prevent an intended or unintentional change to a dataset by an authorized user (civil registry officer). The ICT system should be able to provide a way to revert or roll back changes that are made to individual records, as well as implement safeguards for the accuracy and completeness of data.

4.11.1.1 *Encryption*

Since the birth registry relies on an ICT network and distributed systems, data "at rest" and data "in motion" (data that is transferred across local and wide area networks of the civil registry) need to be protected from unauthorized real-time interception, alteration, or deletion by way of encryption.[14] Standard encryption software should be used for data "in motion". For the Wide Area Network (WAN), however, point-to-point encryption software can be applied between routers. This, however, will also require an extension, known as a Layer 2 Tunneling Protocol (L2TP) and used by internet service providers. Given

[14] The appropriate encryption mechanism should be selected by security experts and regularly checked for its effectiveness.

the lack of confidentiality that is inherent in this layer, an internet protocol security (IPsec) suite will need to be added using a bloc cipher, known as an Advanced Encryption Standard (AES). Alternatively, a Multiprotocol Label Switching (MPLS) network can be used, as its architecture makes it difficult to hack into. Its customers create end-to-end circuits across any type of transport medium, including an ISP.

The wireless (WLAN/WiFi) parts of a local area network should use the WiFi Protected Access (WPA2) or other secure protocols, such as the Secure Sockets Layer (SSL) or the Transport Layer Security (TLS), for stronger data protection and network control. Most web-based applications are equipped to use hypertext transfer protocol (http), an application for communication for the World Wide Web (WWW). Ensuring that all registry ICT network communications browsers are set to https is highly recommended.

In the backbone network, the access from the application servers to the database must also be encrypted to prevent the risk of unauthorized interception, especially if the servers have been outsourced and are located in a third-party data center. Most database management systems (e.g., Oracle, Microsoft SQL), software (IBM's DB2), or other open source alternatives are equipped for encryption interfacing.

For data "at rest", the most important component is the database. The above-mentioned vendors have table-, column-, and row-based encryption capabilities, although some of these options can be expensive. Nevertheless, it is worth installing the advanced security software, so that staff processing data can be prevented from unlawfully accessing the datasets. To locally encrypt data, ICT network functions can be applied or other software can be purchased for the files and folders on the hard drive of the civil registry.

4.11.1.2 *Network security*

Some office buildings already are equipped with the necessary accessories for network infrastructure and WiFi access, which should be strictly managed to exclude access by external parties, including visitors and contractors. This includes the blocking of unused network jacks, as well as the WiFi/WLAN infrastructure. WiFi networks should be encrypted with up-to-date software, mentioned above, and access passwords should be kept confidential. A parallel protected guest WiFi network should be made available for visitors requiring regular changes of access passwords. Alternatively, a token or voucher system can be installed. Access to the registry's main ICT network must be restricted to authorized personnel at the exclusion of external parties.

4.11.1 Secure Data Exchange and Integration

The increasing links between government agencies requires the exchange of high volumes of data, as well as data synchronization. The digitalization of birth registrations will enable the civil registry to efficiently collaborate with other government agencies to map the needs and vital events of its population. It may also facilitate the issuance of unique identification documents, such as ID cards and/or passports, as well as the interaction with various authorities and agencies

at little or no cost. The ICT systems of each agency, however, should be synchronized to handle the data exchange.

Depending on how long the ICT network has been in place, a simple set of digital Application Programming Interfaces (API) will facilitate collaboration. Initially, a standardized system to authenticate a person (e.g., date and/or place of birth, given name and/or surname), known as "e-ID related" data—or master data—is required. For citizens, this information is required to liaise with any government agency or third-party entity (e.g., employer, utility provider).

Standards on how these attributes can be shared between agencies without violating security are a key to creating successful interagency collaboration. Currently, XML-based schemes using JSON/REST are common baselines for designing these APIs.

4.11.2 Digital Signatures

The use of digital signatures requires a separate, complex ICT infrastructure, referred to as a public key infrastructure (PKI). As a public service or a national ID register, it is a technical, as well as legal, challenge to implement and protect a PKI. As previously recommended, a comprehensive legal framework should be in place, defining the use of digital signatures and providing that they are as valid as handwritten signatures on paper documents. The means, therefore, to create digital signatures should be guaranteed as trustworthy and well protected so as to maintain the authenticity of the digital signature. To guarantee such authenticity, there are some elements that need to be taken into account.

4.12 Legal Framework for Digital Signatures

Despite the need to guarantee the protection of digital signatures, experience has shown that there is a challenge to implementing too rigorous a system to issue, validate, and accept digitally signed documents, which can lead to low implementation or abandonment of the approach. The level of balance between usability and security depends on each country's needs; however, basic requirements are needed to prevent the misuse of information that can promote abuse and corruption.

The period of validity of the digital signature should be established and the general minimal rules for issuance should be described in an appendix to the legal framework. The adoption of a PKI and digital certificates can create the foundation for later introduction of an e-ID.

4.12.1 Technical Baseline

A number of technical components need to be in place to be able to support the use of the digital signature. These include the following:

a. Issuance of a digital certificate to those who wish to use a digital signature (individuals and entities);
b. Application for a digital certificate (which may be included with an ID card application if applicable);
c. Use of digital certificate to sign documents electronically;
d. Means to test and verify the validity and authenticity of an electronic signature;

e. Means to prolong or refresh a digital signature on long-term archived documents;
f. Means to revoke a digital certificate before its expiration;
g. Means to refresh a digital certificate automatically on expiration; and
h. Means to maintain an archive of expired certificates for long-term validation.

There are certain elements or components that are needed to enable the application of these technical components. These are as follows:

a. A Certificate Authority (CA), which is the trusted entity that issues and revokes public-key certificates, is comprised of
   - a state-approved root CA (see Section 2.2.3);
   - one or more Issuing CAs; and
   - one or more Certificate Policies.
b. Registration offices (registry office, but can also be third parties, such as banks) with
   - enrollment facilities; and
   - ID validation facilities.
c. Issuing office (same as above, virtual, or a dedicated place) with
   - issuing facilities (e.g., e-ID cards); and
   - ID validation facilities.
d. Client technology for private end-users and legal entities
   - signing of documents; and
   - validation of signatures.
e. Certificate validation and revocation services
   - providing centralized validation (usually a Certificate Revocation List (CRL)) and/or an Online Certificate Status Protocol (OCSP); and
   - providing a centralized way of notifying the CA that a certificate has been compromised.

4.13 Required Components

4.13.1 Certificate Authority

As described above, the Certificate Authority is the entity that issues digital certificates and signatures to people or entities. Cryptography provides the means to the user to create a digital certificate with a private key and a public key infrastructure scheme, signed and validated by the Certificate Authority. The CA becomes the Trust Anchor (or trusted third party) for each and every digitally signed transaction, guaranteeing the validity of the transaction. A number of elements are required to fulfill the activities of a CA.

4.13.2 Offline Root Certificate Authority

The Trust Anchor—or Root CA—should be rigorously protected in view of today's elevated threats and the risks of online hacking. The usual practice for security is to establish a validated Root CA through a trusted provider (e.g., Entrust, VeriSign), which signs the underlying Issuing and Policy CAs. These are taken offline and copied onto a secure and encrypted PC laptop or external hard drive that will be secured by a public authority.

4.13.3 Issuing Certificate Authority

In cryptography, the CAs issue digital certificates to the users by way of one or more Issuing CAs that are identified, validated, and

signed by a Root CA. The Trust Anchor then validates the authenticity of the Issuing CA. In cases where the certificates between legal entities and citizens may vary, it is recommended to create a specific Issuing CA for each of these user groups to avoid conflict of interest. If multiple sites are used to issue certificates, there should be a number of methods in place to guarantee issuance of the certificates in the case of a network outage.

4.13.3.1 *Certification policy*

A Certificate Policy identifies the various actors of a public key infrastructure, including their activities and responsibilities. A dedicated field to handle the management of the different Issuing CAs should be implemented, whereby all policy changes can be made and distributed to the relevant authorities in the public key infrastructure.

4.13.3.2 *Validation check*

In order to validate the authenticity and accuracy of a digital signature, an online check is initiated, either by comparing it with a CRL (a list of expired or revoked certificates) or running it through an OCSP responder. A CRL can be copied and published on the civil registry website, although the validity lasts only until the next refresh of the network (a day or a week later). OCSP is an internet protocol that requires the highest network access (99.999 percent 24 hours a day seven days a week) of a server to host the OCSP responder.

4.13.3.3 *Operational recommendations*

The planning, implementation, and operation of a secure network is very complex and can be costly. Few countries, in fact, have implemented this technology and are operating an in-house system. Many have either developed a public-private partnership to finance it or have outsourced the entire operation to a Trust Center provider that provides most of the prerequisites. The most successful installations are those where the operator of the PKI is the biggest user, such as a bank or ISP, whereby a shared-revenue approach instead of a paid SP one can be established.

4.13.3.4 *Client technology*

Users should be able to easily create and validate digital signatures on any device or platform so as to facilitate the adoption of this technique. Well-established software technology, such as PDF Reader, offers digital certificates as an integral part of the tool. Others, such as text processers (e.g., MS Word or Excel) require the addition of extensions to act with digital certificates. It is entirely up to the civil registry to acquire the appropriate technology for digital signatures.

In general, the validation of digital signatures occurs more frequently than the digital signing of documents. Given the challenges for civil registries to build a complete infrastructure of operating systems and applications, the implementation of a signature validation system can be sufficient. The simple web interface will allow the user to upload a signed document and check its validity. In the case of mass verifications, an API-based solution can be added to automate the process.

4.14 Mobile Devices and Their Impact on Civil Registry

Global network coverage in remote areas and the use of affordable mobile devices

still have not reached expectations in developing countries. Many rural, mountain, and rain forest areas remain as "white spots" on the maps of the mobile network operators. Many communities that may be connected to broadband may not have a mobile device. The most recent models of smartphones are too costly or unsuitable for low-income populations in remote agricultural communities. The short battery lifetime of some new mobile devices renders them useless in areas were electricity is created by small power generators or solar panels.

These facts should deter civil registries from including plans that depend only on the latest mobile devices to improve birth registration coverage. It is, nevertheless, essential to anticipate these new advancements, given that product cycles tend to be for short periods of time and many features of the new devices are quickly adopted by the older and more robust devices not long after their introduction.

4.14.1 Benefits of a Basic Mobile Phone

Basic, robust mobile phones have become an affordable means of connectivity for poor people. The large investments of Mobile Network Operators (MNO) have considerably increased coverage in rural areas by providing GSM radio (Global System for Mobile Communication) to connect isolated villages, farmers, and hunger-gatherers to the rest of the world. The International Mobile Equipment device ID (IMEI) and the Mobile Subscriber ISDN Number (MSISDN) of a subscriber identity model (SIM) card provide the means to identify and authenticate a user. Poor people in some developing countries are now able to bank by way of mobile phones, as well as receive welfare benefits and subsidies without need of a bank account. They require a permanent residence address or a registered ID card and a mobile phone to enable them to bridge the digital divide. In this way, it is possible to capture birth nonregistrations in remote areas (see Section 2.3.2 for procedures).

Depending on the capacity of the phones, the following technical guidance to assist or create live birth evidence can be considered, using GSM connectivity:

a. Midwife or healthcare professional is registered with a mobile device ID (IMEI) and/or MSISDN.
b. On assisting a live birth, the midwife or healthcare professional sends a message, preferably in text format, or short message service (SMS) to the central birth registry, with the attributes, such as time and date, sex, and location code
c. Optional information can be provided, such as the legal guardian (e.g., mother).
d. The message has an authenticated sender ID (MSISDN) and a basic time stamp.
e. Optionally, through the mobile network operator, the SMS can be amended with meta-information of the cell the SMS originated from. This can be used to ensure that the mobile device was within a certain range of the location ID provided in the message text.

The following steps can be added to increase the trustworthiness of the data and to enable validation of the data sent:

a. The content of the message is received, checked (e.g., no live birth messages later than 72 hours after birth, no SMS accepted from mobile networks further than 50 km from the indicated location of the live birth, etc.) and used to detect errors (data checksum) by way of a challenge/response scenario.[15]
b. The registry system acknowledges the receipt of the message by returning the full content and adding the calculated response ID.
c. The midwife or healthcare professional provides the legal guardian with the response in writing as evidence of the live birth.
d. At the time of the birth registration, the legal guardian(s) indicates the response ID, providing as much of the required information as possible.
e. The civil registry searches for the response ID and compares it with the information provided by the midwife or healthcare professional.

4.14.2 Benefits of Advanced Mobile Phone

While the more advanced devices lack adequate battery life and only few can be considered sufficiently tough to operate in extreme conditions (rain, dust, high humidity), nevertheless, there are many features that can be added to the older, basic models. These include the following:

a. Global Positioning System (GPS)
b. High resolution cameras that support flashlights (some with picture-in-picture functionality)
c. Special civil registry applications
d. High-speed data connectivity (from network providers)
e. Fingerprint sensors (limited availability)
f. Encryption (optional)

The following advanced functionalities will guarantee the confidentiality and trustworthiness of live birth registration processing:

a. Midwife or healthcare professional is registered with a mobile device ID (IMEI) and/or MSISDN, and has the authority to notify, or inform, about the vital event.
b. The midwife or healthcare professional optionally downloads and installs a live birth application with a MSISDN.
c. At the time of the birth, midwife or healthcare professional creates a new entry using the live birth application, which contains the basic required attributes (e.g., time, date, sex, and location code).
d. The application adds to this information a geotagged photo of the midwife or healthcare professional, including a time stamp.
e. OPTIONAL: additional information about legal guardian(s) can be added (i.e., a photo of the ID card(s)).
f. OPTIONAL: midwife or healthcare professional adds a geo-tagged photo of the newborn, together with the legal guardian(s), including a time stamp.

[15] The use of SHA3 as a hash algorithm is one method, which is followed by the execution of a Modulo operation to truncate (digest) the hash to fit into a SMS. The response ID is used as the live birth evidence.

g. OPTIONAL: fingerprint sensor on the device is used to take the fingerprint of the legal guardian, preferably the mother.
h. OPTIONAL: application automatically encrypts the dataset with the public key of the civil registry.
i. OPTIONAL: this authority (who may be the midwife or healthcare professional) digitally signs the data entry with her/his private key.
j. A hash digest (response ID) is created and handed to the legal guardian.
k. The application stores the dataset locally until a mobile network with data connectivity is available.
l. The application transmits the dataset to the civil registry.
m. The civil registry system acknowledges receipt of the live birth to the midwife or healthcare professional.
n. At the time of the birth registration, the legal guardian(s) indicates the response ID and adds as much of the required information as possible.
o. The civil registry searches for the response ID and compares the information to the data that has been provided by the legal guardian(s).
p. Data is confirmed and a birth certificate is issued.

ICT Framework Checklist

Have the following issues or activities been considered?

The following table proposes some basic steps for determining the ICT readiness of the civil registry for birth registration. The exercise should be properly planned and prepared as a work process. During the planning phase, the line of responsibilities must be clearly defined. The checking itself should be properly planned and prepared as a process. Within the planning phase, it should be decided which role is doing the checking. It could be done either by self-assessment, peer review, or independent internal or external audit. These types vary in the degree of independence as well as the costs that come along with it. Maturity models as the "Capability Maturity Model Integration (CMMI)" could provide further input for the preparation phase. Initially, the CMMI was developed by Carnegie Mellon University. It delivers a process improvement program and is required, for example, by the US Department of Defense and other US government contracts. The people actually doing the checking should be trained accordingly. There are special trainings available for auditors (e.g., Auditor for ISO/IEC 27010:2012 ISO/IEC 20000-1:2011, or Certified Information Systems Auditor (CISA)), which might be chosen according to the specific requirements.

The following table provides an initial checklist that could serve as a starting point for assessments. It is strongly recommended to extend this with the entity's controls or overwork it as needed. This table outlines the various controls. The control domain is optional and not exclusive; rather, it could be used to structure an assessment. The comments column provides additional information.

When checking whether the ICT to be used for birth registration is aligned with the following checklist, the individual results could vary depending on the observed implementation. The assessment result of Item No. 1 (process definition) could be, for example, missing, incomplete, improperly documented, unauthorized, and so on. Therefore, no course of action can be provided for all the possible outcomes. It is recommended to install missing or incomplete controls accordingly.

No.	Control	Control Domain (optional)	Comments
1	Is there a process definition for ICT to support birth registration?	Process	Process definition should be documented and authorized.
2	Are the roles and responsibilities clearly defined?	People	Roles and responsibilities should be documented and authorized.
3	Is there an access control concept defined?	Organization	Access controls describe who has the right to what and are a vital security control.
4	Does the actual implementation of the access controls comply with the access control concept?	Compliance	The implementation of the access control concept should adhere to the concept. Regular checks should prove compliance.
5	Do all concepts comply with the legal framework?	Compliance	
6	Is there a change management process?	Process	Changes could occur in many dimensions (legal framework, processes, people, etc.) and should be managed accordingly.
7	Are there training concepts defined?	People	Adequate training of involved people should be assured.
8	Are trainings accomplished according to training concept?	Compliance	
9	Is there a supporting organization available (e.g., IT Help Desk)?	Organization	It is a best practice to establish an IT support organization.
10	It there any IT inventory available?	System	Having a list or a system (e.g., configuration management database) with all established and planned IT inventory helps supporting the IT architect and other.
11	Has a requirement analyses been made (before implementation)?	Process	Requirements for the ICT support should be collected comprehensively.
12	Have the identified requirements been authorized by senior management?	Compliance	Senior management should authorize the requirements before starting the implementation .
13	Have a selection of different ICT architecture variants been juxtaposed?	Architecture	Usually, there is seldom a solution that fits all needs. Therefore, different variants should be taken into account.
14	Were adequate resources provided for each phase in the development process?	People	It should be ensured that adequate staff is available when needed (e.g., software developers in the development phase, test engineers in the test phase and so on).

(continued on next page)

(continued)

No.	Control	Control Domain (optional)	Comments
15	Is there a project management method and plan established?	Process	It is recommended to accomplish the project with the help of project management means (e.g., HERMES, PRINCE2). Such methods also provide guidance and establish what kind of artefacts have to been delivered in the specific phases of the development process.
16	Are all artefacts (documentation, plans, specifications) delivered according to the project management plan?	Compliance	Artefacts should be delivered as specified (e.g., test plan should be available before the test phase starts or user documentation should be available, at the latest, at the time of rollout).
17	Are there test plans available?	Process	Test plans describe what kind of tests have to be done in a specific implementation phase.
18	Are tests accomplished in a dedicated test environment?	System	A dedicated test system should be provided to protect live environment.
19	Are test results documented?	Compliance	Test results should be documented and signed by tester.
20	Are rollout plans available?	Process	The rollout phase requires sound planning.
21	Is an operational concept available?	Process	When going live, it has to be ensured that operation is capable of running the systems. An operational concept describes all aspects of operation.
22	Have availability parameters been specified?	Process	Managing availability includes defining the parameters that the involved components, parts, or even people have to meet (e.g., uptime, acceptable outage rate, response time, etc.).
23	Are monitoring facilities available?	System	Parameters, such as availability or capacity, should be monitored. It is recommended to establish thresholds and define course of action when thresholds are met.
24	Are maintenance plans available?	Process	Maintenance has to be planned (kind of maintenance: e.g., hot fix, regular release, security patch, etc.; role responsible for maintenance; required documentation of maintenance; etc.).
25	Are degradation plans specified?	Process, Organization	Degradation plans should describe "what if" scenarios (e.g.,"what if" network is not available?) and provide course of action.

(continued on next page)

(continued)

No.	Control	Control Domain (optional)	Comments
26	Are business continuity plans specified?	Process	Business continuity management is responsible to ensure continuity of business or restore continuity in case of major incidents. Therefore, recovery needs to be considered (e.g., database backups, archival, standby capacity, etc.).
27	Is there an access control concept for privileged users?	Organization	IT staff, administrator, and so on have more elaborate access rights on IT resources. In order to prevent fraud, a privileged access control concept should be available and implemented.
28	Are there encryption mechanisms in place?	Process	Encryption helps to maintain data integrity.
29	Are the encryption mechanisms up to date?	Process	Outdated security mechanisms represent a risk.
30	Is a technology management established?	Technology	The life cycle of IT technology has to be managed. It should be ensured that replacement of outdated IT technology is addressed in a timely manner.

Chapter 5

Conclusions

Birth registration is a fundamental human right. The registration facilitates access to other rights, provides a person with a legal identity, and facilitates the person's ability to participate more fully in society. Birth registration must be timely, continuous, and permanent. The use of ICT may assist in this. It allows for quicker communication between the place of birth and the registry; it may be more accessible by having technology that can move to the location of the birth rather than travel to the registrar's office; and while technology changes, it allows for records to be stored digitally rather than in paper form, which may be more easily destroyed and may make the capacity to retrieve records difficult.

While ICT offers many possibilities to improve registration, it is essential to understand the broader considerations when introducing new means of working. This publication proposes a systematic approach to the application of ICT to achieve universal birth registration within the civil registry. In doing so, it reflects on the importance of having legal, administrative, and technical requirements in place before its introduction, and the importance of having an environment that is beneficial to the user as well as to the registry. The driving force should be on institutional and administrative capacity building on the supply side, and on raising awareness raising on the demand side.

This publication is the result of a background study and a workshop that examined, worldwide, the good practices and challenges that are associated with introducing ICT for birth registration. There is unanimous agreement that the foundation for upgrading the civil registration system should be the legal framework. This document reflects the cautions relating to the required legislative frameworks and the noted flexibility, such that the legal standards can be applied. It is essential to pay special attention to the privacy and confidentiality of the individual's personal information and the conditions under which data will be verified or authenticated and can be shared. The privacy paradox between the state's need to know and the right

to have one's personal information protected is not easily resolved, but it is one that must be carefully analyzed when introducing electronic recordkeeping.

This publication is explicit that introducing ICT requires adaptation, not only of the staff of the registry but also of the user. It stands that the parent(s) and the State are responsible for the registration of a child. The parent is responsible for seeking to register the child and, in turn, the State is responsible for providing the conditions and facilitating the registration of a birth. There was broad consensus among the participants of the workshop that communication is key to success when a new way of doing things is introduced. The person needs to be comfortable with the changes and understand how these are managed. When changes are introduced, their presentation and implementation should be carefully considered in terms of the socio-cultural context of the society and the changing nature of the family and its dynamics, as well as the increasing need for interoperability between public organizations. Increased need for monitoring and evaluation for a results-based public sector management system will require close supervision of the system from the perspective of the users as well as the quality assurance of the system itself, including through audits and user surveys.

One of the most promising elements of ICT use for birth registration is that it facilitates the registration process for the parent(s) and improves the service delivery. Furthermore, there are considerable cost savings associated with ICT, if rolled out properly, with respect to the time it takes to register the child and the time it takes to provide the birth certificate. There is also great potential to catch potential errors in the record.

There is still a ways to go before ICT for birth registration can be rolled out and implemented in every country around the world. This document attempts to present a broad menu of issues and their relevance for timely and universal birth registration with the help of ICT. More than spelling out the details of the design and implementation phase of a project to move from a paper-based environment to one of electronic records, it presents the logic elements that go into the process. The basic prerequisites for success have been described and the potential pitfalls have been identified.

This document is not only for countries that are planning to modernize the civil registry and facilitate birth registration by introducing ICT; it is also for countries that have already done so. Much already has been achieved in this respect by a number of countries, and they have contributed to the evolution of the use of ICT for birth registration.

References

Federal Adminstration of Switzerland. Undated. *HERMES*. "HERMES project management method for IT, services, products and business organisations." Available at http://www.hermes.admin.ch/index.xhtml.

Harbitz, M. and I. Arcos. 2011. "Identification and Governance Policies: The Legal, Technical, and Institutional Foundations that Influence the Relations and Interactions of the Citizen wit the Government and Society." Technical Note IDB-TN-196. page 14. Washington, D.C.: Inter-American Development Bank.

ICAO (International Civil Aviation Organization). Undated. "MRTD: Welcome to the ICAO Machine Readable Travel Documents Programme." Available at http://www.icao.int/Security/mrtd/Pages/default.aspx.

IDB (Inter-American Development Bank). 2012. "Good Practices in Civil Registries." IDB Project No. RG-T2020. Washington, DC: IDB.

____. 2015. "Dictionary for Civil Registration and Identification." Washington, DC: Inter-American Development Bank.

ISACA. Undated. *ISACA – Webpage*. Available at https://www.isaca.org/Pages/default.aspx.

ISO/IEC (International Organization for Standardization/International Electrotechnical Commission). 2008. ISO/IEC 9001:2008. "The Requirements of a Quality Management System." Geneva, Switzerland: ISO/IEC. Available at http://www.iso.org/iso/iso_9000.

____. 2011. ISO/IEC 20000-1. "Service Management System Requirements." Geneva, Switzerland: ISO/IEC. Available at http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=51986.

____. 2012. ISO/IEC 27010. "Information Technology: Security Techniques." Geneva, Switzerland: ISO/IEC. Available at http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42509.

____ . 2013. ISO/IEC 27000. "Information Security Matters." Geneva, Switzerland: ISO/IEC. Availabel at http://www.27000.org/.

UNICEF. 2007. *Implementation Handbook for the Convention on the Rights of the Child*. New York: United Nations. Available at http://www.unicef.org/publications/index_43110.html.

____. 2013. *A Passport to Protection: A guide to birth registration programming*. New York: United Nations. Available at http://www.unicef.org/protection/files/UNICEF_Birth_Registration_Handbook.pdf.

UN (United Nations). 1948. "The Universal Declaration of Human Rights." Available at http://www.un.org/en/documents/udhr/.

____. 1989. "The Convention on the Rights of the Child." Available at http://legal.un.org/avl/ha/crc/crc.html.

____ . 1998. *Handbook on Training in Civil Registration and Vital Statistics Systems*. Studies in Method Series F, No. 84. ST/ESA/STAT/SER.F/84, New York: United Nations.

United Nations General Assembly, Human Rights Council. 2015. "Birth Registration and the Right of Everyone to Recognition Everywhere as a Person before the Law." Resolution A/HRC/28/L.23. Available at http://ap.ohchr.org/documents/alldocs.aspx?doc_id=24720.

World Bank. 2015. World Development Indicators. Washington, DC: World Bank. Available at: http://wdi.worldbank.org/table/2.1. (Accessed January 30, 2015.)

Annexes

Annex A. Interface Design: Recommendations

While application programming interfaces (APIs) can only define the How something is being exchanged, the question of Why? What For? and Under Which Circumstances? must be addressed by further legislation. It has become commonplace, under "OpenGov" (a cloud-based financial analysis platform on which local governments can collaborate more effectively), to access free-to-use data. There are now specific protection options for personally identifiable information—stored in civil registry databases—that set limits on how and to whom this information can be released.

The legislation on ICT usage in a civil registry must include parameters that relate to how data can or cannot be used. The term "user consent" is of significant importance, since the individual is the owner of his/her personal information at any given time and shall have the power to decide who may or may not access what details in registry ICT systems. If specific data (which may identify the individual through inference) is requested by a third party, legislation should define the means to seek the authority of the individual to release this data, either at request or by means of an opt-in/opt-out option. For example, if an individual moves to a new municipality, the civil registry can offer the person an "opt-out" option to prevent the automated release of data to a third party (e.g., certain agencies and companies). The person's denial to release information can extend to include a relative or ex-spouse, for example, but it cannot include tax authorities who may require that information on the same grounds that it was collected.

The exchange of registry information between agencies within a sovereign state should fall within appropriate legislation that defines the circumstances under which specific data can be exchanged. Currently, there are no binding international standards that relate to the format of these datasets and attributes, although the

OSCI-XMeld standard—applied by Germany for interagency communication—is an option to be considered. OSCI-XMELD is an XML-based technical standard for the exchange of transaction information and can be adopted easily by various ICT vendors.

The failure to standardize data formats will inevitably lead to higher administrative and interagency communication costs. At least one common XML data hierarchy should be considered with basic mandatory fields (e.g., pseudonym Unique ID), while the majority of other datasets and attributes should remain "optional" or "upon request" in order to maintain a low profile in the case of mass data extraction.

Since the investment in ensuring a secure environment can be considerable, it is recommended that a specific legislation relating to digital signatures (including creation, validation, and acceptance) be drafted at the national level to ensure that every citizen, including permanent residents, can apply for an electronic or digital identity (usually referred to as an e-ID). The electronic identity will guarantee the representation of the citizen vis-a-vis federal, state, and local governments, as well as third parties. Further consideration is required for those who are not citizens or permanent residents, yet whose personal data is in the registry. The aspects for consideration should include not only the issue of access itself, but also access in a way that does not result in discrimination as a noncitizen or permanent resident. The individual and civil registry must ensure that the validity of the e-ID[16] is maintained and that it is not subject to fraudulent use.

[16] The e-ID may not be issued and managed by a government agency; rather, the responsibility may be that of a trusted public–private partnership. The e-ID, therefore, should be accepted by any government agency and guaranteed by the civil registry as an approved e-government activity.

Annex B. Glossary[17]

Authentication: (a) The process of establishing confidence in the truth of a claim, which could be any declarative statement. (b) The process by which a user conveys data into a system in order to be recognized and to be able to interact with the system. (c) In biometrics, sometimes used as a generic synonym for certification.

Birth certificate: An original document or certified extract, usually issued by a government authority, that states when and where a person was born and usually identifies one or both of his or her parents as per the legal requirements of each country.

Birth registration: The continuous, permanent, and universal recording within the civil register of the occurrence and characteristics of births, in accordance with the legal requirements of a country. The recording can be physical (in a book) or electronic.

Brownfield Environment: A term commonly used in the IT industry to describe problem spaces needing the development and deployment of new software systems in the immediate presence of existing (legacy) software applications/systems (source Wikipedia).

Certificate of Live Birth: A document, provided by the doctor who attends a birth, certifying the birth of the child. It contains information such as the date and place of birth and the names of the child's parents.

Certification authority: A trusted entity that issues and revokes public-key certificates.

Digital signature: An asymmetric key operation, where the private key is used to digitally sign an electronic document and the public key is used to verify the signature. Digital signatures provide authentication and integrity protection. They have the same validity and legal effects as a handwritten signature.

Digital certificate: An electronic document used to prove ownership of a public key. The certificate includes information about the key, information about its owner's identity, and the digital signature of the certification authority that has verified the certificate's contents are correct.

Enrollment: The process of collecting a biometric sample from an end user, converting it into a biometric reference, and storing it in the biometric system's database for later comparison

Greenfield: A project that lacks any constraints imposed by prior work, i.e. starting from scratch.

Identity: A unique set of features and characteristics that individualize a person,

[17] These definitions are extracted from IDB (2015).

including the name and other biographical data of the individual.

Identification: The determination of identity and recognition of who a person is; the action or process of determining what a thing is; or the recognition of a thing as being what it is.

Legal identity: Legal civil status obtained through civil registration at birth and civil identification of unique attributes, such as a personal identification number and biometrics that recognize the individual as a subject of the law and protection of the state.

Registration: A process by which the authorities note, in a manner established by law, all facts, acts, and records whose occurrence must be recorded authentically in a specialized register.

Root certificate authority: The origin of the chain of trust from a national public-key infrastructure. It is the agency that issues the root certificates for each of the certification authorities registered and certified to operate in a country.

Unique identity: The combination of individually assigned numeric or alphanumeric digits with the biographic and biometric data of a person.

Unique identity number: An attribute in the form of a unique number, used to identify individuals upon their inscription in the civil registration or civil identification system.

Verification: A task in which a biometric system attempts to confirm an individual's claimed identity by comparing a submitted sample to one or more previously enrolled templates.

Annex C. Information and Communication Technologies to Support Birth Registration

ANNE FRANK FONDS
FOUNDED BY OTTO FRANK

IDB unicef

Executive Summary of Proceedings

Bern, Switzerland, 2014

The two-day conference on Information and Communication Technologies to Support Birth Registration, held on December 8–9, 2014, in Bern, Switzerland, identified key issues and provided input to the development of a set of guidelines for the use of information and communication technologies (ICT) in birth registration within the civil registry. Following the introductory remarks, participants discussed five topics: ICT implementation in the birth registration process; legal framework and protection of personal data; data storage and retrieval processes; data transmission; and issuance of certificates. Each session was tasked with identifying (i) steps where ICT is or could be successfully used; (ii) examples of the uses of ICT and the instances where technology has helped or hindered birth registration; (iii) areas where guidance is required when introducing ICT; (iv) key characteristics of a well-functioning system; (v) considerations relating to decentralization and access of vulnerable/minority groups; and (vi) risks and ways to mitigate them.

Buddy Elias, Chair of the Anne Frank Fonds, and Susan Bissell of UNICEF opened the conference. Drawing on stories from his family history, Mr. Elias underscored the risks of violence and exploitation that children everywhere continue to face. Ms. Bissell referred to birth registration as a basic human right and urged participating countries to work to prevent abuse. Mia Harbitz of the IDB summarized the current state of birth registration and legal identity, stressing the importance from an economic and social as well as a human rights perspective.

Session 1 explored the use of ICT to support the birth registration process, with panelists providing examples of countries where it is common and where pilots are underway. Panelists stressed the importance of considering birth registration and technology in light of the policy environment and social and cultural norms. While technology can decentralize the process, it is essential that the frameworks of infrastructure, training, security, and government be in place. Recommendations emerging from the session included the need to have backup and mirror systems for ICT, to take technological resources into consideration, and to strengthen human resources.

Session 2 addressed the legal framework for the use of ICT; specifically, the aspects to consider when introducing ICT and the laws that may need to be revised to

protect personal data. The session focused on applicable legal frameworks and the strengths and risks of rules, registration processes, and interoperability. The discussion centered on the benefits and risks related to multiple databases, the need to accommodate religious or cultural distinctions while protecting the individual from abuse, the use of biometrics, the role of public-private partnerships, and the cost of digitalizing historical versus new entrants. Additional areas included sex identity, children of single mothers, and registration of adoptees. Participants recommended training for civil registrars, streamlining procedures, ensuring timely birth registration, and universal, secure, and interoperable ICT.

The topic of Session 3 was data storage and retrieval processes. The panelists presented some of the technical issues in birth registration data storage and the role of ICT in facilitating or hindering its retrieval. They reviewed selected country experiences in data collection and authentication. Emphasis was given to the importance of defining the type of registry, its purpose, and its mandate. The session examined the migration of records to a digital format, creation and storage of new digital records, and recognition of electronic (or paper) documents as legal tender. The shift to a digital system also implies changes in the registration culture and communicating these changes to the user. The discussion centered on the issues of accuracy, ageing, and linking to older data sets. Participants recommended establishing a strong legal framework and strengthening capacity to search and amend. They also recommended agreements on data sharing, issuance of unique identifiers, establishing electronic data trails, and ensuring centralized data storage with decentralized access.

Session 4 discussed data transmission, specifically, the information to be transmitted, the mechanisms, and the format of transmission of civil registry data. Discussed were the interconnectivity of arrangements and institutional structures in different countries and their impact on service delivery, including during disaster situations and when data may be transmitted across borders. It raised the question of balance—supply with demand; speed with level of service; and value of information versus confidentiality/privacy. The session reaffirmed that any sharing of information must be in the best interest of the individual. The wide-ranging discussion highlighted the difficulty of isolating data transmission from other topics. The recommendations emerging from this session were the need to establish strong legal measures to protect data transmission standards and security; develop a long-term vision and business plan to implement ICT; conduct process re-engineering and redesign before automation; and base system architecture on restricted access.

Session 5 centered on the issuance of certificates. Panelists noted the advances in the ability to issue a certificate through electronic transmission and the options for secure paper on which certificates can be printed. The discussion emphasized the importance of relationships with other authorities and departments regarding ICT implementation and use and the need to have clearly delineated roles/responsibilities. Individual country experiences

highlighted the wide variety in technology usage. Public awareness of and access to birth registration was emphasized as crucial to the introduction or ongoing use of ICT in registration processes. Recommendations that emerged from the session were to develop cooperative agreements; ensure the introduction of ICT takes place only after legal frameworks and government support are in place; make birth registration accessible to all people; make technological solutions simpler, cheaper, faster, and sustainable; and reach those in rural and remote areas with sufficient ICT.

The background paper prepared by IDESA on a research project to access civil registration capacity in Latin America touched on many of the issues discussed in the five sessions. It stressed that the role of ICT in more universal and timely registration and better data integrity depends on the appropriate infrastructure and legal framework in place and the overcoming of cultural barriers. The discussion centered on the importance of the legal framework and the difficulties of birth notification.

A summary of Sessions 1–5 consolidated the main points of adjustment or input to guidelines, in anticipation of group work to follow. Conference participants were divided into five working groups to review the background paper and enrich it with learnings from the five technical sessions. The guiding questions for each topic related to guidelines, risks and opportunities, and implementation.

Group 1 (ICT implementation of the birth registration process) stated that guidelines were essential to distinguish between using ICT in facility and non-facility-based births. The risks and opportunities that were identified included connectivity, costs, skills, security, storage, staff turnover, staff motivation, and interoperability. To implement ICT, the group noted the need for a unique registration system as well as a system for notification, tracking, and monitoring. The group also noted that connectivity, personnel, and interoperability, as well as standardization, were required.

Group 2 (legal framework and protection of personal data) stated that existing guidelines, such as EU and ITU guidelines, UN recommendations, and ICAO standards should be adhered to, and they stressed that a survey on existing legislation should be undertaken. The risks that were identified included identity theft, ethnic conflict, commercial value of the data, verification, and fraud. The implementation issues included security and access to data, the need for a flexible amendment process, and placing adoptive parents on birth certificates.

Group 3 (data storage and retrieval process) suggested making guidelines multidisciplinary; providing continuous training to ICT professionals placed in civil registries; using public-private partnerships for marginal issues rather than core operations; clarifying roles and regulations on data handling; developing ICT policies and procedures internally; and putting audit procedures in place. The risks and opportunities identified were verification, loss, destruction (including in disasters), hacking, corruption, loss of data in disasters, and the need for backup sites. The implementation considerations included strengthening support for the use of multiple languages; establishing plans and designs before implementing ICT;

having in place security applications and a tiered system of access; ensuring integrity through verification mechanisms; and adjusting accounting for changes in storage needs and future technology.

Group 4 (data transmission processes) suggested that guidelines should ensure procedural compliance; secure data transmission; ensure the ability to share vital statistics for validation of personal ID; retain continual staff; and have an internal intranet and sufficient resources for its setup, construction, and maintenance. The risk that was identified was the difficulty to match an individual with a record without biometrics. The implementation considerations that were identified included the encryption of data to ensure its safe transmission and validation procedures in cases of cross-border migration.

Group 5 (issuance of birth certificates) stated that the guidelines should include the timely and secure issuance of birth certificates, a global approach to standardization, provisions for testing and auditing the system, security, and a clear vision of goals. The risks and opportunities included confidentiality, lack of legal framework, IT system failures, insufficient technology, and payment by credit card. The implementation issues discussed were the identification of constraints, execution of good governance and piloting, implementation in phases, standardization across regions and borders, and the use of barcodes to secure documents.

The closing session provided participants an opportunity to make brief statements on their final thoughts.


unicef
IDB