MPUELE
MINISTRY OF PUBLIC UTILITIES, ENERGY, LOGISTICS & E-GOVERNANCE
"Building a green future via Service, Innovation & Transformation!"

BELIZE NATIONAL IDENTITY STRATEGY

CONTENTS

6

Acronym List

ABIS: Automated Biometric Identification System

BHIS: The Belize Health Information System

BTS: Belize Tax Service

CA: Certification Authority

CITO: Central Information Technology Office

CR: Civil Registration

CRVS: Civil Registry and Vital Statistics

CSTF: Cyber Security Task Force

DTU: Digital Transformation Unit

EBD: Elections and Boundaries Department

EBC: Voter Identification Card System

ECLAC: Economic Commission for Latin America and the Caribbean

EtD: Electronic Travel Documents

EU: European Union

GoB: Government of Belize

ICAO: International Civil Aviation Organization

IDB: Inter-American Development Bank

ITU: International Telecommunication Union

KYC: Know-Your-Costumer

LOA: levels of assurance

MOHW: Ministry of Health and Wellness

NIN: National Identity Number

NIRA: National Identity and Registration Authority

OAS: Organization of American States

PKI: Public Key Infrastructure

SSA: Social Security Act

SSB: Social Security Board

SSC: Social Security Card

SSN: Social Security Numbers

TIN: Tax Identification Number

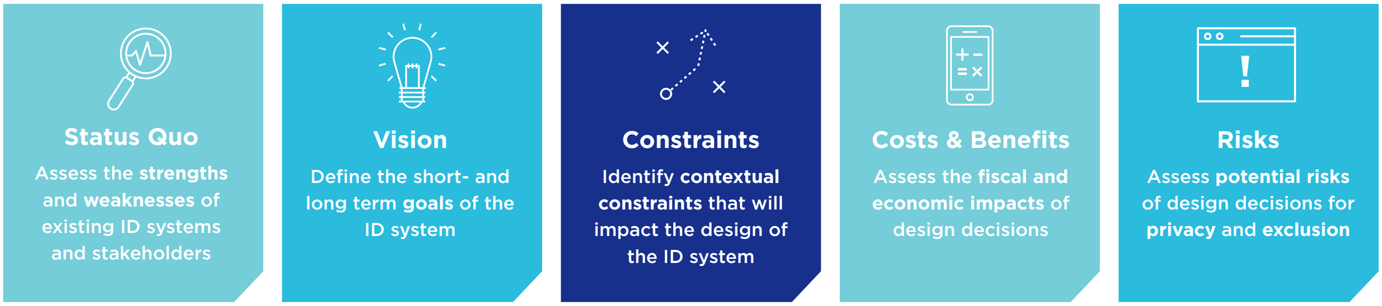
UDN: Unique Document Number

UNDP: United Nations Development Program

VSU: Vital Statistics Unit

Introduction

This document describes the Belize Digital Identity Strategy. It follows the ID4D Practitioner's Guide recommendations and is divided into five steps: status quo, vision, constraints, costs and benefits, and risks.



Status Quo
Assess the **strengths** and **weaknesses** of existing ID systems and stakeholders

Vision
Define the short- and long term **goals** of the ID system

Constraints
Identify **contextual constraints** that will impact the design of the ID system

Costs & Benefits
Assess the **fiscal and economic impacts** of design decisions

Risks
Assess **potential risks** of design decisions for **privacy and exclusion**

In addition, it includes two additional sections on national ID system decisions and recommendations and next steps and timeline.

The document is structured as follows:

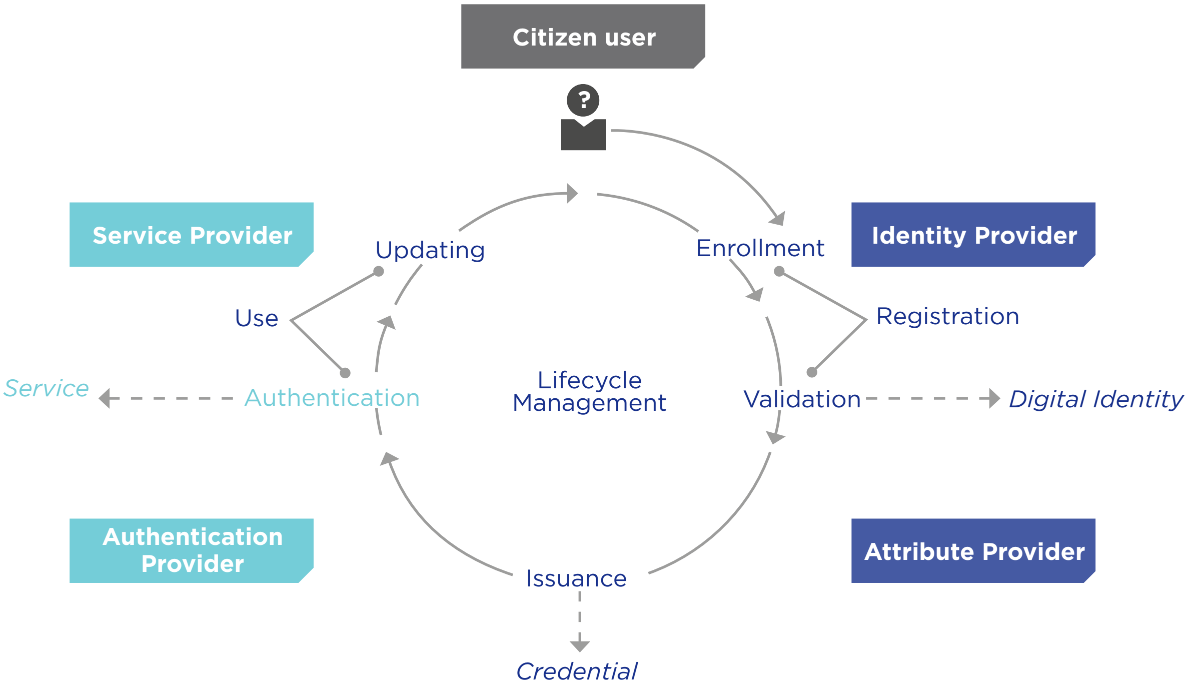
1. An introduction to the digital identity framework and pertinent vocabulary.
2. A review of the Belize identity ecosystem, which anchors the proposed National ID System.
3. Outputs from the second workshop, where the vision of the National ID System was shaped, including goals and use cases that should drive its implementation.
4. Limitations of the context of the National ID System.
5. The major decisions that must be taken before implementing the National ID System and some recommendations.
6. An estimate of the fixed and recurrent costs.
7. Risks that the project may face, which will help design strategies to minimize their occurrence and mitigate their impact.
8. A timeline and a detailed description of the next steps.

1

Digital Identity

Digital Identity

To fully understand a digital identity system, it is important first to define the terms that comprise it. Identity is defined as "who a person is, or the qualities of a person or group that make them different from others."[1] A digital identity is a collection of electronically captured and stored identity attributes that uniquely describe a person within a given context and are used for electronic transactions. A digital identity system refers to the systems and processes that manage the lifecycle of individual digital identities."[2] The person's digital identity consist of biographic data (e.g., name, age, gender, address), biometric data (e.g., fingerprints, iris scans, handprints), and other attributes that are more broadly related to what the person does or something someone else knows about the individual.[3] The following diagram depicts the identity lifecycle, which can be summarized in the operations of enrollment and validation.[4]



[1] https://dictionary.cambridge.org/dictionary/english/identity.

[2] Technical Standards Technical Standards for Digital Identity Systems for Digital Identity. World Bank, 2017.

[3] Ibid

[4] Ibid

A digital identity system refers to the systems and processes that manage the lifecycle of individual digital identities.

- **Enrollment**
  This is the process for capturing and recording the identity attributes from a person who claims a certain identity, which may include biographical data (e.g., name, date of birth, gender, address, email), biometrics (e.g., fingerprints, iris scan), and an increasing number of other attributes. Which attributes are captured during this phase and the method used to capture them have important implications for the trustworthiness of the identity.

- **Validation**
  Once the person has claimed an identity during enrollment, this identity is then validated by checking the attributes presented against existing data. The validation process ensures that the identity exists (i.e., that the person is alive) and is claimed by only one person (i.e., it is unique in the database). In modern digital identity systems, uniqueness is ensured through a deduplication process using biometric data. Links between the claimed identity and identities in other databases (e.g., civil registries, population registries, and so on) may also be established.

In Belize, these two processes are executed by the National ID System. The validation process includes the verification of biographical attributes against each of the corresponding issuing systems: Vital Statistics Unit (VSU) for the birth certificate for citizens and the Immigration Department for residents.

- **Issuance**
  Once an identity has been validated, some kind of credential must be issued, in order for the person to prove their identity in a simple and secure way. There are several ways to do this, and these are not mutually exclusive: a person may have several credentials issued from the same national ID system for different purposes. For instance, a credential may be an ID card, where some information about the person is stored, but a credential can also be a digital certificate stored on a mobile app. In the first case, the ID card can be used on physical transactions (for example, to enter a government building) and the mobile app to perform electronic transactions (for example, confirm a bank wire transfer).

- **Authentication**
  Once a credential is issued, it will be used for the owner to prove identity. The level of assurance is the degree of confidence a third party can have on a claimed identity. It is composed of several parts since the confidence on the information provided for authentication is related to each step in the identity lifecycle.

From an identity management point of view, enrollment/validation is separate from credential issuance. In practice, this means that once the data are collected and validated, the credentials to be issued are totally independent. Moreover, several credentials may be issued for the same identity. This is the case in most countries that make use of digital identity.

Frameworks

The framework of digital identity consists of standards and regulations related to identity management. Two of the most important are the following: ISO/IEC 29115 - Entity Authentication Assurance Framework[5] and eIDAS – Electronic Identification and Trust Services.[6]

ISO/IEC 29115 is an international standard that defines four levels of assurance for different needs and authentication services. The following diagram (from ISO/IEC 29115) illustrates the three major blocks into which ISO/IEC 29115 organizes the identity lifecycle: enrollment phase (including Identity verification/vetting), credential management phase (including credential issuance) and entity authentication phase:

	TECHNICAL		MANAGEMENT & ORGANIZATIONAL
ENROLMENT PHASE	• Application and initiation • Identity proofing • Identity verification	• Record-keeping recording • Registration	• Service establishment • Legal and contractual compliance • Financial provisions • Information security management and audit • External service components • Operational infrastructure • Measuring operational capabilities
CREDENTIAL MANAGEMENT PHASE	• Credential creation • Credential pre-processing • Credential initialization • Credential binding • Credential issuance • Credential activation	• Credential storage • Credential suspension, revocation, and/or destruction • Credential renewal and/or replacement • Record-keeping	
ENTITY AUTHENTICATION PHASE	• Authentication • Record-keeping		

[5] ISO/IEC 29115:2013 - Information Technology - Security Techniques - Entity Authentication Assurance Framework.

[6] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0910).

eIDAS is the European Union's regulatory framework for identification and trust services, with an important focus on interoperability. Although eIDAS considers some of the concepts presented in the ISO/IEC 29115, it is not formally based on it. Conceptually, both define a number of levels of assurance (four in the case of the ISO/IEC 29115 and three in eIDAS), but the requirements vary for each level.

Levels of Assurance

The level of assurance (LoA) concept is included both in ISO/IEC 29115 and eIDAS and is related to the confidence a third party may have in an identity claim made by a given entity (a person, a system, or an organization). Obviously, the LoA depends on the risks that the third party may incur if the identity is not the correct one. For some transactions, there is no risk at all, while for others the risk will be very high. An important concept in digital identity is that there are different LoAs for different authentication requirements.

ISO/IEC 29115

This standard defines four levels of assurance: low, medium, high, and very high.

LEVEL	DESCRIPTION
1 | LOW	Little or no confidence in the asserted identity
2 | MEDIUM	Some confidence in the asserted identity
3 | HIGH	High confidence in the asserted identity
4 | VERY HIGH	Very high confidence in the asserted identity

The following describes each level.

- **LoA1:** There is minimal confidence in the asserted identity of the entity being authenticated, but some confidence that the entity is the same over consecutive authentication events. A typical case is the registration of a user on a news web page to receive an email with the latest news.

- **LoA2:** Some confidence in the asserted identity of the entity exists. Single-factor authentication is accepted for this level, but the authentication must be done through a secure authentication protocol. For example, changing personal data on a non-critical organization (changing billing address) may be considered to require a LoA2 authentication.

- **LoA3:** There is high confidence in the asserted identity. It is used when there is substantial risk of erroneous authentication. This LoA should employ two-factor authentication. It is expected that identity proofing procedures were executed during enrollment phases. All exchanged information should be cryptographically protected. Examples of the need of this kind of LoA is the confirmation of a bank transfer.

- **LoA4:** This is the highest level of assurance. It is similar to LoA3, but it adds in-person identity proofing and the use of tamper-resistant hardware devices for the storage of all the secret or private cryptographic keys. Additionally, all personal information included in the authentication protocols shall be cryptographically protected.

eIDAS

International standard ISO/IEC 29115 has been considered for the specifications and procedures set out in this implementing act as being the principle international standard available in the domain of assurance levels for electronic identification means. However, the content of Regulation (EU) No 910/2014 differs from that international standard, in particular in relation to identity proofing and verification requirements, as well as to the way in which the differences between Member State identity arrangements and the existing tools in the EU for the same purpose are considered. Therefore, the Annex, while building on this international standard, should not refer to any specific content of ISO/IEC 29115. Thus, although related, compliance with eIDAS does not mean automatic compliance with ISO/IEC 29115. eIDAS defines three levels of assurance:

LEVEL	DESCRIPTION
1 | LOW	Limited degree of confidence in the asserted identity
2 | SUBSTANTIAL	Substantial degree of confidence in the asserted identity
3 | HIGH	High degree of confidence in the asserted identity

The LoA is described in detail in the Commission Implementing Regulation (EU) 2015/1502. In particular, for each component or subsystem of the identification scheme, a complete set of technical specifications and procedures are listed. Additionally, this link contains a summary of the situation of each European eID scheme in relation to eIDAS: https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS.

2

Belize Identity Ecosystem

Belize Identity Ecosystem

There are a number of main stakeholders in the Belize Identity Ecosystem, identified by the following means:

- An extensive questionnaire sent to each organization (see annexes).
- Documentation provided by the government of Belize (GoB).
- Direct communication by email or conference calls with representatives of each organization.

When needed, public information available on the corresponding webpage was also included. Because Belize does not have a national identity system, Belizeans have taken advantage of a number of functional identities systems. The most frequently used functional identities are the Security Board Card Registration System (social security ID and corresponding card) and Ministry of Immigration (passport number and corresponding passport booklet). Two additional systems frequently used are elections and boundaries department (voter's ID card) and Belize Tax Service (tax identification number). Information on each of these organizations is presented in six subsections with the aim of easily mapping one system with the others:

- Overview of the organization
- Overview of the identity system
- Identity management processes
- Identification number
- Certificates
- Authentication and other identity services
- Technical details of the solution

Because Belize does not have a national identity system, Belizeans have taken advantage of a number of functional identities systems

A review of the VSU (in charge of issuing birth certificates) is also included, as civil registries and birth certificates are key elements for the creation of an identity for all of these functional systems (birth certificates are also a key element in most national identity systems worldwide).

Finally, two other stakeholders were reviewed and analyzed as part of the future digital identity ecosystem: a company registry and the Central Bank of Belize.

Social Security Board

The social security card (SSC) is the most widely used functional ID in Belize. It is the de facto identity system.

General Overview of the Organization

The Social Security Board (SSB) is a statutory corporation of Belize which administers the country's Social Security Fund. It was established in 1981 by Part IV of the Social Security Act.[7] Citizens can obtain their social security card by registering at the SSB. It is an independent body, part of the portfolio of the Minister of Finance, who appoints a board of directors to administer the program; directors representing employers and employees are nominated by their respective organizations. The CEO reports directly to the board, which has nine branch offices and a headquarters office with 11 units. All branch offices issue SSCs. There are 338 employees, 9 of whom are involved in the issuance of identity documents.

Overview of the Identity System

As it was mentioned before, the de facto identity system in Belize is the Social Security Card Registration System, a web-based application created in June 1981. The card was issued for the first time in January 2000. The official Belize identity system is being deployed that will include biometrics (10 fingerprints acquisition).

Coverage

The target population is all Belizeans, registered aliens, work permit holders, and their dependents. Belizeans should be registered starting at 30 days after birth. Foreigners can apply once they have obtained permanent or temporary status in Belize, such as permanent residency, naturalization, and a valid work permit, among others.

Categories

There are three categories: minors (under 14), adults (permanent resident of Belize, including Belizeans, and youth over 14), temporary (temporary resident of Belize and youth over 14).

[7] Chapter 44, Social Security Act.

Identity Management Processes

Enrollment and Required Documents

To enroll in the Social Security System, the applicant must apply (online or in person). Then, the applicant must visit an office in person to provide required documents for verification and scanning. A photograph and signature are captured for those 14 years of age and older). No other biometrics are included/requested at this time, but a project is in progress that will also request the applicant's fingerprints. The applicant pays the corresponding fee (conditions apply) and this completes the enrollment process.

The documents required to apply are: birth certificate, passport, change of name document, and immigration documents which grant permission to live and work legally in Belize. All documents stated by law (and described before) are required. Any exception needs CEO approval.

Vetting

Vetting is performed based on biographic information. The SSB has access to a copy of the VSU records updated once a month. When an inconsistency or other issue arises, the officer performing the vetting is notified, and they send the corresponding query to the VSU directly. In the future system, fingerprints will be used to do a de-duplication of the database.

With regard to the breeder documents (birth certificate and passport) there is no automatic verification process. With respect to guaranteeing uniqueness, that is, ensuring that a person is registered only once in the database), a person should only be registered once, but there are times when a person is double registered in error. An example is when a person changes their name, such as due to marriage.

Biometrics

Starting in 2022, SSB is taking the 10 fingerprints at each renewal (or new enrollment) process. Each fingerprint is processed to obtain a template, which is then stored in the system (the fingerprint image is not stored: once the template is obtained, the image is discarded). All biometric information is stored on the cloud in cooperation with the biometric system supplier, Fulcrum Biometrics, a Fujitsu company. Details of the implementation have been discussed and can be disclosed on request. The process to create a biometrics database is based on the usual renewal process: the expectation of the SSB is to complete this process without the need for a compulsive and massive re-enrollment process.

Issuance

The estimated time to obtain the card is five working days.

Identification Number

The Social Security Identity System identifies each new register with a 9 digit ID Number (we will refer to it as **Social Security Number**). The number is generated sequentially, following the time of record approval. The numbers are generated automatically by the system and thus, there are no possible number duplicates.

Certificate

The Social Security Identity System issues a physical card. There are three different types of cards, one for each category: minor, adult, and temporary. In the last year, it produced 39,918 cards (including new enrollments and renewals).

The card has a barcode and security features: it has holograms, micro-printing, and UV printing. It also includes pre-printed data from the manufacturer and printed data obtained from the system during personalization. The barcode is mainly for internal processes: it is basically the document number. There is also a magnetic stripe, but representatives of the SSB stated that it is not used (although it is still encoded). The data printed on the card is: ID number, sex, full name, nationality, date of birth, period of validity (issue and expiry dates), captured signature, and photograph (for age 14 and older). It also includes employment status. The card is free the first time it is issued in all cases except those with temporary immigration status (in which case the cost is $26.00). The cost for renewal is also $26.00, and this applies to all cases. Finally, the individual may face other costs: ID photograph, certificates, and photocopies during enrollment. Finally, the CEO can waive card fees in certain circumstances. Cards issued for Belizeans older than 14 years do not expire.

Authentication and Other Identity Services

The SSB has a validation service. This service is provided to third parties. It works as follows: given a set of biographic data and the social security number, the service answers only Yes/No with a confidence index regarding the answer. For example, if the match with the existing data is complete and only one register is found, the confidence index is maximum. Only via memoranda of understanding and signed agreements can institutions access the database.

Technical Details

Database

Photographs and signatures are recorded in the database for individuals 14 years old and older. The new system (October 2022) will also collect fingerprints. The system is linked to the birth and death registry as follows: the birth or date of death information recorded on a birth or death certificate is entered into the registered persons' record at the time of registration, record updating, or claiming a death benefit. For all submitted documents, the document number, issue and expiration dates are stored in each registered person's record. This registration depends on the availability of birth and death certificates being created by VSU. Often, the death registration requires some time depending on the cause and location of death (in-country versus overseas).

Security

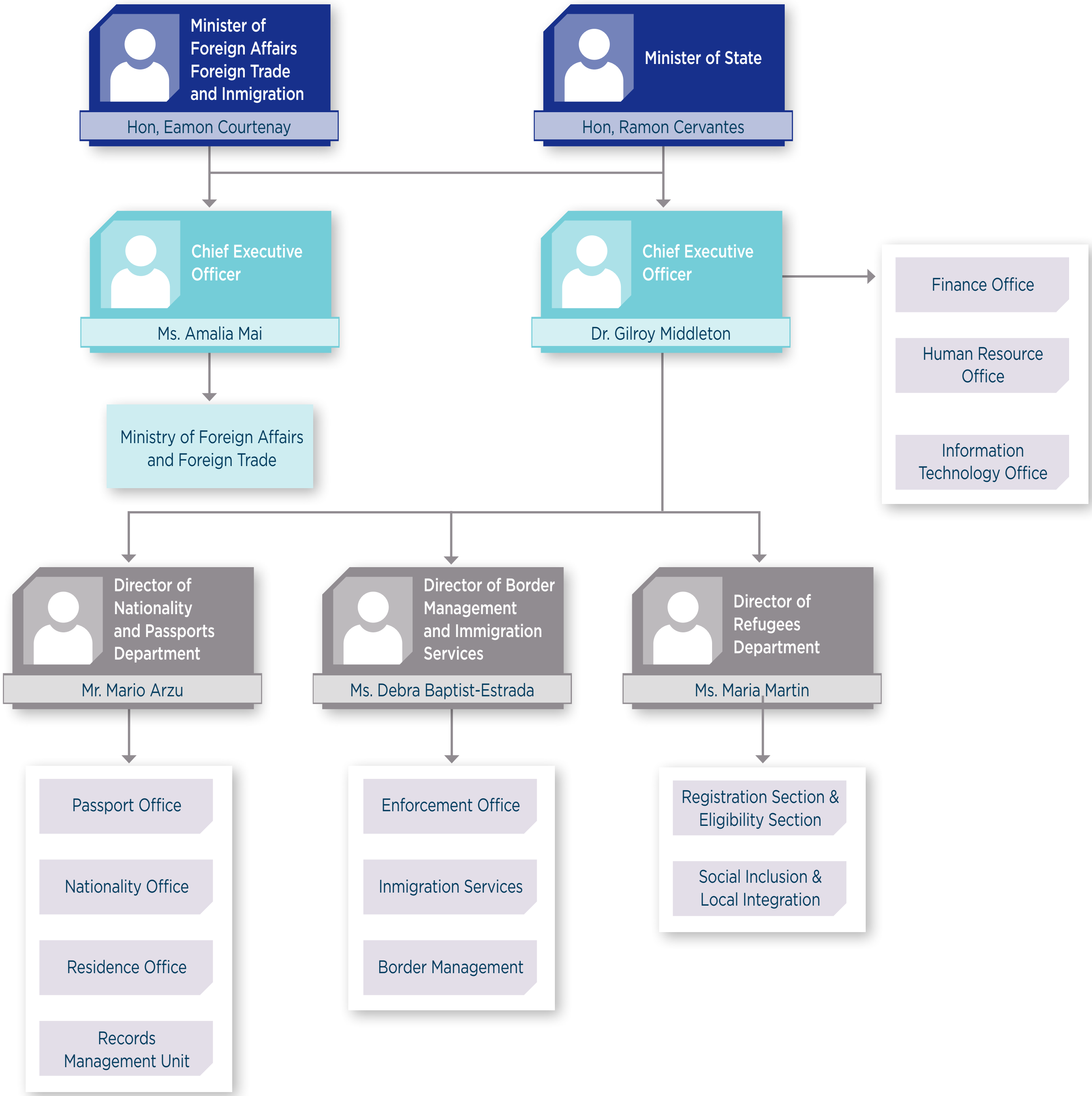
The SSB has an Information Security Policy in place. With respect to separation of duties and accesses, there is a role assignment mechanism to create and manage roles with specific access levels. Finally, the CEO must approve access to the data outside the scope of each role.

Ministry of Immigration

The passport is the second document in order of relevance used as a source of identity in Belize. Usually, when no social security card can be provided, a passport is accepted as proof of identity. This Ministry issues passports for Belizeans and is responsible for the issuance of citizenship, residence, and permits.

Overview of the Organization

The Ministry of Foreign Affairs, Foreign Trade, and Immigration has one central office and offices in two land border ports, four seaports, three districts, and one airport. It also operates in seven missions abroad. The documents related to identity management (passport, nationality, residence) are issued by the Nationality and Passport Department (see chart below).


Minister of Foreign Affairs Foreign Trade and Immigration
Hon, Eamon Courtenay
Minister of State
Hon, Ramon Cervantes
Chief Executive Officer
Ms. Amalia Mai
Chief Executive Officer
Dr. Gilroy Middleton
Finance Office
Human Resource Office
Information Technology Office
Ministry of Foreign Affairs and Foreign Trade
Director of Nationality and Passports Department
Mr. Mario Arzu
Director of Border Management and Immigration Services
Ms. Debra Baptist-Estrada
Director of Refugees Department
Ms. Maria Martin
Passport Office
Nationality Office
Residence Office
Records Management Unit
Enforcement Office
Immigration Services
Border Management
Registration Section & Eligibility Section
Social Inclusion & Local Integration

There are an estimated 220 officers, with approximately 60 involved in ID management:

- Data entry clerks/issuance clerks: approximately 25.
- Approvers: approximately 15.
- Personalization operators: 7.
- Other roles: 10.

Overview of the Identity System

In the case of Immigration, there are four different systems related to identity management:

- Passport system: Started on February 2005, with a new system scheduled to deploy on October 2022.
- Border card system: Started in March 2017.
- Residence system: Started in June 2020.
- Refugee system: Started in 2018.

In all the previous cases, the system is fully IT integrated. The only manual system is the Nationality Certificate (which has no IT infrastructure).

Coverage

It depends on the system, but in all cases cover all ages, starting from birth:

- Passport: all Belizeans.
- Residence Card: all non-Belizeans who qualify for residence.
- Border Card: all Belizeans, holders of Temporary Employment Permits employed in the free zones, qualified retired persons, Guatemalan minors studying in Belize, Mexicans.
- Nationality Certificate: non-Belizeans who qualify for nationality.
- Refugee Card: Individuals approved for recognized refugee status.

In figures, the target population for each system is the following:

- Passports – estimated at 420,000
- Residence Cards – estimated at 3000 yearly
- Border Cards - estimated at more than 420,000
- Nationality Certificate – estimated 2000 yearly
- Refugee Card – estimated at 25 yearly

Categories

- Passport: regular, official, diplomatic, and temporary.
- Residence Card: permanent and temporary.
- Border Crossing Card: regular, student, freezone, and qualified retiree program.

Identity Management Processes

Enrollment and required documents

All issued cards/certificates have a similar process:

- Acceptance – clerk – at any immigration office.
- Approval – Section Supervisor – at HQ.
- Personalization – Personalization Operator - at HQ.
- Issuance – clerk – at any immigration office.

The applicant presents the form and the required documentation at any immigration office, where a clerk performs a first check. Clerks have basic training to detect fraudulent documents. They keep the original BC and a copy of the card. They contact the Social Security office via email if they find an irregularity.

Passport

The applicant must provide a birth certificate and a photo identification. There are two IDs that are accepted: SSC and the voter card. The application is not accepted without the proper documentation. For passports, fingerprints are also collected. In the actual system, they capture the two indexes. For the new implementation, they will capture all 10 fingerprints.

Residence

To apply for residence, individuals must be legally residing in Belize to access this service. For individuals who have had a long stay in Belize without the proper legal status, an amnesty program or a legalization procedure needs to be followed.

Required Documents

Every process requires different documents but in general the following documents are accepted: passports, birth certificate, valid ID (SSC or voter's card), marriage certificate, deed poll, and nationality certificate.

Biometrics

A picture is taken at time of registration for all services (digital facial image). For passports, two fingerprints (indexes) are needed. In the new system, all 10 fingerprints will be captured. This means that the process of creating the biometrics database will be driven by the renewal process. For border cards, a digitized holograph signature is required.

Vetting

For residence, a precheck is done to avoid duplications in the system, but in the case a duplicate is created, no procedure currently exists to eliminate the duplicate. For the remaining systems, pre-checks and searches are done prior to the creation of a new application. Duplicate records are cancelled. Biometrics are not used during vetting. The new system will include fingerprint matching. Details of how the new fingerprint matching will be used to clean the existing database will need to be discussed during the next phase of the National ID program.

Issuance

The time to complete the process and obtain the required document is as follows: new applications: 1 day to 20 days; renewal: 1 day to 20 days; and lost or stolen: passport 6 weeks; other documents do not have a time limit.

Identification Number

No Identification number is printed on card/passports; only the document number corresponding to the physical certificate (passport or card). In addition, and because of the issue with the biometrics system mentioned before, no biometric vetting is performed. This is why each new application is considered as a new registry.

Further analysis will be necessary to understand the implications of this fact, as there is typically a hierarchy between the person registering and the ID number assigned versus the document number assigned to that person if their application is successful.

Certificates (Document issued)

The Ministry of Immigration could not give an estimate of the total of documents issued from the beginning of the IT systems. The following is the approximate documents issued per year per system:

- Passports: produce 20,000 yearly.
- Residence cards: estimated at 3000 yearly.
- Border cards: produce 10,000 yearly.
- Nationality certificate: estimated 2,000 yearly.
- Refugee card: estimated at 25 yearly.

The following table describes the types of certificates issued under each system, their main security features, associated costs, and validity. All services require the submission of a secondary official ID with photo and photocopies, and translations of non-English documents when required.

SYSTEM	CERTIFICATE	CHARACTERISTICS	SECURITY FEATURES	VALIDITY
Passports	Booklet	Passport grade security features	Holograms, micro printing, UV printing, Tactile	5 to 10 years
Residence cards	MRZ Card	PVC, serialized with MRZ zone, secure laminate and designed blank card	Holograms, micro printing, UV printing, Tactile	5 years
Border cards	MRZ Card	PVC, serialized with MRZ zone	Tactile	1 year
Nationality certificate	Secure Paper	Secure, watermarked, serialized blank certificate	micro printing, UV printing	No expiry
Refugee card	MRZ Card	PVC, with MRZ Zone and secure laminate	Holograms	

Associated costs for each system:

DOCUMENT	COST
PASSPORTS	Regular fee $50.00 Adults/$30.00 Minors, expedite fees: 50, 100, or 200 additional to the regular fee. These fees are being revised to reflect the new costs of production of the ePassports. Replacing or stolen passport fees: $85.00
RESIDENCE CARDS	$300.00 for five years Replacing or stolen card fees - $300.00
BORDER CARDS	$40.00 per year Replacing or stolen card fees: None
NATIONALITY CERTIFICATE	A processing fee of either $40.00, $100.00 or $300.00 Replacing or stolen card fees: $ 100
REFUGEE CARD	No cost. Recognized Refugee Card deployed in collaboration with the UNHCR agency.

Authentication and Other Identity Services

In the case of Immigration, no other agency accesses the immigration database, and no services are available for verification purposes.

Technical Details

Database

Voter ID, birth certificate and Social Security ID are stored on the database. From biometrics, they also stored fingerprints and digital face image (for passport) and digital face image only for all other documents.

Security

Depending on the responses obtained, the Ministry of Immigration has a number of security policies in place: Process Regulations and Procedures, System and Network Security Policies and Procedures, and Database Security Policy and Procedures. Data are not encrypted, but communication between offices and systems is encrypted. Physical access to servers is monitored and regulated. Physical access to computers is monitored and restricted to personnel. During the course of the preparation of the technical requirements for the National ID System, a more complete assessment of the security framework of existing ID systems will have to be performed on site in Belize.

Elections and Boundaries Department

The voter's card is also one of the most frequently used documents in Belize for identity verification.

Overview of the Organization

The Elections and Boundaries Commission and Department are responsible for registering voters to ensure that eligible persons have an opportunity to vote. The Elections and Boundaries Department reports to the Ministry of Public Service, Constitutional and Political Reform and Religious Affairs on staffing and financial matters. There is one central office which prints all ID cards, and 15 registration offices countrywide. All offices distribute ID cards. There are a total of 70 employees.

Overview of the Identity System

The department issues a Voter's Identification Card. This ID card is designed and printed from a Card Five Software. The data from Microsoft Access Files are connected to the software, and ID cards are sent to print. The Voter Identification Card System (EBC from now on) stores all voter registration data without images. The Taranis system stores both data and images. The Software EBC was built by the Organization of American States (OAS). The ID card issued by the EBD is the Voter Registration Card. According to the answers in the survey: "We have lost the ability to do electronic searches with the Vital Statistics Unit. We are only able to submit information for them to cross check and provide feedback. Our access to remotely search their system has been discontinued."

The identification system was created in 2010 and replaced the typewritten laminated picture ID cards. However, slight modifications to color were made in 2018 to make it more easily identifiable due to re-registration exercise. There are no specific social protection programs using the identification system. ID cards issued are used and accepted as secondary ID for persons obtaining services at the Belize Social Security Board and the Immigration Department.

The Representation of the People Act is the legal framework for the voter's card.

Coverage

The age at which one is eligible to apply for a Voter's ID card is 18. Out of the total population of 220,000, 186,897, or 85 percent, are 18 years of age or older.

Categories

Only one category of ID card is issued. However, the official responsible for each office signs the ID cards. All cards are printed at the Central Office.

Identity Management Processes

Enrollment and Required Documents

Applicants must present themselves in person with a source document to prove nationality and required time at given address. Source documents are verified with the Vital Statistics Unit or Immigration Department manually, on an ad-hoc basis (there is no service online). Commonwealth citizens are required to show stamps in their passports to prove that they have been residing in Belize for one year consecutively, as required by the Representation of the People Act.

Required Documents

- Belizean birth certificate.
- Nationality certificate, passport or deed poll.

At enrollment, the applicant provides a photo, which is incorporated into the enrollment data.

Vetting

There are no biometrics involved in the vetting process. Regarding biographic information, checks are made with the Vital Statistics Unit or Immigration Department to verify information.

If the applicant cannot produce a valid birth certificate, then their information is taken and verified with the Vital Statistics Unit or Immigration Department. Additionally, to verify residence, an investigation is carried out at the address given by the applicant. The applicant's name is published on a supplementary list, and if there are any objections, the matter is heard in open court and the reviewing officer determines whether the name of the applicant remains on the list. Only after that process is completed is the applicant a registered elector and eligible to be issued a Voter's ID card.

Demographic information is entered into the database (names, dates of birth, sex, address, date of residence at given location, occupation, place of employment, marital status, document type, document number and document issue date, color of eyes, skin, and distinguishing marks).

A homonymous report is run to detect if there are any duplicate voters. Once those are identified, electors are given the option to select which registration they will keep and the other is removed. If the elector does not respond to the letter the last registration remains. This is mandated in the Representation of the People Act.

There is no direct link with any system so verification against BC or Passport is done outside the system.

Identification Number

The Voter Registration Number is the number assigned to an application upon the completion of registration. The first 2 digits identify the electoral division in which the elector is registered. This number does not change even if the person changes address and resides in another electoral division. The voter's ID given remains with that voter until another re-registration exercise is conducted.

Document Issued

The specifications for the Voter's ID Card are outlined in the Representation of the People Act therefore changes would need to be made to the laws in respect to any proposed changes in respect of the voter's ID card.

Only one category of ID card is issued. However, the officer responsible for each office is responsible for signing the ID cards. All cards are printed at the central office.

Last year: 4,100
In total: 250,000

The card is a PVC card with holograms as security features. The information printed on the card is: ID number, last name, address, sex, date of birth, date issued, registration number, place of birth, color of eyes, height, distinguishing marks, first name, color of skin, signature of elector, Chapter 9 of the Laws of Belize. No MRZ.

Time required

- New registration 1 month 1 week (this is due to the cycle of registration as ID is only issued after the name is approved by the official on the voter's list).
- Renewal - 1 week.
- Lost or stolen - 1 week.
- Corrections -1 week, rectification of particulars - 1 month 1 week (requires publication and therefore has to go through the monthly registration cycle).

Expiration

ID cards are not replaced. However, after a re-registration exercise due every 20 years, a new ID card is issued.

Cost

Free, but renewal costs $5.00 for first replacement and $10.00 for subsequent replacements.

Authentication and Other Identity Services

The Voter's ID card is used to obtain a cell phone account, a passport and to vote, as well as to apply for the social security card. The Voter's ID is valid throughout the country but only recognized by a few institutions.

Technical Details

Database

- Deceased persons are removed from the database (required by law). To verify the deceased's identity, the information is received from the Ministry of Health on names and date of birth for deceased persons. Officers use death announcements, information from funeral homes, and other sources to get information. Once the information is gathered, officers personally visit the addresses of these individuals to confirm with a relative that the person is deceased. Once the death is confirmed, they remove the name from the list of electors.

  Note: deceased persons can only be legally removed during the months of February, May, June, July, August and at Annual Review (November) of each year. The date of birth is critical because several people may have the same name. If a relative cannot confirm the death, the person's name remains on the voter's list until it can be verified with certainty.

- Other numbers stored are the voter's card, birth certificate ID, SSC, and passport.

To verify the deceased's identity, the information is received from the Ministry of Health on names and date of birth for deceased persons.

Security

From a security standpoint, the EBD reported in the answers from the questionnaire that the data is not encrypted. Also, some isolated cases of corruption were detected.

Belize Tax Service

The Belize Tax Service assigns a tax identification number for individuals and companies. There is no special certificate issued and because of that, this tax identification number is not used as proof of Identity.

Overview of the Organization

The Belize Tax Service (BTS) is a department within the Ministry of Finance. The BTS has a headquarters (central office) and seven regional offices. Currently it has about 240 employees. Taxpayer Services is the main unit assigned to work with Registration. About 40 employees play a role in the registration process. Any officer can register a taxpayer. However, the branch offices only have the authority to register employees, while all other types of taxpayers must be registered at headquarters.

Overview of the Identity System

The tax identification number (TIN) is an ID issued by the department for all individual and non-individual taxpayers. The enterprise application automatically generates a random number. The GoB revenue system has been in operation since 2002. The Customs Department uses the TIN to verify that a company is registered before doing business with them. The system covers employees, shareholders, companies, partnerships, sole proprietors, NGOs, government, educational institutions, and international companies. It represents all employees and businesses. Approximately 105,000 taxpayers are considered active, and more than 250,000 identities have been issued since the system's inception.

Identity Management Processes

Approximately 105,000 taxpayers are considered active, and more than 250,000 identities have been issued since the system's inception.

Enrollment and Required Documents

All registration processes are free. The individual or entity must submit the requisite registration forms. Once the document is received, the registration information is captured and then vetted and approved by a manager. The last step of the workflow in the system is the generation of the tax identification number. The documents required are company registration number for entities, passport for non-residents, and SSC for residents. No birth certificate is required. If a resident does not have an SSC, a passport is also accepted. It takes on week to complete the registration process.

Vetting

BTS is validated manually with Social Security and has in-house reporting to select potential duplicates. Currently, a social security number or a business registration number can only be used once in the system. Nevertheless, the system still has duplicates. During the survey, BTS representatives mentioned that when they find duplicates, they attempt to merge the records.

Identification Number

The BTS issues a six-digit randomly generated number. It has a seventh digit, which is a checksum not visible to the taxpayer.

Document Issued

The BTS does not issue cards that can be used as a proof of identity. Of the more than 250,000 tax ID numbers that have been issued during the life span of the system, approximately 100,000 have been purged and not included in the newly implemented system, as they were considered inactive.

Technical Details

Database

Social Security IDs are stored in the system, but there is no direct link or validation against the Social Security database. It is encrypted. Both the social security number and the passport are stored. No biometrics are stored in the system.

Security

BTS is part of the CITO Network, which is ISO27001 certified.

Vital Statistics Unit – Attorney General's Ministry

Civil registries are a key element of any identity system. Most identity systems start with a birth certificate as the source of the individual's biographical data: names, date and place of birth, and others. This section is organized slightly differently than the previous one because the Civil Registry is not considered a functional ID rather a component of any foundational ID.

Overview of the Organization

Registration of births and deaths is governed by the Registration of Births and Deaths Act, Cap. 157 of the Substantive Laws of Belize, Revised Edition 2011. The system is administered by The Attorney General's Ministry and the Belize Ministry of Health. It registers all vital statistics, including adoptions and deed polls, except divorces. There are eight offices throughout the country. All the offices distribute certificates and all of them are places of registration (only the central office produces certificates, which are sent to the district offices to distribute). Finally, all the offices have the infrastructural capacity to register and issue certificates: photocopier and printers, phones, computers, a system to fill out forms electronically, and the ability to transmit data over the internet.

Civil Registry System

Both birth and death records are digitized, indexed, and stored electronically, and the information is centralized at the national level. Limited digital system: 90 percent of the information has been inserted into the system. Most of the information starting in 1920 is now in the system. Some information is scanned but some is not. Scanned copies are not linked to the actual system. Further review will be needed to determine the obstacles that are preventing 100 percent digitization of documents in the civil registry.

Birth Certificate

An estimated 95 percent births take place in medical institutions and an estimated 90 percent of births are registered in the VSU. There is no regulation or standard that requires hospitals to provide information to the VSU, but the VSU has books at hospitals.

Data Collection And Verification. Death Registration Process

- In accordance with the law, a family member or authorized person (i.e., the informant) visits the VSU office of the district the place of death occurred.
- The informant shares the particulars of death/ cause of death with the clerk at the VSU office.
- The clerk upon certifying the authenticity of the information proceeds to register the death of the individual.
- The information is then registered in the register and then in the digital system.

Issuance of Certificates

- The individual must apply in person: no online application form exists today.
- The Individual visits any VSU office and makes an application for a copy of a birth or death entry.
- VSU staff verifies the information requested from the register and digital record.
- A document is then approved, printed, and issued to the requester.

Services Provided

Data are shared with the Social Security Board (via an MoU) to provide a bulk copy of their database monthly. Data were also shared in the past with the Electoral Boundaries Organization when Belize was conducting a re-validation of electoral data. When sharing data with other government agencies and organizations, they typically use memorandums, but only within the government. They anticipate being included in the government enterprise bus.

Other Stakeholders

The following are stakeholders that have some relationship to identity management but that are not users. The IDs they issue are not valid in other contexts beyond their scope.

Department of Transport

The Department of Transport issues a Driver's License for anyone 17 years of age or older. The driver's license is not accepted as a valid ID for other entities because it was a laminated document with no national standard. The card was recently changed, adding security features and an integrated platform (2014), but there are still a lot of cards in use in the previous format.

Municipalities can also issue driver's licenses within their municipal boundary. The Department of Transport system currently only allows connection with an independent system for which municipalities pay annual licenses to use.

The Department of Transport is not the only entity that can issue driver's licenses: all municipalities can also issue driver's licenses within their municipal boundary. An information system integrates all the municipalities with the Department, but this is still a work in progress. The Department of Transportation system currently only allows connection with an independent system for which municipalities pay annual licenses to use. Not all of them have this system.

Regarding biometrics, the photograph of the person is stored in the database. Each municipality has its own system, but they must send the information to the central repository at the Department of Transit. There are difficulties with respect to identifying each individual, because each municipality issues documents with their own serial number. The individual has no ID number other than the serial number attached to the card.

The most frequently used document required to obtain a driver's license (at least those issued by the Department of Transport) is the Social Security card. It is also used as proof of age. Those who do not have a Social Security card can use their passport. Finally, for an individual that cannot produce either a social security card or passport, a valid birth certificate is acceptable. In all cases, no further verification is done against the document presented.

Ministry of Health and Wellness

The Ministry of Health and Wellness (MOHW) provides the general public with a Patient ID through the hospitals and clinics throughout the country. Its purpose is to provide people with a unique identifier to track their medical history in a unified platform called The Belize Health Information System (BHIS), begun in 2005. This ID is only used for health services. The patient can use any document as proof of identity: the most used are the passport and Social Security card, but driver's licenses and ID from a foreign country in the case of non-Belizeans are also accepted.

The patient can use any document as proof of identity: the most used are the passport and Social Security card, but driver's licenses and ID from a foreign country in the case of non-Belizeans are also accepted.

It is paramount for a good health information system to guarantee uniqueness in the registry, but there are duplicates. During the interview, one special case was mentioned related to the mother's name. In most Latin American countries with the exception of Belize, the mother's name is part of a person's name. This creates some discrepancies during registration.

Although the BHIS has mechanisms to detect duplicates and correct them, it is more a reactive process: each time a duplicate is detected, there is a process in place to analyze it and eventually fix it. Two special cases were also discussed during the interview: children and Mennonites. With respect to minors, MOHW registers them in the system attached to the mother's registry until the minor obtains a valid proof of identity: birth certificate, passport, or social security card. In relation to Mennonites, there is a law in Belize that authorizes them to not have a social security card and no other form of identity. The representative of the MOHW mentioned that it is extremely difficult to identify some of them because some have the same names and addresses and no valid ID. Finally, the representative of the MOHW was not aware of the existence of the SSB verification service. They specifically mentioned that they did not fluent communication with SSB.

Companies Registry

The main interest of the Companies Registry is the use of a National ID as a way to verify identities. Today, the social security card is the main proof of identity. All Belizeans require a Social Security Number: passports are only accepted for foreigners but even in this case, once they obtain an SSN, this must be registered in their system. During the interview, the representative of the Registry mentioned that Social Security Number is a workaround for them: the Registry requires a true source of identity information, so they believe that a National ID System is a major step in that direction.

Central Bank of Belize

The Central Bank of Belize regulates and encourages the development of Belize's financial system. During the interviews, there were discussions about the National Financial Inclusion strategy 2019–2022 and the creation of a digital wallet. The strategy report (National Financial Inclusion strategy report 2019–2022, Central Bank of Belize) provides evidence of the difficulty of supporting identity verification for financial institutions: 17 percent of the population lack necessary documentation, as the process of checking ID is very cumbersome due to the lack of automated ID verification infrastructure.

The Central Bank of Belize has already requested the introduction of a national identification assessing the potential for digital ID, real time integrated ID verification systems (extract of the strategy document, p. 31). Rural areas face greater difficulties due to the lack of specific addresses and the lack of financial institutions present in their areas. The recent introduction of the digital wallet by two banks and two telephone companies is a sign that under the guidance of the Central Bank of Belize, the country is evolving fast to respond to financial inclusion in a different way by facilitating financial transactions without having to have a bank account. The digital wallet process involves remote verification of ID. Guidelines to perform this type of verification must be reviewed, as the documents provided did not explain how this process is being implemented.

General Findings

- Overall, there is strong support for a National ID initiative from all stakeholders. Some examples of the findings:

  - **The SSB** (during the interview) mentioned that a National ID Card will relieve the SSB of the requirement to issue a card. They want to have a secure and reliable identity service provider so that they can refocus on their core business, which is managing funds for Social Security coverage and eligible disbursements.

  - **The Department of Transport** uses the Social Security card or the passport as proof of age. For people who do not have either of these documents, they request a birth certificate, which is not an identity document.

  - **The Ministry of Immigration** mentioned that a national ID is key to improving their services: their biggest concern is to validate identity, and this is why a national ID system is important. Also, the ministry representatives mentioned that online services and the Immigration Management Unit to verify the documents provided are relevant for their needs.

- There is no evidence of a documented strategic plan for national identity management, except for a vision and internal Digital Transformation Unit (DTU) work for a digital wallet, as well as the Digital Agenda for Belize and support for the acquisition of a new centralized Civil Registry and Vital Statistics (CRVS) solution. However, the CRVS system request for proposal initiative needs to be completed by referencing the National ID program and the need to generate and manage the unique identity number of the person registered.

- A significant number of passports have been issued, but no consistent de-duplication was performed until now. Technical issues with the prior passport-issuing system will need to be addressed by the new e-passport issuing system being implemented.

Ongoing Projects

There are a number of ongoing projects related to identity management being implemented by the different stakeholders. All of them will improve the trustworthiness of the existing systems, but there is a need to further investigate the objectives, the implementation features, and the results to be achieved. It is also important to understand them in the context of a future National ID System and how this National ID System will impact the projects mentioned.

- **The SSB** is executing a project, that will incorporate fingerprints to the enrollment process, to be used both for de-duplication of the database and for identity verification.

- **Immigration** is implementing a new system for e-Passport issuance. As required by International Civil Aviation Organization (ICAO) standards, it will include an ICAO PKI. The new system will enable (again) the use of biometrics (fingerprints) for de-duplication during the vetting process. The architecture presented would also allow support for other public key infrastructure (PKI) services to be determined, but the overall governance of PKI at the state of Belize level will need to be addressed.

- **Vital Statistics Unit:** There is a clear interest from the government to improve VSU systems and operations, in particular those related to civil registries, by the implementation of a new CRVS System. The United Nations Development Programme (UNDP) will help improve operations, and the Inter-American Development Bank (IDB) will provide funding to acquire the new CRVS. The digitization of paper records, data validation, indexing, and checking, will also be analyzed.

Biometrics

- There is minimal use of biometrics in Belize today, and they are not used at all for de-duplication during the vetting process. This is a major concern, as it enables the creation of multiple identities for the same individual.

- The good news is that there are a number of ongoing projects which will incorporate the use of biometrics in several systems: the passport office and immigration, due to e-passport issuance (the solution will come from CBN /Innovatrics) and the SSB (Fulcrum Biometrics/Fujitsu). In the context of the creation of the National ID program, the use of biometrics by different organizations will need to be revisited to recommend a more integrated strategy .

Interoperability

- **There is minimal interoperability between identity agencies.** From all functional ID systems used in Belize (social security card, passport, and voter's ID card), only the SSB has an online service to verify demographic data associated with the social security card. This service is underutilized: only a handful of organizations use it. In particular, some organizations mentioned that they were not aware of the existence of such a service. Again, some ongoing projects are taking the SSB service into consideration to be integrated into their future systems (for example, Company Registries).

- **Manual verification of identity data.** Because of the minimal interoperability, most of the verification of identity-related data is done manually. Ad hoc verification requests are sent to the issuing agency in case of doubt.

Civil Registry

- Birth registration rate is over 90 percent. The plan to improve the operations and the capabilities by acquiring a new CRVS will need to define how these improvements will enable an increase in the birth registration rate to 100 percent.

- Only one organization accesses the Civil Registry database: the Social Security Board. It does so through a copy of the database that is sent to the SSB once a month. Other agencies that use birth certificates (Immigration, Electoral Boundaries) do not have this access, which limits their ability to validate data.

Know Your Customer/Digital Wallet

- The Central Bank of Belize has authorized two banks and two telephone companies to launch a new know-your-customer (KYC)/digital wallet system for financial services. The objective of creating a financial digital wallet is to promote financial inclusion by proposing a financial instrument easier to obtain by downscaling the existing KYC requirements to open a bank account. The type and number of payment transactions are limited but offer an alternative to cash payments.

The objective of creating a financial digital wallet is to promote financial inclusion

Legal Framework

In addition to the acts and regulations governing the existing identity ecosystem in Belize, the following acts were recently passed.

- **Data Protection Act 2021.** The act was enacted in November 2021; it is not yet implemented. The Act promotes confidentiality and regulates the use of personal identifiable data. This legislation is not specific to the use of data in the national identification database. Although it mentions the existence of biometric data, the existing legislation does not define how the use of biometric data will be managed.

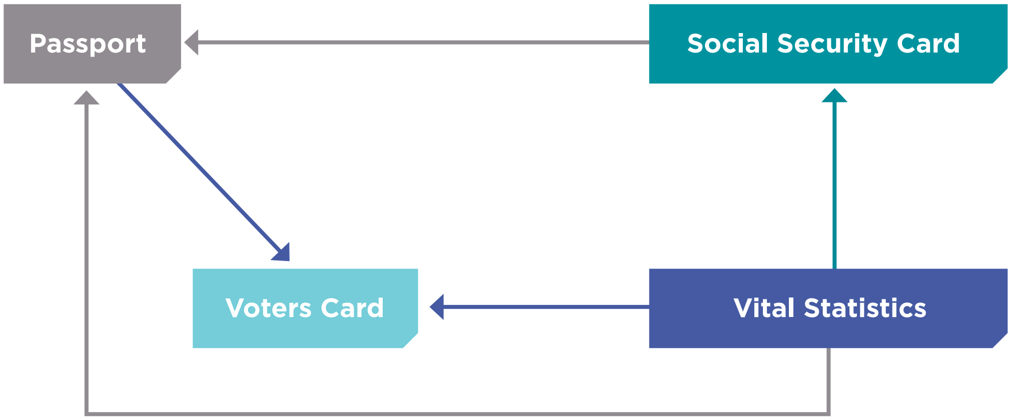
- **Public Sector Data Sharing Act 2021:** This Act provides a legal framework to facilitate data sharing and interoperability between government agencies, allowing for automatic linking and verification of identity data.

- **Electronic Evidence Act and Electronic Transaction Act 2021** are usually the basis for full digital process implementation.

Assessing the Trustworthiness of the Existing Systems

Uniqueness

The following diagram depicts a cross-referencing of Belizean functional IDs:



The process starts at vital statistics with the birth certificate. This is the only document used to enroll in the social security system and obtain a voter's card. In both of these cases, there is no use of biometrics for de-duplication, implying the possibility of having duplicate registries in both datasets/systems. For instance, the representative of the SSB responded, *"a person should only be registered once, but there are times when a person is double registered in error."*

The process will soon involve fingerprinting, which will be used for both identity verification and de-duplication. The other functional ID system being used regularly as proof of identity is the passport. In this case, although there was a biometrics de-duplication process based on fingerprints, it is no longer in use because the software is not supported, which prevents the correct use of the system. In summary, there are no current functional systems in Belize that confirm identity with biometrics, reducing the level of assurance of existing functional IDs.

There is some concern about the quality of the VTU data: "There is a key risk in the identity management system right now: if they don't fix vital statistics, the problems will continue." On one hand, the future UNDP consultant will define how the new organization should look to achieve these goals. On the other, the new CRVS system will enable a better, more digital and integrated implementation of CRVS activities.

Accuracy

Death reporting is not accurate. The SSB flags them but only when they learn of a death, which is when someone else asks for a benefit. Another source of error is when a person changes his or her name due to marriage. This can create a duplicate entry.

Security

Credentials and Authentication

The SSB issues a card with some security features, but it is not a highly secure credential in accordance with international best practices: it is not polycarbonate, and it is not an electronic document (eID). In addition, although the SSB provides an authentication service, only a handful of organizations use it, and it is also limited in the type of verification it can provide. Nevertheless, the SSB is the only available service: neither Passport nor Electoral Boundaries provides a similar service.

Challenges and Improvements

Considering the situation of each agency, as well as the present review, the following tables present the challenges at hand and necessary improvements.

CHALLENGES

- VSU civil event registration is 90 percent, complete if the completion rate of birth records registration is considered. More in-depth analysis may be necessary for minorities.
- There are no systems in place that use biometrics to confirm identity, which reduces the level of assurance of existing functional IDs.
- Before the end of 2022, the Ministry of Immigration introduced biometrics (i.e., fingerprint capture and de-duplication), but conditions of use in the context of the National ID require more in-depth investigation, coordination, and planning to reach the goal.
- **Minimal interoperability between identity agencies.** It is still not possible to verify ID documentation electronically or digitally for all parties; there is only one MoU in place between the SSB and the VSU that allows access to updates of the VSU civil events database.
- **Manual verification of identity data.** Because of the minimal interoperability, most of the verification of identity-related data is done manually. An ad hoc verification request is sent to the issuing agency in case of doubt. There is a need to interface with other agencies on a daily basis, in a way that reduces time and errors.
- **Accuracy.** The SSB flags a death only when someone else requests a benefit, which impacts the verification required. Another source of inaccuracy is a name change, which either creates difficulty in updating an existing record or creates a duplicate entry.
- **SSB.** The SSB issues a card which is used as a de facto National ID, with some security features, but it is not a highly secure credential as per international best practices: it is not made of polycarbonate material, which is harder to counterfeit, and it is not an electronic document (eID) (eIDs are electronically sealed). In addition, although the SSB provides an authentication service, it is not widely used and the types of verifications that it provides are limited.

- Most agencies do not include biometrics as part of their identity validation processes or have only recently introduced the deduplication service in operational conditions. This will need to be reviewed to comply with both the legal framework regarding personal data protection and the new operational conditions of a National ID identity verification service.

IMPROVEMENTS NEEDED

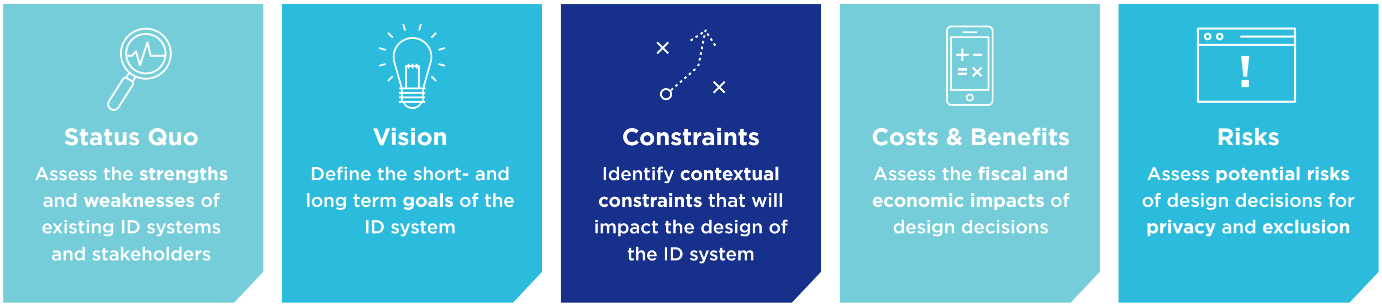
- The E-Governance and Digitalization Unit, which is working with the IDB to produce a National Identification Strategy and Action Plan, will identify all assets which are already available or will be available in the next 12 months to support the National ID initiative, to leverage existing assets: secure hosting of government applications and services, CERT, PKI, interoperability via the enterprise bus to be implemented, and a roadmap for government digital services, starting with a web portal for citizens.
- Most of the stakeholders have confirmed their interest in having a National ID card issued, which will save them time and money. There is a need to focus on the definition of the use cases of the National ID card—both the physical and the digital card.
- Each agency in charge of issuing a document should implement a web service that enables them to verify the authenticity of the National ID card and data. This will help determine the authenticity of a National ID document being presented to perform a transaction.
- The use of biometrics at the national level needs to be planned to ensure at least optimal efficiency of ID verification and start to do a formal legal view on how the biometric data are securely stored and managed. There is a need to investigate whether and how to facilitate interoperability between biometric databases.
- A new vision for identity management is needed that aims to incorporate identity verification, automated approval processes, and an integrated trust framework in preparation for the launch of the national digital identity.
- A legal and institutional framework must be developed to support the vision for National ID. A number of recent acts, such as the Personal Data Protection Act, exist but a legal framework and future bill must be drafted to support implementation of the National ID vision, including governance aspects.

3

Vision

Vision

The second step in the design of a national ID system roadmap is to define the vision:



Status Quo

Assess the **strengths** and **weaknesses** of existing ID systems and stakeholders

Vision

Define the short- and long term **goals** of the ID system

Constraints

Identify **contextual constraints** that will impact the design of the ID system

Costs & Benefits

Assess the **fiscal and economic impacts** of design decisions

Risks

Assess **potential risks** of design decisions for **privacy and exclusion**

Two sources provided input to the definition of the goals of a national digital ID. The first one is the National Digital Agenda for Belize 2022–2025, which is the guiding document on which the entire national digital ID is based. The second source was the output of the second workshop, during which the participants came up with goals that the National Digital ID initiative should seek to achieve.

Goals of the Digital ID System

National Digital Agenda

As the leading institution for digital transformation, the e-Governance and Digitalization Unit has launched the current National Digital Agenda for Belize 2022–2025, aiming to create the enabling environment for a digital government. Hence, this digital agenda must be understood as a strategic plan and a working framework for the Belizean government to achieve complete inclusion and digitalization by carrying out high-impact programs designed to transform the public sector and society itself. The second pillar, digital government, includes e-services and digital identity and focuses on improving service delivery within government and transforming the way government operates.

e-Government: Context

Although Belize's National Digital Agenda strategy was launched some years ago, its implementation has been fragmented and has had little impact in improving e-government solutions and capturing its benefits. The current administration decided to update the strategy by presenting, in the presence of the Prime Minister, the Digital Agenda: Towards a Digital Belize 2022–2025.

> **In the Online Service Index (OSI), Belize's rank had fallen every year, from 90th in 2014 to 168th in 2020.**

In 2020, Belize continued to lag on the United Nations E-Government Development Index, ranking 136th out of 193 countries, for the E-Government subindex and 163rd in terms E-participation. Furthermore, in the Online Service Index (OSI), a sub-pillar of the Survey, Belize's rank had fallen every year, from 90th in 2014 to 168th in 2020. These rankings reflect the slowness of government units in adopting information and communication technologies (ICTs) as a tool for service delivery to its citizens.

Furthermore, Belize's performance has also been impacted by systemic challenges such as little or no interconnectivity and data-sharing among government agencies, lack of unique citizen identifiers common to all government management information systems, and lack of standards and guidelines regarding e-government solutions.

Regarding digital infrastructure, the ICT Development Index of the International Telecommunication Union (ITU) shows that Belize performs well in areas such as international internet bandwidth per internet user but requires more efforts in fixed-telephone subscriptions and broadband subscriptions or households with internet access. Belize's position was steady relative to its rank in 2016 (120th out of 176 countries in the overall index) and is comparable to that of El Salvador and Guatemala. However, this result reveals the historically low level of connectivity throughout the territory. Regarding competitiveness and digitalization of enterprises, Belize's private sector is relatively less prepared for the digital age than that of other Latin America and Caribbean countries.

A recent survey carried out by the Statistical Institute of Belize in 2021, the Governance Acceptance Survey, examined the factors associated with e-government acceptance in the Belizean context, including perceived usefulness, perceived ease of use, trust in e-Gov, and perceived behavioural control. One of the main findings was that 49 percent of respondents had accessed government services in the past year, and 65 percent of them expressed the intention of using e-services in the future and believe that they will increase their productivity, save them time in daily tasks, and provide significant advantages over the physical channel (against 35 percent who expressed low intention to use e-gov). These numbers show a great demand and intention to use e-services and ICT among Belizeans and underscore the importance of creating a clear path for the deployment of digital government and digital services. Moreover, the survey reveals that public institutions should focus on creating a trustworthy and accessible environment for digital services and highlight their significant benefits. This goal includes first addressing more time-consuming services for citizens, such as immigration and vital statistics transactions.

Key Programs

To achieve its objectives, the digital agenda proposes three Pillars, structured on different strategic themes, each one with several key programs. In particular, Pilar 2: Digital Government, has as one of its strategic themes "e-Services & Digital Identity." Specifically, Program 3 is devoted to a "National Identity Solution."

PROGRAM 3: *NATIONAL IDENTITY SOLUTION*	
JUSTIFICATION	Belize's current identity system may cause issues when attempting to develop a digital identity. Belize does not issue a unique identity document; the most used and accepted documents to verify a person's identity are passports, residence cards, national cards, or social security cards. Nor do Birth certificates have a unique number that can identify a person, which is a requisite to build an identification system. Not having a unique identification number represents a major challenge regarding identity, since a unique number that can identify a person is necessary to make his or her information interoperable among different government entities and services. There is a latent demand for the implementation of digital identification so citizen and business can save money and time doing procedures that requires identity verification for different purposes, i.e., cards to vote, pay taxes online, access digital services, etc. Therefore, digital identification has become Belize's government number one priority as a result of the need for stronger means of online authentication. Such identification becomes a de facto requirement for all online services from government, and even other stakeholders such as healthcare providers or multinational companies.
PROGRAM OBJECTIVES	(1) Create an identification framework that will help government improve the quality of customer identity data, improve assurances around identity claims, and facilitate the provision of online identity services. (2) Study different solutions for digital identification and validate the most suitable for Belizeans to access the e-service platform. (3) Implement a secure and efficient solution for all citizens.
COMPONENTS/PROJECTS	**1. Implementation plan and pilot to improve identification system (IDB technical cooperation)**

PROGRAM 3: *NATIONAL IDENTITY SOLUTION*	
LEADING INSTITUTION	Ministry of Youth, Sports & E-Governance (E-Governance and Digitalization Unit)
PARTNERSHIP	Attorney General's Ministry, Social Security Board, Ministry of Foreign Affairs, Foreign Trade & Immigration
JUSTIFICATION	Any trip for Belizeans to the registry office will clearly demonstrate the importance of this department for citizens, as they attempt to obtain certification of major life events for different purposes: insurance, access to finance, obtaining a passport, or even getting married.

"Program 4: Digitalization of the Civil Registry" is also a critical program, strongly related to a robust national identity management system.

PROGRAM 4: *DIGITALIZATION OF CIVIL REGISTRY*	
JUSTIFICATION	Any trip for Belizeans to the registry office will clearly demonstrate the importance of this department for citizens, as they attempt to obtain certification of major life events for different purposes: insurance, access to finance, obtaining a passport, or even getting married. Moreover, the digitalization of the civil registry is a foundational pillar for the national e- ID scheme and inclusive e-Government services. Thus, the digitalization of the Civil Registry is an enabling program for the development of digital identity solutions, interoperability and the development of other projects. In addition, it is a crucial tool to fight poverty, corruption and inequality and a key element of sustainable development for Belize and its citizens.
PROGRAM OBJECTIVES	(1) Ensure that Belize CRVS system is universal, accurate, and reliable by improving the quality of data and the management of vital statistics information and reduce the total cost to the government of collecting information regarding this field. (2) Improve CRVS systems to support the census and household surveys in determining population size and status. (3) Optimize inefficient ID systems that are often paper-based or decentralized, which leads to issues such as data duplication, delayed updates, and identity theft and fraud, by putting the necessary resources, technologies, and legal frameworks in place to support the process of linking its ID register and CRVS system. (4) Incorporate inputs arising from the digitalization of the CRVS systems into their decision-making processes to control corruption, promote equality, coordinate policy, and inform decision - making processes in Belize.

PROGRAM 4: *DIGITALIZATION OF CIVIL REGISTRY*	
COMPONENTS/PROJECTS	1. Digitalization of vital events services: births, marriages, deaths, divorces, and others civil status. 2. Improve access of services for Belizeans residing abroad, naturalized, and marriages of foreigners that occurred abroad, and other vital statistics. 3. Digitization of records 4. Support Institutional Strengthening & External Relations
KEY ACTIONS	1. Improvement of the legal and institutional arrangement for the digitalization of the civil registry by identifying legislative gaps and human resource needs 2. Establish data quality standards and maintenance guidelines 3. Assure the quality of the data that will be digitalized according to international standards for future interoperability with other entities. 4. Public awareness of the benefits from a robust integrated e-civil registry, especially when it comes to service delivery. 5. Build human resource capacities and consider organizational restructuring 6. Conduct a digitization exercise including data cleansing for all existing records and files
LEADING INSTITUTION	Attorney General's Ministry
PARTNERSHIP	Statistical Institute of Belize, Ministry of Youth, Sports & E-Governance (E-Governance & Digitalization Unit)

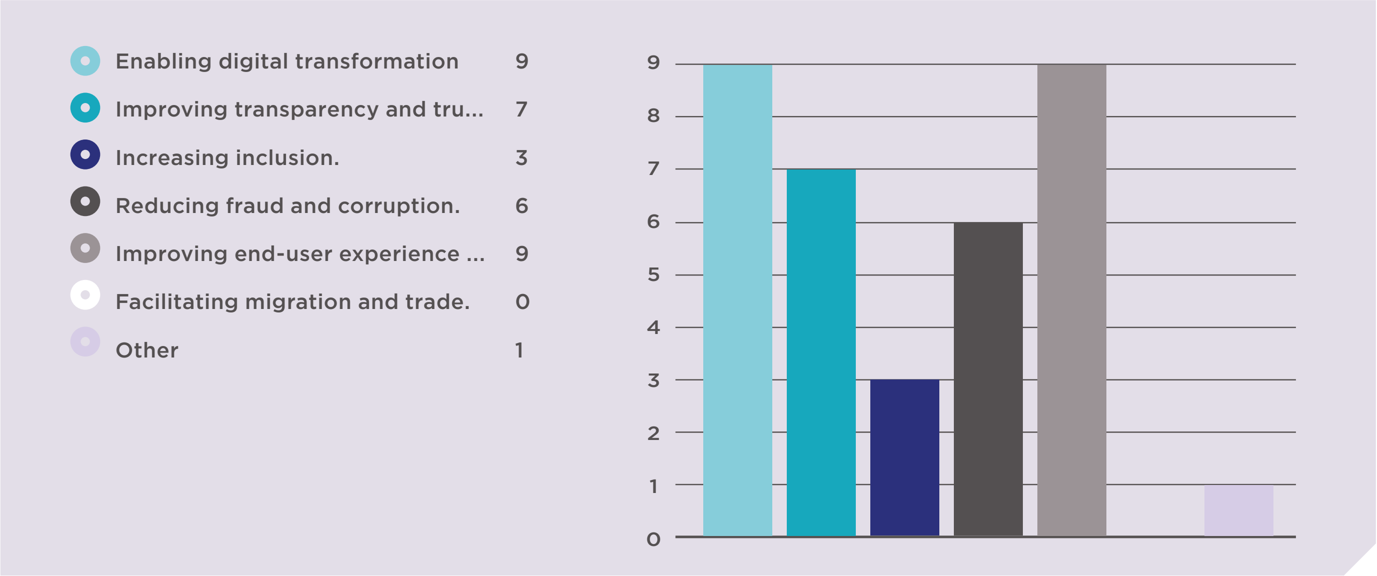
Second Workshop

During the second workshop, a number of possible goals were presented for discussion:

- Digital transformation of services and economy (digital economy and government)
- Improving transparency and trust in government
- Increasing Inclusion
- Reducing fraud and corruption
- Improve end-user experience with identification
- Facilitating migration and trade

During the workshop, a poll was conducted to ask participants to indicate goals that should be pursued by the National Digital Identity Strategy:

Which goals do you think the National Digital Identity Strategy should pursue?



The **top four** (4) goals that should be pursued according to the poll are:

1. Enabling digital transformation of services and economy
2. Improving end-user experience with identification
3. Improving transparency and trust in government
4. Reducing fraud and corruption

These goals are aligned to the problems detected in the National Digital Agenda for Belize 2022–2025. Note that there is a strong correlation between the goals that a digital identity should pursue and the objectives defined in the digital agenda:

- **Enabling digital transformation of services and economy.** This is strongly related to objectives 1) and 2):

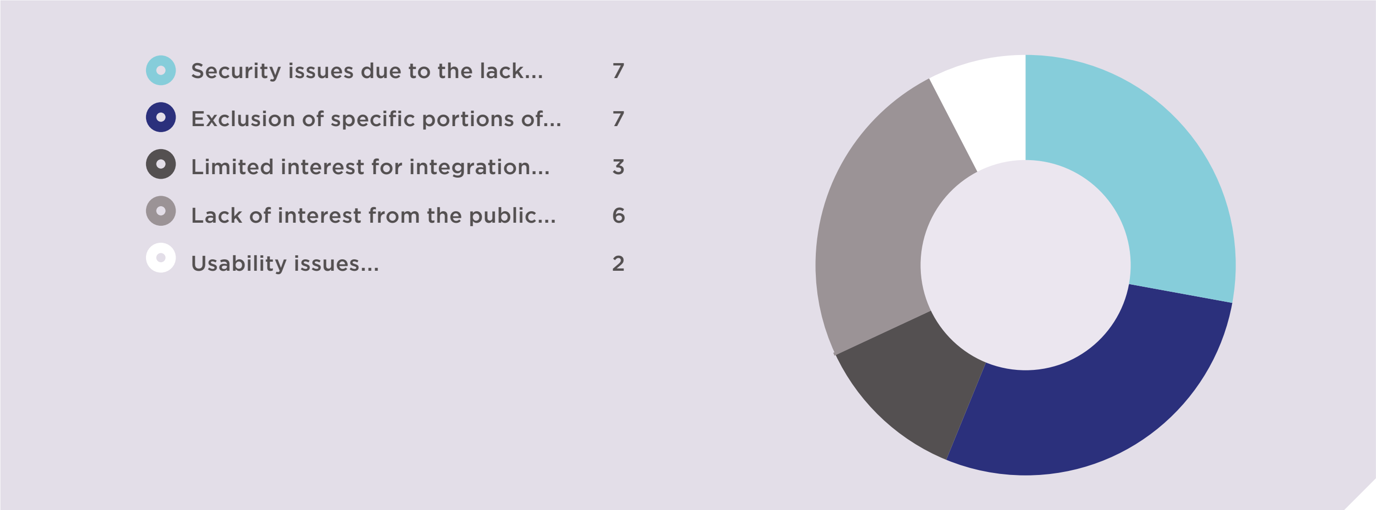
  - Create an identification framework that will help the Government improve the quality of customer identity data, improve assurances around identity claims, and facilitate the provision of online identity services.

  - Study different solutions for digital identification and implement the most suitable for Belizeans to access the e-service platform.

- **Improving end-user experience with identification.** This is correlated to objectives 1) and 3):
    - Implement a secure and efficient solution for all citizens.
- **Improving transparency and trust in government**
    - Create an identification framework that will help the government improve the quality of customer identity data, improve assurances around identity claims, and facilitate the provision of online identity services.
- **Reducing fraud and corruption.** This goal is related to Objective 3):
    - Implement a secure and efficient solution for all citizens.

In addition to these goals and objectives, one more point was discussed during the workshop. In another poll to select the major risks a digital identity system would face, the results indicated that exclusion was one of them:

What are the main risks you envisage that a Digital Identity framework will face?



Inclusion must be part of any Digital Identity initiative, and therefore it should be a goal.

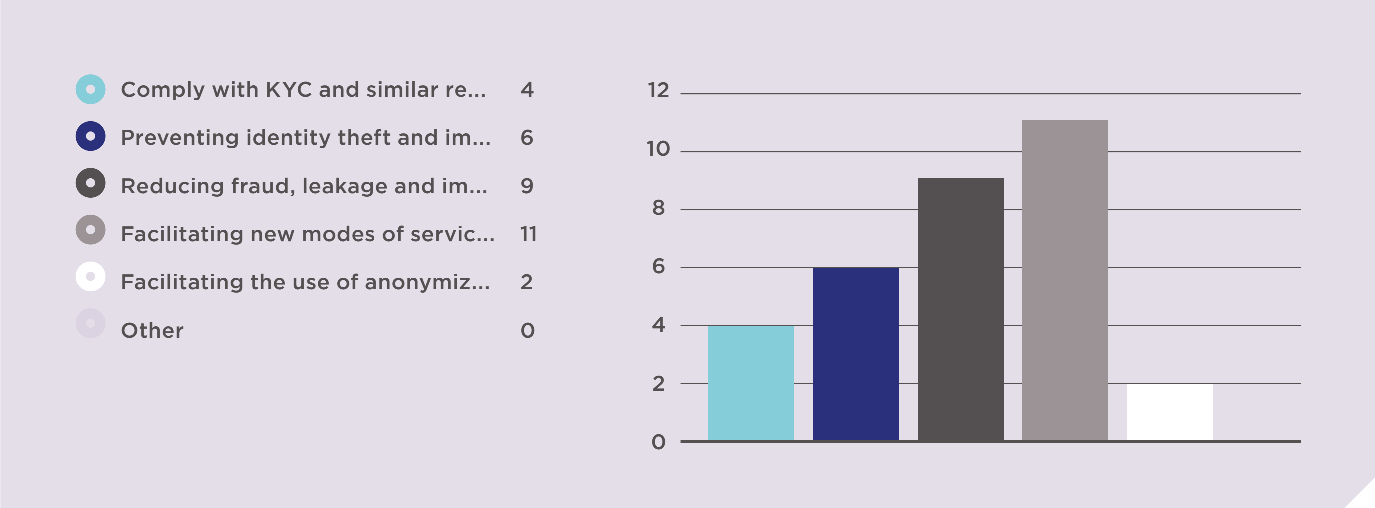
In summary, the identified goals are well aligned with the National Digital Agenda and can be considered the basis for the development of the National Identity System:

- Enabling digital transformation of services and economy
- Improving end-user experience with identification
- Improving transparency and trust in government
- Reducing fraud and corruption
- Increasing inclusion

Define Sector-specific Use Cases

During the design of a Digital Identity Framework, it is good practice to define a number of specific use cases. With those use cases in mind, it is possible to map them into a Digital Identity Framework, highlighting the pros and cons of the different options. For example, if one use case is to help the financial sector in the KYC process, and if KYC requires an address to be part of the information to be verified, a Digital Identity Framework should consider including an address as part of the personal attributes to be captured during enrollment. During the second workshop, stakeholders were presented a list of possible use cases, with the option to add any other if required, to discuss which one should be the driver for the National ID System. The following is a summary of the results:

Which of the following use cases do you believe should be prioritized on a National Identity System ?



As can be seen in the bar chart, “Facilitating new modes of services delivery” and “Reducing fraud and leakage and improving targeting and service delivery for government programs” were selected in first place. This is in accordance with the Digital Agenda, where providing new ways of providing services while reducing fraud (or in other words, increasing the trustworthiness of the identification process) was considered a major objective.

The **use cases** for the National ID System should be the following:

- Facilitating new modes of services delivery
- Reducing fraud and leakage and improving targeting and service delivery for government programs

4

Constraints

Constraints

A National ID System will be implemented in a specific context with its own limitations and constraints. Knowing those constraints is important to design the National ID System properly.

The following section summarizes the major constraints found.

Belize Digital Infrastructure

Government Capacity

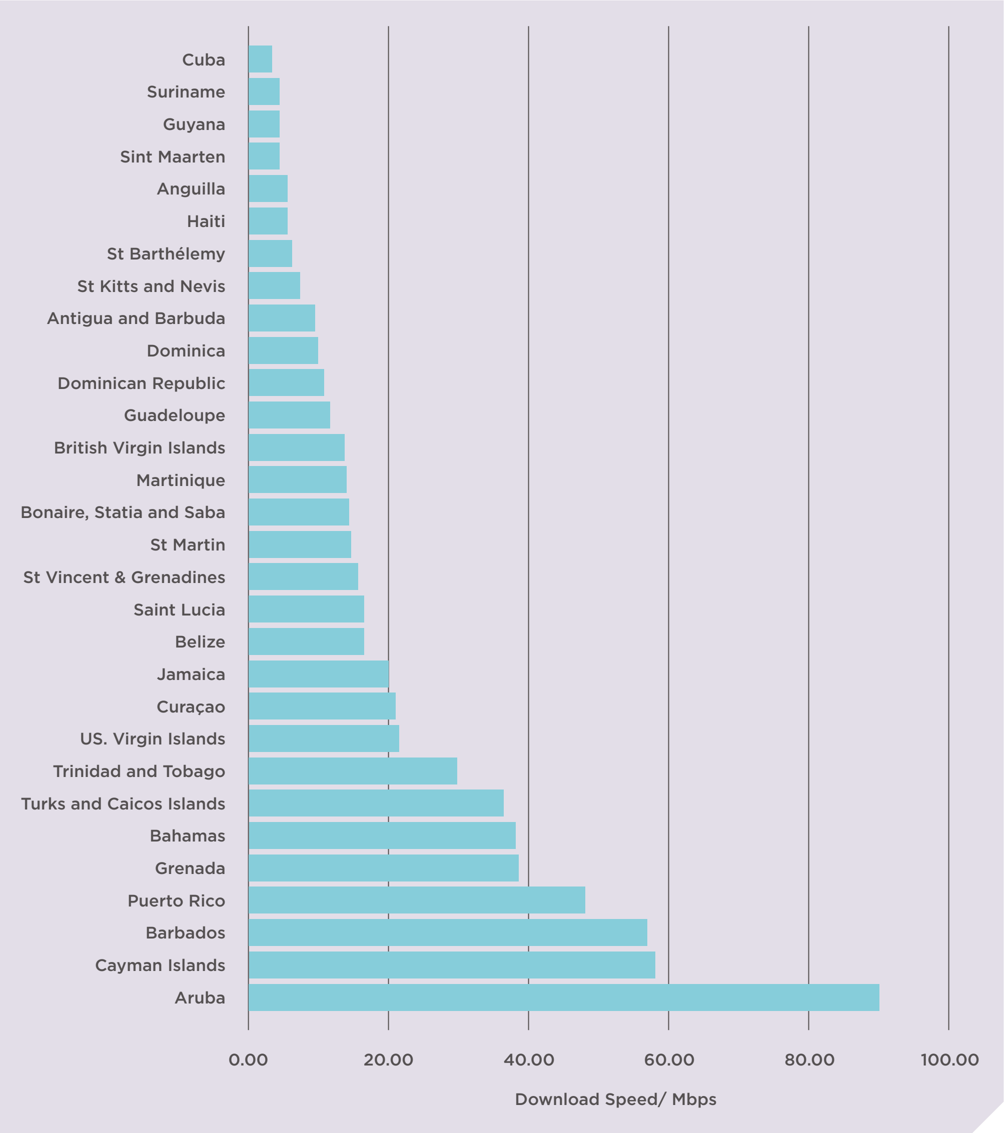
The Central Information Technology Office (CITO)[8] is the agency in charge of the government IT infrastructure and data centers. The government of Belize (GoB) has two data centers: a primary one, with 31 rack units (U) available, and a secondary one with 38 U. There is already a requirement from an existing client for more rack space, which means that the primary data center will have less than 31 U. In a meeting with the CITO team, representatives informed that although there may not be enough space in the main data center, it is not possible to increase the size of the data center because there is not enough physical space to do so. They also informed that the secondary data center does not have same capabilities as the primary one, and that the secondary data center should be considered more as a backup data center than an operational one.

The GoB has also implemented a network, and on which some organizations are already connected (for example, Belize Tax Service). This is a fibre optic network, provided by one of Belize's telecom companies. The only service provided is the physical connection: there is no application layer provided by GoB to the connected organizations. Finally, the CITO representatives mentioned that the network connected agencies that require connection with Belize Tax Services, but it is not a "government network" per se: if two agencies need to connect, they have to resolve their connection between them: at this time, CITO is not providing any services to do so. The price list for different services regarding hosting and network is provided in the Annex. This information was used to calculate the estimates in the "Costs" section.

[8] https://cito.gov.bz/.

Communication and Internet Coverage

There are two telecom companies: Belize Telemedia Limited / Digicell (previously, the national telecom organization) and Smart Telecom Limited /SMART. But the regulatory authority was not able to provide accurate information about national coverage. It was mentioned that penetration may be nearly 50 percent, with the rural communities having less coverage. According to Belize.com, the information presented on telephone and internet coverage and Belize's ranking in the region are shown in the figure below.



Actual Internet download speeds recorded in 30 Caribbean countries/country groupings, as of June 2020 Source: Cable UK.

Among the countries with the fastest internet download speeds, in addition to Aruba, were the Cayman Islands, with an average download speed of 57.96 Mbps, and Barbados, with 56.90 Mbps. At the other end of the spectrum, and in addition to Cuba, were Suriname, with an average download speed of 4.42 Mbps, and Guyana, 4.43 Mbps. Belize's average falls just behind Jamaica's. The maximum residential internet offered by Diginet Belize is 150 Mbps down and 75 Mbps up, for US$99.99.

Telecom network coverage is considered just above-average in Central America. The trunk network based primarily on fibre optic underground network is backed up by microwave radio relay. Another source of information is from the cybersecurity report IDB/OAS[9]:

- Cell phone subscriptions: 239,441 (2017)
- Persons with Internet Access: 176,992 (2017)
- Internet penetration: 47 percent (2017)

Because of the lack of complete coverage, it is mandatory that the solution can work in an offline mode, and cannot base its credentials only on mobile app options.

Although the information contained in the report is now five years old, it is in accordance with the information provided informally by the GoB of about 50 percent internet penetration. Two conclusions can be derived from this. Because of the lack of complete coverage, it is mandatory that the solution can work in an offline mode, and because cell phone subscriptions do not reach a significant portion of the population, the system cannot base its credentials only on mobile app options (eWallet/Mobile ID).

Cybersecurity

The GoB has a National Cybersecurity Strategy, which is planned to be updated as it expires this year. For this update process, a National Cyber Security Task Force (CSTF) will be put in place to contribute to the drafting of the new version.

In terms of capacity building, there are no cybersecurity degrees at Belizean universities. However, the Faculty of Science and Technology of the University of Belize offers a bachelor's degree in information technology.

Currently, Belize has four laws that relate indirectly to cybersecurity (i) the Telecommunications Act, (ii) the Electronic Evidence Act, (iii) the Intellectual Property Act, and (iv) the Interception of Communications Act, but there is no law

[9] https://publications.iadb.org/publications/english/document/2020-Cybersecurity-Report-Risks-Progress-and-the-Way-Forward-in-Latin-America-and-the-Caribbean.pdf

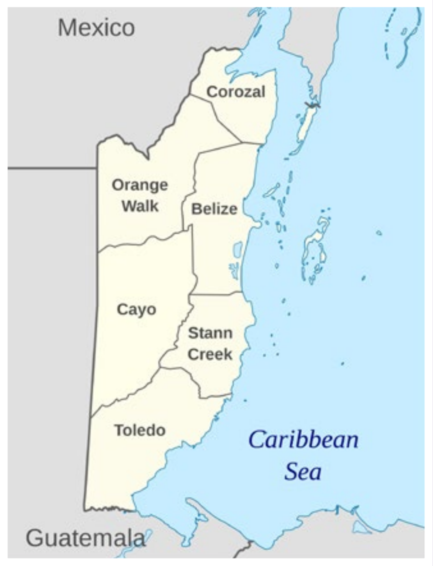
focusing specifically on cybersecurity[10]. Belize also has a Data Protection Act that was approved in 2021, but the oversight agency (data protection commissioner) has not yet been created and implemented.

There is a comprehensive e-government plan that details the road map for the design and implementation to achieve the country's e-government vision of "an integrated, collaborative government delivering secure, quality public services that connect and empower people." However, to date, an e-government portal has not been implemented.

Geography and Population

According to the last census (2010), Belize has 324,528 people living within its borders, with an estimated 3.6 percent undercount (11,683). In the last available statistics from 2020 (2020 Abstract of Statistics), the population is estimated to be 419,199. Because of the important difference between the last census and the most recent statistics, it is preferable to use the more recent figures, which are much closer to the actual population. The rest of the information is derived from that source (2020_Abstract_of_Statistics). The United Nations anticipates that the population of Belize will increase to 550,000 by 2050.

BELIZE IS ORGANIZED IN SIX DISTRICTS[11]:



DISTRICT	CAPITAL	AREA
Belize	Belize City	4,310 km^2 (1,663 sq mi)
Cayo	San Ignacio	5,200 km^2 (2,006 sq mi)
Corozal	Corozal Town	1,860 km^2 (718 sq mi)
Orange Walk	Orange Walk Town	4,600 km^2 (1,790 sq mi)
Stann Creek	Dangriga	2,550 km^2 (986 sq mi)
Toledo	Punta Gorda	4,410 km^2 (1,704 sq mi)

[10] https://unctad.org/page/cyberlaw-tracker-country-detail?country=bz

[11] From Wikipedia: https://en.wikipedia.org/wiki/Belize#Administrative_divisions

The population is distributed along these six districts in the following way:

MID-YEAR POPULATION ESTIMATES BY DISTRICT AND SEX: 2018 - 2020

	2018			2019			2020		
	Total	Male	Female	Total	Male	Female	Total	Male	Female
Country Total	398,050	199,028	199,022	408,487	204,247	204,240	419,199	209,603	209,596
Urban	178,195	86,963	91,232	182,663	89,155	93,508	187,249	91,405	95,844
Rural	219,855	112,065	107,790	225,824	115,092	110,732	231,950	118,198	113,752
Corozal	48,429	24,148	24,281	49,446	24,649	24,797	50,490	25,163	25,327
Corozal Town	12,652	6,034	6,618	12,979	6,187	6,792	13,314	6,343	6,971
Corozal Rural	35,776	18,114	17,663	36,467	18,462	18,005	37,176	18,820	18,356
Orange Walk	51,749	25,925	25,824	52,550	26,299	26,251	53,373	26,683	26,690
Orange Walk Town	13,674	6,617	7,057	13,669	6,602	7,068	13,665	6,586	7,079
Orange Walk Rural	38,075	19,307	18,768	38,881	19,697	19,184	39,708	20,097	19,611
Belize	120,602	59,554	61,048	124,096	61,305	62,791	127,683	63,102	64,581
Belize City	63,423	30,639	32,784	64,287	31,051	33,236	65,173	31,474	33,699
San Pedro Town	19,477	10,087	9,390	20,542	10,644	9,897	21,634	11,216	10,418
Belize Rural	37,701	18,828	18,873	39,268	19,610	19,658	40,875	20,412	20,463
Cayo	96,197	48,059	48,138	99,118	49,524	49,593	102,115	51,028	51,086
San Ignacio/Santa Elena	22,335	10,958	11,377	22,951	11,263	11,688	23,582	11,576	12,007
Benque Viejo	6,880	3,466	3,415	6,982	3,522	3,460	7,087	3,581	3,506
Belmopan	23,038	11,326	11,712	24,294	11,954	12,340	25,583	12,598	12,985
Cayo Rural	43,944	22,309	21,635	44,890	22,785	22,105	45,861	23,273	22,588
Stann Creek	43,459	22,514	20,945	44,720	23,171	21,550	46,015	23,844	22,170
Dangriga	10,442	4,949	5,493	10,559	4,995	5,564	10,680	5,042	5,637
Stann Creek Rural	33,017	17,565	15,452	34,161	18,175	15,985	35,335	18,802	16,533
Toledo	37,614	18,828	18.786	38,557	19,299	19,258	39,525	19,783	19,742
Punta Gorda	6,272	2,886	3,386	6,399	2,937	3,463	6,530	2,989	3,541
Toledo Rural	31,342	15,942	15,400	32,158	16,363	15,795	32,995	16,794	16.201

Source: Statistical Institute of Belize

One important characteristic of Belize's population is that more than half the population lives in the rural areas: 231,950 which corresponds to 55 percent of the population. The urban and rural populations are distributed as follows by district:

DISTRICT	URBAN		RURAL		TOTAL	
	Population	%	Population	%	Population	%
Corozal	13,314	26	37,176	74	50,490	100
Orange Walk	13,665	26	39,708	74	53,373	100
Belize	86,807	68	40,875	32	127,683	100
Cayo	56,251	65	45,861	35	102,115	100
Stann Creek	10,680	23	35,335	77	46,015	100
Toledo	6,530	17	32,995	83	39,525	100

Belize birth rate was 22.9 births/1,000 population (2018 estimate), and the death rate was 4.2 deaths/1,000 population (2018 estimate)[12].

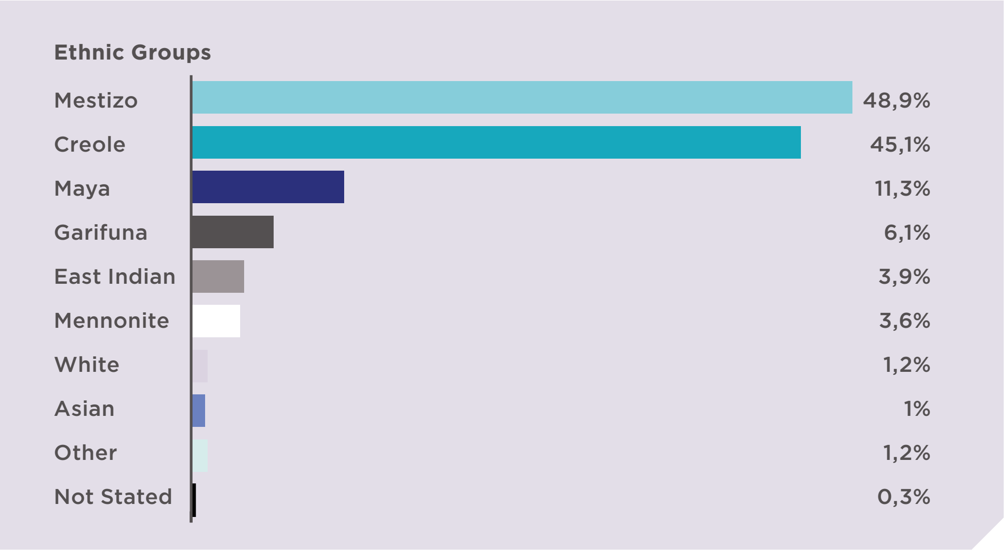
Regarding the distribution of the population by age, we have the following:

	TOTAL	%
Less than 15 years old	149,198	35
Between 15 and 19	45,047	11
Between 20 to 65	207,290	49
More than 65	17,664	4

[12] https://en.wikipedia.org/wiki/Belize

Cultural Considerations

Ethnic Groups in Belize



In terms of identification, the Mennonites are a special case. Today, approximately 12,000 people in Belize are classified as Mennonites. Most Mennonites live in exclusive communities, but some members regularly trade their goods in town fairs or at the local markets in the western and northern part of the country. Mennonite communities in Belize include Shipyard (Orange Walk District), Upper and Lower Barton Creek (Cayo District), Spanish Lookout (Cayo District), Springfield (Cayo District), Indian Creek (Orange Walk District), Little Belize (Corozal District), Pine Hill (Toledo District), and Blue Creek (Orange Walk District).[13]

Mennonites are not required to be registered at the Social Security Board: "There should be a document/agreement regarding the Mennonites in the Mennonite community regarding Social Security contributions but in regard to insured persons registration, Section 4(4) states that The Board shall register all Belizeans, registered aliens, holders of work permits, and their dependents. Therefore, once the applicant falls within one of the different types of Immigration Status below and the valid registration document is provided, the person can be registered with SSB."[14]

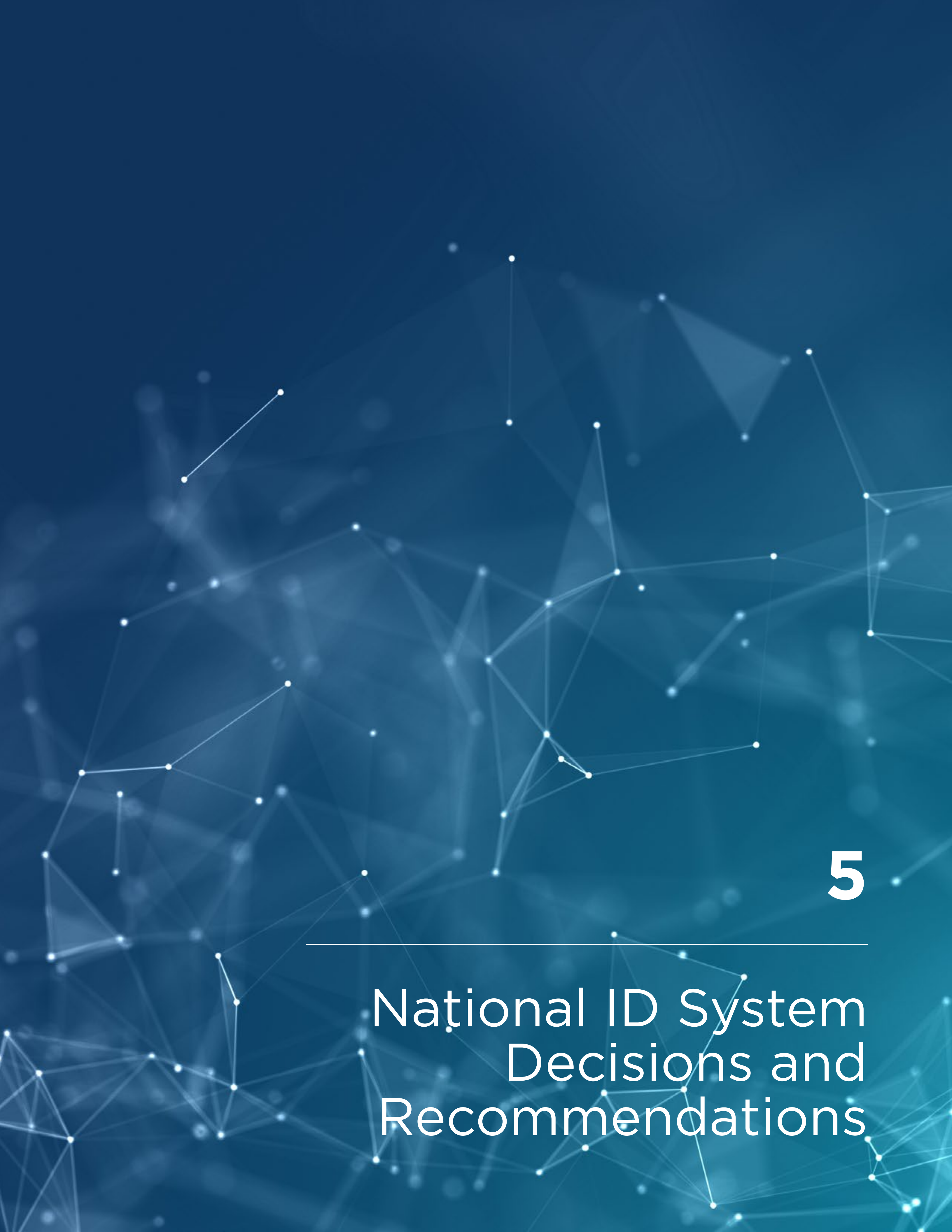
[13] https://www.belizehub.com/belize-destinations/

[14] Directly communicated by Mrs. Carmela Reneau from Social Security Board

Timeline Requirements

The tentative start date for the enrollment process is the last quarter of 2023 or the first quarter of 2024. To achieve this, a number of critical decisions must be made: any delay in making decisions on the following items will delay the start date:

- The tentative budget must be approved
- The legal framework must be drafted and approved
- An organization must be established to manage the implementation of the project and the future ID management operations
- An accelerated procurement strategy must be planned



5

National ID System Decisions and Recommendations

National ID System Decisions and Recommendations

This section presents a set of recommendations to be used as a guideline in the implementation of the National ID System. It serves also as a basis for the cost estimation presented in the next section.

Legal Framework

This table of guiding principles is a collaborative effort between a number of large international organizations, including such as the World Bank, the UNDP, UNICEF, and GSMA, based on international standards with the goal of ensuring that identity systems are inclusive, protective of individuals' data and rights, and designed to support the Sustainable Development Goals[15]:

PRINCIPLES	
INCLUSION: Universal coverage and accesibility	1. Ensuring universal coverage for individuals from birth to death, free from discriminarion. 2. Removing barriers to access and usage and disparities in the availability of information and technology.
DESIGN: Robust, secure, responsive and sustaunable	3. Establishing a robust--unlue. secure, and accurate- identity. 4. Creating a platform that is interoperable and responsive to the needs of various users. 5. Using open standaras and ensunna vendo and techno day neutrally. 6. Protecing user weivacy and control through system design. 7. Planning for tinancial and operational sustainability without compromising accesibility.
GOVERNANCE: Building trust by protecting privacy and user rights	8. Safequarding data privacy, secursy, and user fonts througn a comprehensive legal and regulatory framework. 9. Establishing clear institutional mandates and accountability. 10. Enforcing legal and trust frameworks trough independent oversight and adjucication of grievances.

10 main principles have been listed and are distributed in three main categories:

1. Inclusion
2. Design
3. Governance

[15] ID4D Practitioner's Guide: https://id4d.worldbank.org/guide

By following these principles, the legal and institutional framework can be created to support digital identity.

Given the overwhelming trend toward digitalization of economies and societies, the principles reflect the increasingly digital nature of official identity systems. For that reason, the wording of Principle 8 was changed from security to cybersecurity to support this reality.

Legal identification systems provide proof of legal identity. The name and nature of these foundational systems varies under national law but typically includes civil registration systems, national ID systems, and population registries.

Functional identification systems provide official proof of identity and authorization for specific purposes or sectors. This typically includes identification systems that provide voter identification, a social security number and card, passports, and driver's licenses. In some cases, these credentials may also be recognized as proof of identity for purposes other than the initial one.

Main Findings on the Legal and Institutional Framework

Work is ongoing to address noncompliance with standards on GDPR, national identification data, and internet privacy laws. There will be a need to define more specifically in the Act and in future regulations how biometric data will be managed for the National Identity program as well as for other document issuance or identity verification activities by third parties.

The data protection commissioner has not been selected, as the oversight agency has not yet been established. The creation and Implementation of the agency is forecasted to be completed by November 2023.

Public Sector Data Sharing Act of 2021, which should be updated to facilitate identity data validation via exchange of information.

The Data Protection Act promotes confidentiality and regulates the use of personal identifiable data. This legislation is not specific to the use of data in the database of national identification data.

There are no interoperability or data sharing laws that pertain to identity data management by the government to accommodate how government agencies should link and verify identity data automatically. There is a Public Sector Data Sharing Act of 2021, which should be updated to facilitate identity data validation via exchange of information.

Another important area needing attention is the risk of misuse of identity number and other identity data. This includes the risk associated with the current SSB card and number, specifically how personal information is made available within government agencies and to other parties. Typically, provisions for misuse are documented in computer misuse-related legislation. This should be revisited when the new legislation for National ID is drafted.

Legal and Trust Framework Objectives

The following are objectives that should inform the legal and trust framework.

- Ensure that all recommended design elements adhere to existing treaty and legislation and/or recommend areas where legislation needs to be introduced or amended.

- Ensure that the system, including all laws, processes and procedures, engenders trust with stakeholders at all levels (legislators, issuers and citizen users). This is essential to promote widespread adoption and use.

- Establish a governance structure/authority to issue and manage the digital identity, including the personal foundational identity data.

- Provide an approach that protects individual privacy and integrity of citizens' personal data: Privacy by Design. Good data protection implementation helps inspire public trust and confidence and enables an effective digital identity strategy.

- Carry out an assessment of the existing legal and regulatory framework to ensure that the national ID system and operations will be able to be created and perform its functions:

  - Legislation drives all of the frameworks for purpose-driven identification.

  - Establish a new institutional governance approach for National Identity in cooperation with VSU.

  - Update personal data protection legislation.

  - Review and update other legislation impacted by the creation of National Digital Identity.

National Digital ID Legislation Considerations

The purpose of the legislation is to:

- Enable the government and the private sector to use the system to access and rely on identity and attribute verification services throughout the system

- Formalize the creation of the authority to manage digital identity operations, expand, maintain, and regulate the system and the oversight authority to ensure the system is run efficiently and is trusted.

- Provide privacy and consumer protections specific to the system to support and encourage trust.

Specific protections should include the following:

- Requiring express consent before enrolling and enabling user authentication as a service
- Defining conditions for the collection and use of biometric information
- Defining the creation and use of a unique identifier across the system

The legislation could include amendments to other primary legislation to address provisions which may prevent, hinder, or otherwise inhibit the system operating as intended or a participant from performing their role in the system.

The legislation will apply across the range of activities involved with the system. At the broadest level, the legislation will define the term “national digital identity,” who can have one, what it can be used for, and any limitations on its use.

A national digital identity relies on information about an individual. The details, or attributes, used to create, use and re-use digital identity involve personal information. If this process involves facial verification or any other type of biometric data verification, then sensitive information is also involved, and adequate protection must be implemented.

The national digital Identity system also involves information about when a person last updated their email and /or mobile phone number. The system will also facilitate an individual acting on behalf of another individual.

Extending the system to provide for state and private sector participation requires the development of an appropriate liability framework for holding the participants accountable for loss and damage suffered by other entities, including relying parties and users of the system

While there is an existing legislation on Cybercrime, the future ID legislation will need to add provisions to cover the National ID Program in relation to Identity theft.

The legislation should also include support for victims of cybercrime and identity theft by making reference to the national ID components such as ID card, unique ID number and identity data stored in the national ID database. While there is an existing legislation on Cybercrime Act 32, 2020, the future ID legislation will need to make reference to this Act but add provisions to cover the National ID Program in relation to Identity theft.

The accredited participants for digital identity should address risks of cybercrime and identity theft by demonstrating strong security and privacy safeguards, having processes for users to temporarily suspend their account if they think it is being used fraudulently, and providing users with cybersecurity support services to help users who believe their digital identity might have been compromised.

Safeguards

Safeguarding personal data should be one of the most important design features of the system. The legislation will define these safeguards designed to protect the personal information of the users.

Security

The National ID System will be subject to comprehensive end-to-end cybersecurity assessments and risk treatments to ensure ongoing security enhancements. The system will have to be based on a trusted digital identity framework to be able to support a secure way of proving an individual’s identity online.

Privacy

Privacy by Design must be the first principle to consider in the technical design and policy framework. In particular, it will be important to define strict requirements related to the following processes:

- Collection, use, and disclosure of personal information/ identity attributes (partial or complete)

- Disclosure of any data breach to the oversight authority and any other authority dealing with this type of issue

- use of a universal digital identifier and the use of biometric information for digital identity creation as well as authentication

While a strategy is developed to enable government services to be proposed and completed end-to-end on line, government obligations to ensure services can be accessed via non-digital channels.

Choice

Workshop participants emphasized that creating and using a national identity is voluntary. But this option will have to be revisited during or after the review of the report. While a strategy is developed to enable government services to be proposed and completed end-to-end on line, government obligations to ensure services can be accessed via non-digital channels. Also, there are smaller public and private sector services that can provide only one mechanism to verify identity.

Restrictions on Data Profiling

The National Identity System will have to be designed with a range of both technical and policy restrictions to limit data profiling. For example, in order to limit the collection, use, and disclosure of information about a user for the purposes of verifying the identity of an individual and assisting them to receive a digital service from a relying party, supporting identity fraud management functions, and improving the performance or usability of the accredited participants, the system will be designed to be easy for the individuals to prove their identity, by, for example, passing some limited and relevant attributes through the system (e.g., date of birth).

Biometrics

Biometric one-to-one matching technology provides a secure, convenient, and reliable way to check that a person is who they claim to be. However, biometric one-to-one matching is different from the initial use of biometrics when the system used a 1:N search process to look for the unicity of the person in the database. The digital identity system should limit the use of biometric information by accredited participants to permitted purposes such as proofing (e.g., face matching), as long as the matching process uses a verified photo of the person. Users who choose to verify their photo ID documents, such as a passport, would require an in-person verification of identity by presenting them at a government-accredited check point. If the process is performed online, the remote biometric-matching process might be executed by the system, but the end result will have to be reviewed by a trained operator. All of these processes will need to be clearly defined to guarantee protections of sensitive information such as biometric information.

Consent

The system should be built around user consent. User consent should be sought each time the person transacts with a relying party.

Age

As different standards are applied in different contexts for minors, a minimum age limit for access to the system should be set, with override mechanisms to enable the system to be flexible and responsive.

Disclosure of Personal Information

Legislation should expressly prohibit improper disclosure of sensitive or other personal information. Mechanisms should be put in place in the existing Privacy Act which could apply and could be reused.

Accessibility and Anti-discrimination

The National Identity System should be implemented using the government's Digital Service standard by requiring services to be accessible and inclusive of all users, regardless of their ability and environment. Typically, alternative identity proofing processes should be implemented to assist individuals who face difficulties in providing necessary documents when seeking to verify their identity.

The oversight authority should be guided by the following principles: independence, transparency, and accountability.

Governance

Effective governance of the system is essential for its efficient operation and for instilling public trust and confidence. The legislation will provide for the creation of an oversight authority to manage the Digital Identity System. The oversight authority should be guided by the following principles: independence, transparency, and accountability.

While there is a global trend in emerging countries to create a National ID agency to integrate civil registry operations within the same structure to improve the efficiency of identity-related operations, this can be achieved by defining the principles of governance for identity management in country, including civil events registration. After discussion with local stakeholders, the recommendation would be to define how a new centralized and integrated governance authority will support both the registration of civil events and the administration of the National ID program. This is what the government of Jamaica defined when it documented the creation of the National Identity and Registration Authority (NIRA) in the National Identity Act. There are many other examples in Africa, the most recent one being the creation of the National Identification Office in the Ivory Coast.

In conclusion, this list of considerations should be used as a guide to draft the future bill supporting the creation of the National Identity initiative. The review of existing legislation related to personal data protection show that the Economic Commission for Latin America and the Caribbean (ECLAC) benchmark study determined moderate alignment with GDPR and identified other areas of noncompliance to be addressed. A stronger focus on identity fraud and misuse will have to be developed and included in existing legislation related to cybercrime. Finally, it will be also mandatory to identify amendments to other legislation and policies regulating identity management across different agencies in Belize given the focus on electronic identity verification transactions and interactions supporting the National Digital Identity System.

Design Components of a National Identity System

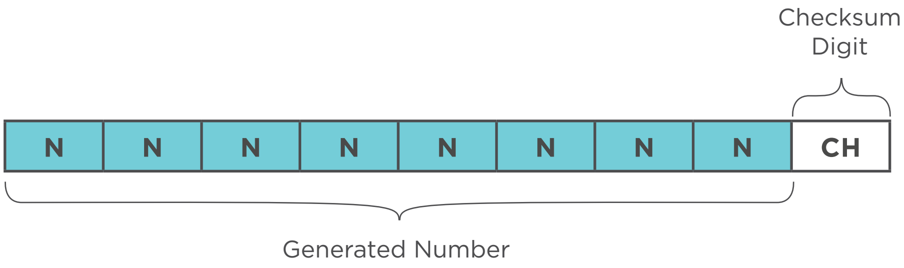
A number of design decisions must be made for the National ID System at very earlier stages. Some of them were already mentioned with respect to the legal framework, and some were also briefly mentioned while presenting the constraints. The following are some of the most important design considerations, which include technical, business, and operational elements.

National Identity Number

The national identity number (NIN) can be a nine-digit unique random number issued to each enrollee in the system and shall conclusively resolve an identity. The format provides maximum compatibility with legacy systems that were designed to support existing ID numbers. For instance, the Social Security Identity System also identifies each new register with a nine-digit ID number: thus, any system that supports SSN can be easily updated to support the NIN.

The National ID System shall support the creation, issuance, and life cycle management of the NIN. The number generation process implemented shall guarantee and assure uniqueness; protect and maintain an individual's privacy; be transparent; and allow full, 100 percent auditability and reconciliation to mitigate fraud and identity theft.

The proposed format for the NIN is based on current best practices applied to the context of existing identity frameworks. Further, this approach allows the NIN to co-exist with the Social Security Numbers (SSN).



NNNNNNNN	8-digit numeric portion Computer generated Not guessable and non-sequential
CH	Modulus 11 check digit Computer generated from the numeric portion and appended to the number

As a good practice, we recommend leaving out the actual Social Security Number range: although the systems are not related and any number can be assigned to the NIN, it creates less confusion if numbers are used that are out of the range of the social security card. As of August 5, 2022, the last Social Security Number assigned was 000591605.

Finally, the process for generating the NIN shall exclude undesirable number sequences (if any).

A modulus 11-check digit shall be appended at the end of the unique identifier to provide an integrity mechanism to ensure that the NIN is internally consistent. Use of the check digit allows a quick offline verification of the integrity of the number and helps prevent the mis-keying of the number if it is being manually entered into a system. Note that the checksum only assures the integrity of the number; it does not assure that an identity is valid.

Accepted Documents

In most countries, and following UN recommendations, a birth certificate is the document used to create a National Identity. It is usually linked with biometrics from parents (mother for example), creating a link that represents a permanent and unique registry. In other words, a birth certificate is linked to an individual by means of the biometrics acquired to that individual, and that registry is identified by a National Id Number or NIN. This is also the recommendation for Belize.

In the case of residents (non-Belizeans), the document used to create the identity should be the one issued by Immigration and the passport or other ID document issued by the country of origin.

National Identity System Data Requirements

Stored data should be minimized, and required data to complete an enrollment should be the minimum set that is required to generate an identity.

Following "privacy and security by design" recommendations, stored data should be minimized, and required data to complete an enrollment should be the minimum set that is required to generate an identity. The data architecture identifies and standardizes the data elements that are required to represent the personal information associated with an enrollee in the National Identity System. It defines the data elements (e.g., first name, last name, date of birth, residential address, etc.) as well as the data element type (e.g. number, alphanumeric, date, etc.).

In an ideal world, all government systems would use standardized data architecture. Such an approach would include a common set of data elements, a common metadata specification, and a standard data and metadata framework for interoperability. Such standardization provides consistent data representation and enables efficient exchange and processing between systems and removes inconsistencies/ambiguities.

Central Civil and Biometrics Database

The National ID System database shall maintain and manage the identity information associated with each enrollee in the system, including links to the biometric data. The database will conform to accepted international standards. The dataset will consist of the core identity elements recorded during the enrollment process. This dataset will be queried by the Verification Service to confirm identity. The set of data elements to be supported should be kept to the minimum required. The data will be stored in the database with an electronic signature of the data record as a protection mechanism against unauthorized modification. Encryption shall be employed on key data elements in the database to ensure confidentiality of the information. A flexible database structure and schema will be used to allow for modification/enhancement as required over time.

Credentials

The most important use of a National ID credential is as a proof of identity. In the context of a National Digital ID System, this proof has to be done in both the physical and the digital world. In most countries, a national ID card is issued that serves as the first purpose. If the national ID card also includes digital certificates (i.e., an e-ID card) then the same credential can also be used in the virtual space to conduct electronic transactions. In reality, most national ID card programs have suffered from the complexity of implementing what is called the middleware (card readers and software) necessary for the use of the applications on the smart card in the field as well as the lack of connectivity throughout the country.

Most national ID card programs have suffered from the complexity of implementing the middleware necessary for the use of the applications on the smart card in the field.

Physical Transactions

The Social Security Board issues a Social Security card, which is a PVC card. The same happens with the Elections & Boundaries: an electoral card is issued, which is also a PVC card. Thus, one option is for the National ID System to issue a PVC card.

However, the approach followed by most countries is to use a polycarbonate card. This card is much more secure and more durable than the PVC, but it is more expensive. One of the driving reasons for making these changes is to improve the trustworthiness of the system, which may also imply improving the actual physical credentials (based on PVC). This is why we recommend polycarbonate as the main option.

Electronic Transactions

In order to select the correct credential for electronic transactions, is necessary to refer to the levels of assurance explained in Section 1. The ISO/IEC recommends the following levels, depending on credential management and authentication process:

- Level 1: User/Password (no restrictions).
- Level 2: User/Password with strong password policies (NIST 800-63)
- Level 3: Two factor authentication (including OTP, PIN)
- Level 4: Multi-factor authentication (at least two), where one is always a Digital Certificate issued by an approved PKI and It must be stored on secure devices.

In some countries, biometrics is added as one of the possible authentication methods for Level 3 or Level 4. To obtain Level 4, several options are available: mobile ID/ eWallet app, the cloud (HSM), secure Tokens, and eID Cards. In a National ID System, several options can be used at the same time.

Biometrics Requirements

Biometrics is one of the key elements of a National ID System. It links an individual with the biographic information, creating a unique identity. In Belize, both the Social Security Board and the Ministry of Immigration are incorporating biometrics (and in particular fingerprints) into their processes.

Biometrics can be used in any of the identity lifecycle processes: (i) enrollment and renewal, (ii) vetting and registration, (iii) credential issuance, and (iv) authentication. Biometrics are strongly recommended, at least for the vetting, to ensure the uniqueness of each identity. For this purpose, fingerprints are the preferred option. Although facial recognition systems have improved significantly in recent years, fingerprints (especially, ten fingerprints) ensure greater accuracy.

If possible, ten-fingerprint acquisition is recommended to ensure uniqueness. It is easier to acquire them the correct way (there are scanners that detect fingerprint positions if done with slaps), and it also ensures the capability to continue identifying the person even if some of the fingerprints are damaged or missed.

The biometrics will be captured during enrollment and used to assist in the vetting process (adjudication of the presented identity to assure the applicant has not previously enrolled and was issued a NIN). Depending on the decisions made, it can also be used for identity verification. However, subject to legal regulations/requirements, biometrics will only be enrolled for applicants over the age to be determined by law. If enrollment occurs before that age (e.g., at birth or upon entering school) the biometrics should be added to the system once the specified age is reached at the appropriate renewal point.

With respect to facial recognition, even if it has improved significantly in the last 10 years, all systems degrade its performance for children.

Biometrics (fingerprints and facial) can be enrolled starting at birth, but both face and fingerprint cannot be used for de-duplication (or any other identity verification process) until the person is at least 6 years old. In fact, most countries that implement fingerprints start to acquire and use them between 12 and 14 years old, although in some countries the age is from 6 years old (Uruguay, Jamaica). Although not related to national ID systems, there are also cases of newborns being enrolled with fingerprints (Brazil). With respect to facial recognition, even if it has improved significantly in the last 10 years, all systems degrade its performance for children. This is why, regardless of when biometrics will be acquired, if the system is supposed to enroll from birth, two cases need to be differentiated:

Enrollment without Biometrics

If the decision is to enroll into the National ID System from birth (which is highly recommended), this first enrollment will not include the acquisition of biometrics. The biometrics for the specific individual will be acquired at the renewal of the National ID Card. The following strategies can be considered to improve the security of the system:

> Capture biometrics but not use them for de-duplication. In this case, the fingerprints and face can be used for verification when faced with an issue. It also serves as a dissuasive element.
>
> Capture the biometrics of the person responsible for the enrollment. This, too, is a dissuasive element because if something is done illegally, that person will be linked with the registry and can be prosecuted later.

These two strategies are not mutually exclusive: both can be implemented at the same time, which will increase the security of the entire system.

Enrollment with Biometrics

For persons older than the defined age, a full biometrics enrollment will be performed. This includes capturing 10 fingerprints and a face image. The major processes associated with biometrics are (i) enrollment, performed during the initial in-person interview (and at renewal) with digital cameras and electronic fingerprint readers; (ii) extraction, conversion of the raw captured data to comply with standards; and (iii) comparison, either verification with the biometric data stored or a search of the database for a match.

A minimum of four fingerprints (two from each hand) is needed for matching purposes to assert uniqueness, but we recommend acquiring the full ten fingerprints. This will ease the process and the identification of each fingerprint and will increase the coverage of cases. Exception processing will be implemented for situations where fingerprints cannot be captured (e.g., loss of a limb, etc.) but it must follow a strict process, with the approval of a supervisor.

Fingerprint data should be acquired and stored in both a full image (for future new biometric matching improvements) and in the corresponding minutiae template for all ABIS processes (1 to 1 and 1 to N searches). Acquisition quality will be ensured by a minimal quality threshold on fingerprint scanners at enrollment points. The biometric information shall be stored in an ABIS system, and all biometric data shall be stored in a dedicated, separate, and protected civilian database environment to ensure system integrity.

Biometrics Standards

The National ID System should base the implementation and use of biometrics on well-established standards, in particular those related to storage and interoperability. This will increase interoperability and reduce the risks of "vendor lock-in." The ISO/IEC has several biometrics standards that a National ID System should follow:

- ISO/IEC 19794: defines the interchange format for several biometrics (fingerprint, facial, etc.). In particular, 19794-2 defines the way fingerprint minutiae are stored and interchanged, and 19794-5 defines the same for facial images.

- ISO/IEC 29794: specifies different quality criteria to capture biometrics samples. This is very important, as the quality of any biometrics system strongly depends on the quality of the stored data.

- ICAO Document 9303. ICAO Standard is endorsed by the International Organization for Standardization as ISO/IEC 7501-1 and regulates the entire lifecycle of travel documents (ID cards, passports, visas, etc.). It is particularly important for the acquisition of the facial image. It is strongly recommended that the system includes ICAO quality rules for the verification of the facial image acquired during enrollment.

Depending on the use of biometrics (for instance, if the eID card will have a Match on Card application), other standards may be required. Finally, while there are many vendors (both hardware and software) that can support these baseline requirements, the performance results to the NIST tests and the track records and references of National ID cards projects shall provide direction for the selection of biometric hardware and software vendors for the system.

Automated Biometric Identification System (ABIS)

The component in charge of managing biometrics is known as Automated Biometric Identification System (ABIS). It will store all the biometrics associated with enrollees (fingerprints and digital photographs). It is a highly specialized component and is critical to the security of the entire system. This is why care should be taken at the moment of selecting, installing ,and operating the system. The ABIS shall complete the following:

- Provide 1-to-1 (1:1) biometric authentication (fingerprint, facial or both)
- Provide a 1-to-Many (1: n) search capability (fingerprint, facial or both)
- Conform to internationally accepted standards for biometric capture, storage, and matching
- Provide local and offsite data backup and redundancy/failover protection and disaster recovery

Security Framework

The future Belize identity and attributes trust framework will let people use and reuse their identities (both digital and physically). It will also give them a way to share their attributes with other people and organizations more easily.

One reason why this does not currently happen is because one organization does not know how another creates digital identities or attributes. This means that they are unable to trust the security of the processes followed by other organizations.

The trust framework is a set of rules that different organizations agree to follow to deliver one or more of their services. This includes legislation, standards, guidance and the rules in this document. By following these rules, all services and organizations using the trust framework can describe digital identities and attributes that they have created in a consistent way. This should make it easier for organizations and users to complete interactions and transactions and share information with other trust framework participants. The development of the Security framework will have to be integrated in the one developed to support the government’s Digital Agenda.

Identity Framework and Interoperability

One important component of the National ID System will be the interoperability layer. It will provide unified and secure data exchange between organizations and in relation to ID verification as a gateway to validate Identity verification requests.

During the consultations for this study, respondents mentioned an initiative called “enterprise bus,” which could be developed to support this purpose. One of the best-known examples is the X-Road software product originated in Estonia, now a digital public good open-source software product. It is a standardized, cohesive, collaborative, interoperable, and secure data exchange layer that gives service providers an entirely new opportunity to make themselves visible in services directed at citizens, businesses, and civil servants. Creating entities that combine many different services and data sources is easy and cost-efficient.

X-Road is a centrally managed distributed data exchange layer between information systems that provides a standardized and secure way to produce and consume services. X-Road implements a set of standard features to support and facilitate data exchange and ensures confidentiality, integrity, and interoperability between data exchange parties:

address management
message routing
access rights management
organization-level authentication
machine-level authentication
transport-level encryption
time-stamping
digital signature of messages
logging
error handling.

The reference to X-Road could be used to define the necessary functions and features of such a capability. The direction proposed in Belize of an interoperability bus architecture could also be recommended as a sound option.

Public Key Infrastructure

There are usually two possible relations between a National ID System and a public key infrastructure (PKI): PKI for travel documents and PKI for digital signature and authentication.

The first PKI is related to the issuance of electronic passports (ePassports) and electronic travel documents (EtD). This is a very specific PKI, with well-defined requirements included in the standard for travel documents from ICAO. In particular, ICAO 9303 Part 12 standard governs the use of PKI for ePassport and states that the certification authority (CA) for the ICAO PKI must be a root CA with no sub-CAs or cross certifications. This implies that the ICAO PKI must be a separate PKI with its own CA, independently of any other PKI that can be implemented in the country.

In Belize, the Ministry of Immigration is already installing an ICAO PKI for the issuance of ePassports. Because the standard defines that only one PKI can issue travel documents per country, if it is decided that the National ID Card should also be a travel document, then a connection with the ICAO PKI is required. Note that the use of the National ID Card as a travel document requires regional or inter-country agreements. A good example of this is Mercosur, where all member countries accept National ID documents issued from any other member country.

The second PKI is the one used for digital signature and authentication. The National ID System need not be the agency in charge of issuance of the digital certificates. Digital certificates are usually included either on the eID Card or in the Mobile ID App. Note that this is not a requirement for a National ID System; in fact, the National ID System can be used as a support for digital signatures. This second PKI should be analyzed in the light of a National eGovernment Strategy, related to the National ID Strategy but independent of it. Whether it can be implemented at the same time will depend on the level of maturity of both strategies.

In conclusion, for the time being, there is no PKI implementation strategy at the government level.

Physical Locations

Core Identity Management System and Networking

The government of Belize should host the core identity management system, including the identity database (biographic and biometrics). It already has some key security features, as being ISO 27001 certified. If the government data center does not have the required space (which seems to be the case, as there is today no space for an additional rack), it is recommended that the existing government data center should be leveraged rather than creating a completely new one.

Biometrics System and Database

These components should be located at the government's data center but on different physical servers than the core identity management system. Usually, ABIS systems operate on dedicated but not specialized (COTS) hardware.

Enrollment Centers

One of the core principles of a National ID System is inclusion, which comprises coverage and accessibility. For this reason, it is key to have broad distribution of the national ID services around the country. It is strongly recommended to have a physical presence in every region, with at least one enrollment center in each district capital. The geographical distribution should be carefully designed to be profitable (or at least not too expensive). Because of Belize's small population size, the number of required enrollment officers per office (after the massive enrollment project is completed) can be small.

However, there should be at least one enrollment officer in charge of the enrollment process and one supervisor in each office. The reason for having at least two persons in the office is security. In some operations that require alternative paths (e.g., not taking a person's fingerprints), a supervisor should authorize such operations. Ideally, a third person should perform two other activities: receive the people to be enrolled and organize the internal flow of the office, and deliver the card to the citizen. In offices with very low activity, these other tasks can be done by the supervisor.

Vetting

Vetting should be done in a centralized environment, with no physical connection with any enrollment workstation, and isolated from the credential production room (although it can be in the same physical space). Usually, access to the vetting operations room is restricted to accredited operators.

Credential Production

Card production requires a dedicated and secure environment, ideally temperature-controlled. The space allocated must be different from the one allocated for the Identity Management System, in the sense it has to be located in a dedicated room but it can be physically located in the same building.

Credential Delivery

Credentials can be delivered at the enrollment offices. This is generally the best approach in terms of cost, as there is no need to distribute the cards throughout country or to have other dedicated places for delivery. In any case, credential delivery can be done independently of the enrollment centers, although the activity should be integrated within the National ID System.

National Identity System and Operations

Enrollment and Renewal

During enrollment, biometrics are captured live, by means of fingerprint scanners and cameras. It is not advisable to accept biometrics on a previously captured record (for example, paper-based photograph). This is the main reason why enrollment must be done in person, with the intervention of an enrollment officer. The demographic characteristics of Belize, where 55 percent of the population live in rural areas, present some challenges to the deployment of enrollment centers. The following approach is recommended:

- Locate one enrollment center on each major city/town (for instance, on each capital District). The enrollment center can be an independent building, rented for National ID-specific purposes, or it can also be a defined space on an existing office (for example, SSB or VSU offices). In Jamaica, for example, NIRA offices are located in Jamaica Post Offices.

- Place semi-mobile units in smaller locations, such as government buildings or NGOs, on specific days of the week, based on a well-defined schedule.

- Finally, there should be some fully mobile units that can reach remote locations and perform the entire process using mobile equipment.

This scheme applies to both enrollment and renewal, but it can also be used for the delivery of the national ID card. Mobile enrollment workstations (and in general, all workstations) should be able to work offline, to prevent a possible outage of internet connection.

Vetting

Vetting is the process by which the data presented by an applicant at the enrollment step are screened for legitimacy before they can be incorporated into the National ID Database as a valid identity. A robust vetting process helps assure the integrity of the system and thereby establishes trust in the system.

Applicants should be informed during enrollment that the information presented, including their biometrics, will be vetted and they should be offered an overview of the process. Vetting includes the steps for confirmation and validation of biographic data presented. The depth of the checks will vary according to the level and quality of the supporting materials presented.

Also, during enrollment, the applicant must declare and confirm that the information given is true and complete and acknowledge that any false statement or deliberate omission may be grounds to deny the issuance of a credential, at a minimum, or may also be grounds for prosecution. This attestation must also be signed and recorded as part of the enrollment record.

The proof-of-identity information presented should be validated against the issuing authoritative identity data sources to confirm legitimacy if necessary.

Trained vetting officers shall adjudicate the information presented at enrollment, including biometrics, with a view to approving the applicant for acceptance into the system. The proof-of-identity information (including provided documentation such as birth records if not already approved during enrollment, driver's licenses, voter's ID cards, etc.) presented should be validated against the issuing authoritative identity data sources to confirm legitimacy if necessary. Wherever possible, an electronic interface is preferred to verify the correctness and authenticity of the information (for instance, with a connection to the VSU to verify birth certificates, or to the Social Security Board to verify social security card information).

To prevent duplicates, the biographic and biometric data are screened against all the identities already registered in the system. The vetting process must be physically and operationally independent of enrollment to prevent collusion.

Experience shows that issues encountered in vetting rarely arise because of a single problem: it is usually a combination of factors that bring about potential issues and risks. It is therefore essential that the vetting process carefully in an auditable way builds a complete identity picture, so that a broad understanding of the person can be gained, and all the facts verified.

Credential Personalization

Once vetting is complete and an application is approved, an ID card may be authorized for production. To provide the greatest cost efficiency, a centralized card production approach should be implemented, with a single facility responsible for printing. Cards shall be pre-personalized by vendor(s) who are vetted and approved for supply. Vendor(s) will use a secure handling methodology and supply the pre-personalized stock to the central printing facility. The final personalization (including programming if a smart card) shall be carried out at the production center and the cards forwarded for issuance.

Credential Delivery

Following production, the national ID card must be delivered to the enrollee. The cards are produced at the central card production center and securely shipped to the enrollment center for issuing to the applicant. While this is inconvenient for the applicant, who must make a second visit to the enrollment center, it provides the added security that the card will be issued in person to the applicant/recipient and verified with the biometric. Notifying the applicant via email, SMS, or another means that that their card is ready to be collected should be considered.

While delivery is an independent process step, it is commonly performed at the same location as enrollment. This is more cost effective than establishing a separate delivery location (the equipment needed for delivery is already there) and typically is also convenient for the enrollee.

Scheduling and Pre-registration System

Complementary to the enrollment system, we are considering scheduling and pre-registration to facilitate the enrollment process. This system will be responsible for scheduling an appointment to perform the enrollment or renewal of the document. It will include remote/online pre-registration and in line pre-registration, while also facilitating payment processing for lost, stolen, and damaged cards (both online and in-line). This will be a cashless operation; payments will be made via bank payments or credit/debit card.

Identity Lifecycle Management

The key guiding principles that a National ID System should follow for the management of the identity lifecycle are:

- Transparency and accountability
- Increased efficiency
- Cost optimization
- Scalability and incremental expansion
- Enhanced stakeholder experience

A well-designed Identity Lifecycle Management System must address all of these principles. The identity lifecycle consists of four basic processes: origin, use, control, and retirement/archive. With respect to identity origin, the focus of most recent standards/practices has been on travel documents (e.g., the electronic passports based on ICAO 9303 specifications, the new generation of e-ID cards, etc.). These have focused primarily on the way the breeder documents, such as birth certificates, are generated and consequently how such identity data are registered, validated, and managed over time.

For consistency in use and control, identity management within the system framework is based around the use of a unique personal identifier (NIN) for each enrollee. Generation of the NIN serves as an anchor point for the identity lifecycle, including management of associated attributes. For transparency and accountability, once the NIN is permanently assigned to the enrolled identity, it will never be re-used or re-assigned. Authorized system users may only update attributes associated with an identity (e.g., name, address, etc.) under circumstances/conditions defined in policies, with an auditable log being maintained of all changes made.

The unique NIN identifier enables more precise maintenance and update of the identity over time, including validation and reconciliation of changes in civil status (such as marriage, divorce, name change, death, etc.). The NIN also enables identity verification as a service for participating stakeholders (both in government and in private industry) and the unambiguous sharing of data across entities (where legally permissible).

The identity (and, by association, the NIN) is never deleted. Its status may become "active," "questioned," "retired," "inactive," or "revoked," but its record must remain indefinitely in the database and/or archives for transparency and future audit purposes.

Identity management is an evolving process. Processes must adapt as technology and environments change. The identity management framework and infrastructure must provide the flexibility to incorporate such changes as required.

ID Credential Life Cycle Management

ID credential management is a subset of identity management. While an identity never expires, best practices dictate that ID credentials should be issued for a finite period only. The option within the system to set the expiration date for an ID credential should be fully configurable to provide the maximum flexibility in meeting different lifecycle requirements for different credential types.

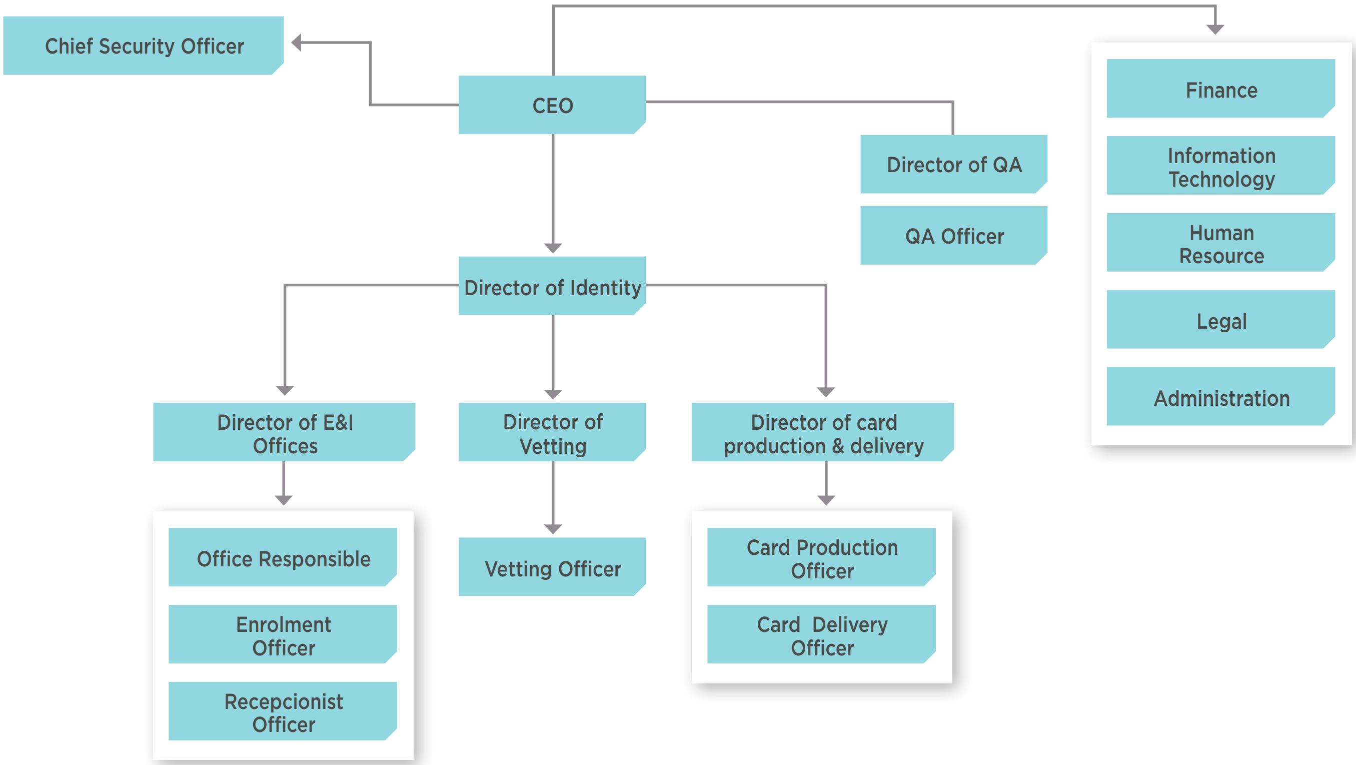
In the case of cards, there are at least two unique identifiers involved. One is the stock number, printed on the card by the card vendor during pre-personalization. This allows tracking and auditing of inventory to prevent misuse or abuse of card stock. The second mandatory unique identifier is the unique document number (UDN) that is printed on the card when it is personalized. The UDN shall be linked with the NIN in the database along with its expiration date. A replacement card or renewal card will be given a new UDN and the database will be updated accordingly.

The objective of this system is to track the life of each of the security materials used to build a card (in this case just the card), starting from reception of the blank material from the supplier and ending at issuance of the document to the corresponding applicant for the duration of the card.

The National ID System shall support independent renewal and replacement cycles for cards.

Human Resources

The following diagram depicts the usual roles of a National ID Agency:



Based on the proposed business process described in section "National Identity System and Operations" (which are based on best practices), a number of specific roles can be derived. The following is a short description for each one:

- **Enrollment & renewal officer:** The officer in charge of executing the enrollment and renewal process.

- **Enrollment office supervisor:** In charge of oversight of all the activities performed in the Enrollment Office (Enrollment & Renewal, Reception, and Credential Delivery). This is the highest authority in the enrollment office.

- **Vetting officer:** In charge of executing the vetting processes.
- **Vetting supervisor:** In charge of the overall supervision of all vetting processes.
- **Credential production officer:** In charge of credential (card) personalization.
- **Quality control officer:** In charge of performing quality control, in general on the credential produced. Quality control includes both the visual and the electronic components (if the credential has an electrical component).
- **Credential production & delivery supervisor:** In charge of the entire credential and delivery processes.

The following table contains estimates of required enrollment officers by district population.[16]

DISTRICT	URBAN	IN REGIME	RURAL	IN REGIME	TOTAL	IN REGIME
Corozal	13,314	0.40	37,176	1.11	50,490	1.50
Orange Walk	13,665	0.41	39,708	1.18	53,373	1.59
Belize	86,807	2.58	40,875	1.22	127,683	3.80
Cayo	56,251	1.67	45,861	1.36	102,115	3.04
Stann Creek	10,680	0.32	35,335	1.05	46,015	1.37
Toledo	6,530	0.19	32,995	0.98	39,525	1.18
Total	**187,247**	**6**	**231,950**	**7**	**419,201**	**12**

In some cities (Toledo, Orange Walk), the number of required enrollment officers is less than one, but as discussed in the Physical Location section, it is advisable to have

[16] Note that several reasonable assumptions were made: a) enrollment + new renewals per year correspond to 20% of the population size, b) enrollment/renewal take 15 minutes and c) there are 240 working days. For more information see the corresponding spreadsheet in the annexes.

three people per office. Adding two additional people yields the following number of people per office:

DISTRICT	POPULATION	# PERSONS PER OFFICE
Corozal	50,490	3.50
Orange Walk	53,373	3.59
Belize	127,683	5.80
Cayo	102,115	5.04
Stann Creek	46,015	3.37
Toledo	39,525	3.18
Total	**379,676.00**	**21.30**

In some districts, the rural population is greater than the urban one (e.g., Corozal, Orange Walk). In those cases, a mobile unit can be deployed to reach the rural areas. Each unit should have two officers: an enrollment officer and a supervisor (plus any other supporting personnel required, such a driver). This final table shows a configuration where each physical office has at least three people and each district has a mobile unit with two people.

DISTRICT	URBAN	# PERSONS	RURAL	# PERSONS	TOTAL	# PERSONS
Corozal	13,314	3.00	37176	2.00	50,490	5.00
Orange Walk	13,665	3.00	39708	2.00	53,373	5.00
Belize	86,807	5.00	40,875	2.00	127,683	7.00
Cayo	56,251	4.00	45,861	2.00	102,115	6.00
Stann Creek	10,680	3.00	35,335	2.00	46,015	5.00
Toledo	6,530	3.00	32,995	2.00	39,525	5.00
Total	**187,247**	**21**	**231,950**	**12**	**419,201**	**33**

If the recommendations are followed and more offices per district are added, the totals are as follows:

DISTRICT	URBAN	INC. SUPERVISOR + RECEPTION	RURAL	INC. SUPERVISOR + RECEPTION	TOTAL	INC. SUPERVISOR + RECEPTION
Corozal (+2 more)	13,314	3.00	37176	6.00	50,490	9.00
Orange Walk (+2 more)	13,665	3.00	39708	6.00	53,373	9.00
Belize	86,807	5.00	40,875	6.00	127,683	11.00
Cayo	56,251	4.00	45,861	3.00	102,115	7.00
Stann Creek	10,680	3.00	35,335	6.00	46,015	9.00
Toledo	6,530	3.00	32,995	2.00	39,525	5.00
Total	**187,247**	**21**	**231,950**	**29**	**419,201**	**50**

Note that each new office requires at least two extra people: a receptionist and a supervisor.

Regarding the other roles, the number of people required is the following:

ROLE	# PERSONS
Vetting officer	3
Credential production officer	2
Credential delivery officer[17]	2
Quality control officer	2

This exercise estimates requirements once the system is ready and most people are enrolled. The following section analyzes the number of officers required for the massive enrollment effort.

[17] For credential delivery and quality control, only one person is required (if only the number of credentials to be produced is considered). However, it is recommended that at least two people in the organization perform those tasks.

Registration (Enrollment) and Coverage

Belize has a population of 419,199. The objective of the system is to register the entire population, starting from birth. To enroll everyone, a massive enrollment effort must be undertaken for a given time period. Once the massive enrollment is completed, the system will demand fewer resources. This is mainly because most of the population will be enrolled and only renewals and new enrollments will require the officers' services. We call this second phase "in regime."

For the "in regime" system there should be at least six permanent physical locations, one in each district capital. The following is an estimate of the number of enrollment and vetting officers required to reach the enrollment of 75 percent of the population within a year[18]:

MASSIVE ENROLLMENT

TOTAL POPULATION	419,199
PERCENTAGE TO BE ENROLLED	75
EXPECTED POPULATION	314399.25

# years	# enrollment per year	# enrollments per day	# enrollment officers	# vetting officers
1	314399	1310	47	32
2	157200	655	23	16
3	104800	437	16	11
4	78600	327	12	8

To complete the massive enrollment process in one year, the number of officers needed is 79. In regime, the system will require 32 additional officers. That means that if the GoB wants to complete the process in one year, additional resources should be hired and trained. The following section (costs and benefits) analyzes the economic impact of this alternative.

[18] Annex "National ID - Estimates" includes an xlsx spreadsheet to be used for further estimates.

The “massive enrollment” process is a project in itself. This means that it must be carefully designed to reach its objectives. A key question is whether system will be mandatory or not. If the system is not mandatory, then a public relations campaign must be implemented to convince Belizeans to enroll. Another important consideration is how to reach all Belizeans, especially those living in rural areas.

One important consideration is how to distribute the expiration date of each card to have a smooth renewal process. Ideally, the same number of renewals should be performed each year. If the massive enrollment process is conducted in one year and all those documents are assigned the same expiration date (usually in 5 or 10 years), nobody will be required to renew for 5 or 10 years, but then the entire population will have to renew, creating peaks in the demand for the service.

6

Cost and Benefits

Cost and Benefits

Estimate Cost of ID Systems

Human Resources

To estimate the number of human resources needed, the following assumptions were followed.

- All clerks and personnel are on pay scale 7 (internal checks by the DTU team confirm that this is the case for the majority of VSU personnel: we believe that this is a good approximation for the new Identity organization). The PayScale in that case (from [approved budget estimate 2021-2022.pdf]) is the following: Pascale 7 = 17,675 (starting minimum salary) X 902 (yearly increment) - 34,813 (maximum salary).

- Directors of Unit/Department: Salary range 65k-70k BZD. Entertainment allowance: approximately 500BZD.

- CEOs: Salary range: 76K BZD. Entertainment allowance: 1,500 BZD

The figures used for the estimates are the following:

- All clerks: a mean value between minimum and maximum salary: 26,244 BZD, nearly US$13,122

- Directors: 70,000 BZD, nearly US$35,000 .

The analysis is based on the system operating with the offices and officers for the "in regime" phase. A specific section is included that details the economical effort for the massive enrollment phase.

FIXED COSTS

DESCRIPTION	UNITS	UNIT COST (USD)	TOTAL COST
Project Execution Team	1	$ 500,000.00	$ 500,000.00
		Total	**$ 500,000.00**

The estimate for processional services considers all services required to put in place a national ID system: ICT and business consultants to implement the business processes, legal advisors to develop the legal framework, program and project managers, and others.

RECURRENT COSTS	UNITS	SALARY PER YEAR	TOTAL (ANNUAL)
Required operational officers in Regime	36	$13,200.00	$475,200.00
Senior Management & Executives	14	$35,000.00	$490,000.00
Supervisors & IT Support	9	$20,000.00	$180,000.00
		Total	**$1,145,200.00**

Credentials

The type of credential will have a great impact on the cost. A typical eID card costs a little more than US$2, whereas a non-eID card (but still polycarbonate) costs US$1.0. In most countries, eID cards are only issued starting at a certain age, such as 14 or 18 years of age.

The following is a budgetary exercise:

	PRICE PER UNIT	POPULATION	TOTAL	RECURRENT COST (YEAR)
OPTION 1 eID Card	2.3	41,9199	**964158**	**192,832**
OPTION 2 Mobile ID for persons 15 years or older	1	27,0001	270,001	
ID Cards (no eID)	1	41,9199	419,199	
		Total	**689,200**	**124,339.95**
OPTION 3 All non-eID Cards	1	41,9199	**419,199**	**83,840**

eWallet or Mobile ID App

	TOTAL
Development/Implementation of Mobile ID/eWallet solution	100,000
Total	**100,000**

This estimate assumes that the Mobile ID or e-Wallet App is only provided for people older than 15 years of age.

Central IT Infrastructure

FIXED COSTS	UNIT	UNIT COST	TOTAL
ABIS Software	1	$250,000.00	$250,000.00
ABIS Hardware	1	$125,000.00	$125,000.00
National ID System Solution			$974,300.00
National ID Hardware			$1,040,000.00
Enrollment Workstations	25	$8,000.00	$200,000.00
Quality Control Workstations	10	$3,000.00	$30,000.00
Issuance Workstations	25	$5,000.00	$125,000.00
Reception Desk Workstation	10	$2,000.00	$20,000.00
Vetting Workstations	10	$1,200.00	$12,000.00
Mobile Enrollment Workstations	20	$1,700.00	$34,000.00
Investigative (forensic) workstation	2	$3,000.00	$6,000.00
Card production equipment	2	$80,000.00	$160,000.00
Card production software	1	$200,000.00	$200,000.00
Interoperability framework	1	$500,000.00	$500,000.00
		Total	**$3,676,300.00**

RECURRENT COSTS		TOTAL
Support & Warranty	15.00%	$605,775.00
CITO Hosting & networking	1	$40,000.00
	Total	**$645,775.00**

Physical Establishment to Locate the Enrollment and Issuance Centers

Several options have been discussed:

- VSU is not recommended because of the negative perception the population has about them. The same is true of police stations: there is a general mistrust of them.
- The Social Security Board is an option to be explored, at least in the towns.
- Other options are:
  - Telecenters managed by NGO
  - Public libraries
- It is not advisable for the enrollment process to be performed by people from outside the agency. A hybrid approach can be to use the infrastructure at the telecenters and public libraries but with officers from the National ID Agency. For example, the officers would be present on certain days and times.

Furniture & other office equipment	50	$500.00	$25,000.00
Building refurbishment			$50,000.00
Organizational Development & Management Plans			$50,000.00
National ID Legislation, Regulations and Policies			$170,000.00
National Identity Authority Personnel Establishment			$527,600.00
		Total	**$822,600.00**

RECURRENT COSTS	UNITS	COST PER UNITS	TOTAL
Rent of the Central office	1	$78,000.00	$78,000.00
Rent of district capital office	6	$2,000.00	$12,000.00
Office supplies, expenses, etc.	7	$50,000.00	$350,000.00
		Total	**$440,000.00**

Summary

DESCRIPTION	COST (USD)	RECURRENT COSTS (PER YEAR)
Polycarbonate cards (not eID)	$689,200.00	$ 124,339.95
Mobile ID / eWallet (more than 15 years old)	$100,000.00	
Human resources	$500,000.00	$ 1,145,200.00
Central IT Infrastructure	$3,676,300.00	$ 645,775.00
Physical stablishment	$822,600.00	$440,000.00
Public Awareness and Communication Campaign	$300,000.00	
Massive Enrollment (one-year effort)	**$1,168,000.00**	
Contingency (20%)		$471,062.99
Contingency (5%)	$365,055.00	
Total	**$7,621,155.00**	**$2,826,377.94**

A “massive enrollment” campaign will put in place 9 additional offices and 32 more officers that are not required after completion. These line comes from the following:

	ESTIMATED	SALARY PER YEAR (USD)	TOTAL (PER YEAR)
Additional operational officers	45	$13,200.00	$594,000.00
		sub-total	**$594,000.00**
		COST PER UNIT	TOTAL
Rent of district capital office	9	$2,000.00	$18,000.00
Office supplies, expenses, etc.	9	$50,000.00	$450,000.00
		sub-total	**$468,000.00**
COST			
Furniture & other office equipment	32	$500.00	$16,000.00
Building refurbishment	9	$10,000.00	$90,000.00
		sub-total	**$106,000.00**
		TOTAL	**$1,168,000.00**

Note: This total does not include telecommunications costs.

The recurrent costs does not include the additional cost to maintain these nine offices.

7

Risks and Success Factors

Risks and Success Factors

The following section is an extraction from the ID4D Practitioner's Guide, a good summary of the major risks any that ID system should monitor. Building an ID system that meets developmental goals is a multifaceted challenge in any context. It must mitigate potential risks to privacy and inclusivity, as be self-sustaining. In addition, developing countries face a unique set of challenges to implementing ID systems, particularly when digital. However, while no system is perfect, global experiences have also shown that there are common success factors that can help overcome these risks and challenges.

Risks of ID Systems

The experiences of a broad range of countries at varying levels of development highlight four main risks to implementing new or upgraded ID systems:

- **Exclusion.** In contexts where people were previously able to prove their identities through alternate or informal means, the formalization of a new ID system and the tightening of identification requirements—e.g., making access to social programs or voting conditional on a particular ID—risks further marginalizing vulnerable people who may not be covered by the system. Likewise, the failure of—or biases in—ID systems (e.g., failure of biometric authentication mechanisms, collecting data that is difficult for some people to provide, poor data quality, etc.) can lead to the exclusion of people from the ID system or accessing related services. Establishing a pro-developmental ID system therefore requires an exclusion risk assessment and explicit strategies to ensure access to identification for all, with particular attention to groups that are at higher risk of exclusion, such as remote and rural residents, the forcibly displaced, ethnic and linguistic minorities, people with disabilities, marginalized women and girls, and those with low connectivity or technical literacy. As part of the planning process, decision makers should also carefully consider the exclusion risks of formalizing or increasing identification/authentication requirements for different transactions.

Establishing a pro-developmental ID system therefore requires an exclusion risk assessment and explicit strategies to ensure access to identification for all, with particular attention to groups that are at higher risk of exclusion.

- **Privacy and security violations.** Inherent in the capture, storage, and use of sensitive personal data are risks associated with privacy violations, data theft and misuse, identity fraud, and discrimination. The emergence of new technologies and the increased collection and use of personal data by state and non-state actors compounds these concerns and brings new threats from cybercrime and cyberattacks. ID systems therefore require strong legal and regulatory frameworks and a privacy-and-security-by-design approach to mitigate these risks and ensure data protection and user control. Cybersecurity of the system within a secure environment should be part of the a priori design. Furthermore, an assessment of risks to privacy and security should be incorporated into the planning process (e.g., a Data Protection Impact Assessment, cybersecurity penetration tests and audits) and continuously through the implementation of an ID system.

- **Vendor or technology lock-in.** Dependency on a specific technology or vendor can result in "lock-in" and/or dependency, increasing costs and reducing flexibility of the system to meet a country's needs as they develop. This can occur, for example, through the adoption of a technology for which a limited number of suppliers are available, or contractual provisions in supply contracts or licensing agreements (e.g., for software) that restrict changes in technologies or vendors over time or may limit data ownership and access. Another cause of vendor dependency is when a vendor does not transfer knowledge or capacity to the government, which is a higher risk in poorly-designs public-private partnership and build-operate-transfer models. The risk of vendor and technology lock-in can be partially mitigated by the adoption of open, international standards and strong procurement practices that minimize unnecessary constraints in the choice of technology or supplier over unnecessarily long periods of time.

Ensuring that systems provide a good return on investment and are sustainable over time requires a detailed appraisal of local context and capacity and robust procurement guidelines.

- **Unsuitable or unsustainable technology and design choices.** In many cases, countries have adopted high-cost systems that have failed to achieve development goals because they were unsuitable for the context or unsustainable in the medium or long term. For example, many countries have rolled out expensive multi-purpose smartcards for their national ID systems without relevant use cases or institutional structures to leverage this technology. Ensuring that systems provide a good return on investment and are sustainable over time requires a detailed appraisal of local context and capacity and robust procurement guidelines. Policymakers can also explore various models through which ID systems may produce cost savings for governments, as well as partnerships with the private sector that may reduce upfront costs. For example, linking an ID system with a strong CR system reduces the need for expensive, ad-hoc mass registration drives to update data. To anticipate and control costs, a cost-benefit analysis of the system design should be completed during the planning process.

Challenges Specific to Low- and Middle-Income Countries

In addition to these universal risks, many low- and middle-income countries face an additional set of challenges when implementing ID systems:

- **Weak civil registration systems.** Both civil registration (CR) and ID systems are crucial to ensuring legal identity for all (SDG 16.9) throughout a person's lifetime. In much of the developed world, ID systems are based on strong CR systems that have provided universal or near-universal coverage of life events, including births, marriages, and deaths (with certified medical causes) for generations. In many developing countries, however, CR systems have historically been weak. For example, approximately 60 percent of children under five-years old living in the least developed countries have never had their births registered (UNICEF 2017), while death registration rates are even lower. This can complicate the identity proofing process for ID systems—i.e., people may have no or only low-quality documentation of who they are, especially when a birth certificate is a requirement—and makes it difficult to automatically retire identities after a person has died.

- **Limited connectivity and other infrastructure.** In many countries, rural and remote areas lack reliable mobile and internet connectivity. This can create difficulties when implementing digital ID systems that require power and connectivity during enrollment (e.g., for data transfer or duplicate biometric enrollment check) and for authentication. Furthermore, core ICT infrastructure, such as secure data centers, may not exist. In addition, the general lack of infrastructure such as reliable roads in rural areas and regions with difficult terrain make certain households difficult to reach and can increase the time and cost of enrollment. If these issues are not addressed through technology choices and outreach, ID systems are likely to be exclusionary in low connectivity areas.

- **Lower literacy levels.** In low- and middle-income countries, significant portions of the population may have lower literacy levels, both in terms of reading ability and the use of digital technology. This may translate into difficulties with enrollment, as well as the use of these systems for segments of the population who are likely to be among the most vulnerable. It also has implications for people's ability to provide informed consent to the collection and use of their data. As with low connectivity, illiteracy rates should be reflected in system design and implementation to minimize the potential for exclusion.

- **Lower government capacity and/or trust.** In certain countries, governments may have limited fiscal, technological, and administrative capacity to implement and/or regulate ID systems. Political instability and violent conflict may create or compound these difficulties in certain geographic areas or country-wide. In addition, past negative experiences may reduce people's confidence in the government and its ability to responsibly use and/or protect their personal data. While identity documents have been highly politicized in many countries—e.g., because of their link to certain rights such as voting—this may be exacerbated in contexts where the distribution of IDs can be more easily manipulated for political gain.

- **Poor procurement.** Low- and middle-income countries may have weak capacity and institutions to handle procurement and vendor contract management for an ID system, which is complex because of the wide-range of technologies available and different types of procurement that need to be completed. Further exacerbating this challenge are the tight deadlines that governments often impose for the introduction of an ID system, which puts pressure on agencies to reduce their planning time. The consequences of poor procurement processes and vendor contract management include failed procurements, delays (e.g., because of appeals), and vendor and technology lock-in.

- **Insufficient national cybersecurity capacity.** Low- and middle-income countries often have capacity gaps in their central cybersecurity agencies, which are needed to build a secure enabling environment for digital ID systems. Gaps can take the form of insufficient threat intelligence, breach monitoring and emergency response, sub-optimal hardware or software platforms, too few or insufficiently skilled cybersecurity analysts, weak cybercrime and cybersecurity legislation and weak cyber prosecution. The capacity of the central cybersecurity agency needs to be assessed for its ability to adequately support digital ID projects.

Success Factors

Addressing these risks and challenges requires thoughtful design and thorough planning, along with sufficient technical, political, and financial resources. In addition, it requires the following factors, which are critical for successful ID systems, and which are presented as risk mitigation recommendations:

- **Outcome and context-based design.** Key decisions regarding the design, rollout, and use of ID systems should be driven by the context, national goals, and people-centered perspectives, rather than by the technology itself. Technology choices should be based on a thorough analysis of the country's constraints and a clear understanding of how the system—including databases, credentials, etc.—will be used, what its primary applications will be (e.g. improve targeting of social protection programs, improving financial inclusion, etc.). Practitioners must look beyond mass registration—which is only an input into an ID system—when they are designing an ID system and pay sufficient attention to its authentication functions and other uses, as this is what will drive the impact of an ID system.

Technology choices should be based on a thorough analysis of the country's constraints and a clear understanding of how the system will be used

- **Coordinated governance and sustained political commitment.** ID projects and systems are ambitious and involve and extremely high number of actors and stakeholders, including ministries, levels of government, private companies, and international organizations, civil society organizations, and more. Few projects touch every single person in a country like the introduction of a foundational ID system. For ID projects to succeed, they therefore require a high level of political commitment, a "whole of government approach," and coordination to ensure a shared vision and a system that is useful to a variety of stakeholders. In addition, ID providing agencies require clear institutional and operational mandates and governance structures that provide enough capacity and resources to manage identification in the long run.

- **Strong legal, regulatory, and operational frameworks.** ID systems require an enabling environment that adequately protects individual data and rights, minimizes security risks, provides clear operational mandates and accountability, and ensures equality of access to identity documents and services. This includes primary and secondary legislation as well as internal operational guidelines, which should be updated to provide a holistic view of the collection, use, and management of personal data throughout the identity lifecycle, and is fit-for-purpose for the digital age.

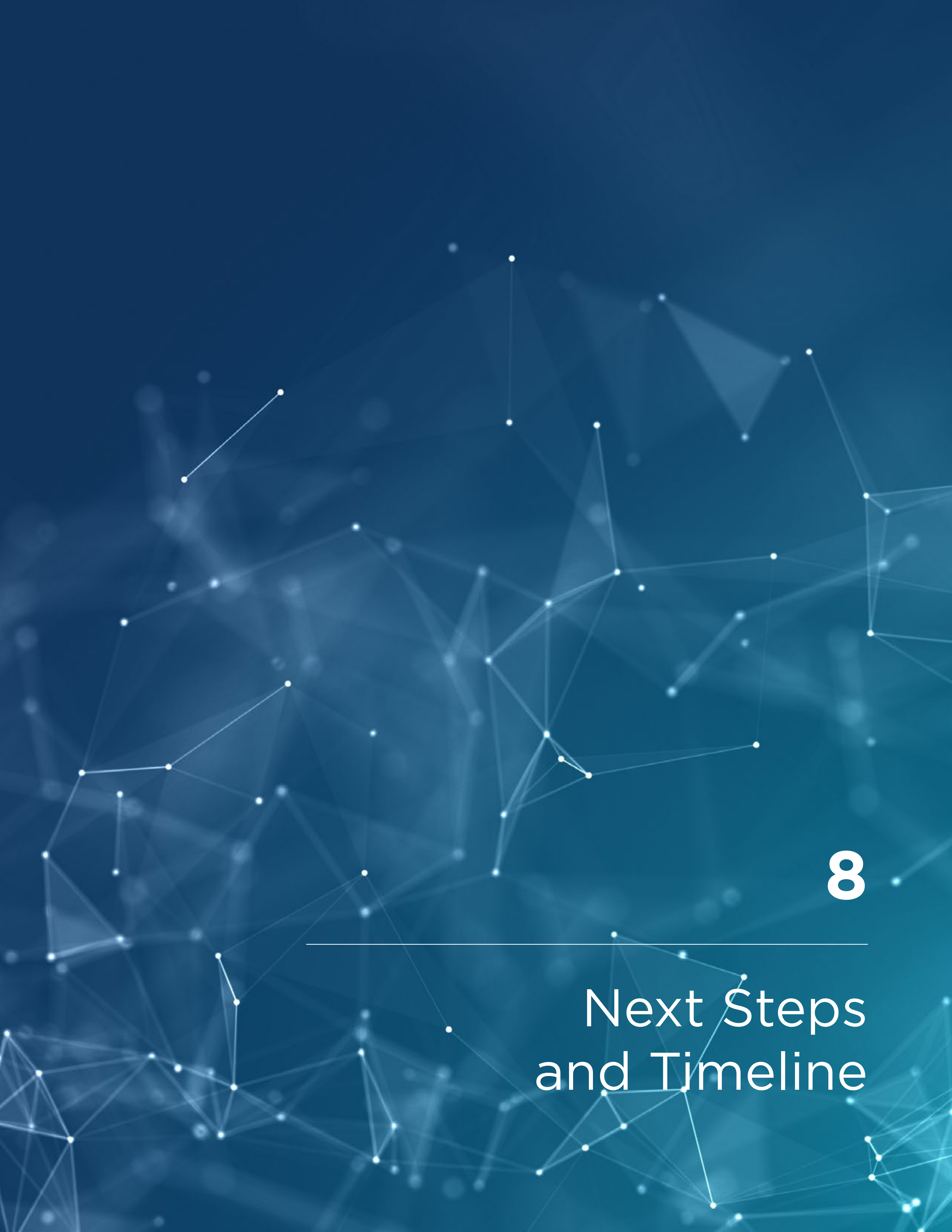
- **A "privacy-and-security-by-design" approach.** Privacy and security should be built into the enabling environment and the functional and technical design of ID systems from the beginning—rather than as an afterthought. This includes adopting state-of-the-art legal, management, operational, and technical controls to ensure the protection of personal data from misuse, unauthorized disclosure, security breaches including cyberthreats and cyberattacks, and function creep. In addition, it includes building mechanisms to ensure user consent, control, and oversight of personal data.

- **Specific strategies and efforts to reduce the risk of exclusion during enrollment and authentication.** To ensure universal access to ID systems, practitioners must adopt a deliberate, ongoing strategy to ensure that no one is left behind. This may include updating laws and procedures to remove discriminatory measures, outreach efforts to specific groups that face higher barriers to obtaining ID or have concerns, exception-handling policies and procedures for those without ID that prevent exclusion to basic rights and services and minimizing data collection and documentation requirements for registration.

- **Public engagement and consultation.** People are the subject and primary end-users of ID systems, yet these projects are often designed with little input from those they are designed to serve. Consultation during the planning phase and throughout implementation is crucial for understanding and mitigating barriers to access and designing ID systems that are user friendly and solve real problems. Conducting qualitative end-user research can help improve the design of ID systems from the perspectives of people (i.e. a bottom up rather than top down approach). Furthermore, intensive information campaigns are necessary to educate the public about registration, and—along with easily-accessible grievance redress mechanisms—are vital for reducing exclusion and improving trust in the system.

- **A holistic approach to CR and ID.** In order to (1) provide legal identity for all (SDG 16.9), (2) fulfil obligations for the continuous, permanent, compulsory and universal recording of vital events, and (3) ensure the accuracy and integrity of identity data overtime, countries should adopt a coordinated approach to simultaneously strengthen CR and ID systems and the linkages between these systems. In addition to independently investing in strengthening both systems, this could include interoperability and interfaces that allow for data exchange and/or queries, the assignment of a unique identity at birth from the ID system and through the CR system, and/or shared infrastructure and/or administration. Like any data exchanges between information systems, the linkages between CR and ID systems should be governed by relevant data protection laws and regulations. For example, a CR system collects more data for its statistical functions than are needed for identification, and thus only a limited amount of data needs to be shared.

- **Use of international standards.** Standards establish universally understood and consistent interchange protocols, testing regimes, quality measures, and good practices with regard to the capture, storage, transmission, and use of identity data, as well as the format and features of identity credentials and authentication protocols. They are therefore crucial at each stage of the identity lifecycle and help ensure that the building blocks of identity systems are interoperable and can meet desired performance targets. Furthermore, the use of international standards can help prevent vendor and technology lock-in by enabling the system to change its technology (e.g., ensuring data can be migrated and is compatible with different software), which is a key ingredient for operational and financial sustainability.



8

Next Steps and Timeline

Next Steps and Timeline

Based on this risk analysis list, while any project incurs a number of risks, the identification of these risks and the acknowledgement of potential success factors already existing or in development will help mitigate them. At the same time, after reviewing the challenges identified, the following plan is recommended.

- Alignment of the National ID project with the Digital e-governance agenda and strategy in terms of infrastructure, capacity, governance and planning of services which will require the adoption of Digital ID with a special attention to secure hosting, CERT, PKI

- Governance of the National ID initiative starting with the creation of a formal committee in charge and the appointment of a chairman. The work of this committee will be supported by a project office and an external subject matter / technical assistance

- Specific points of attention would be the need to update the on-going CRVS RFP to ensure future integration with the National ID program as well as the need to do a more in depth analysis of the Central Bank of Belize Digital Wallet program where development experience and lessons learned could be leveraged.

- Special attention should be given to ongoing biometric system implementation from SSB and the e-Passport to be issued by the Belize Immigration Department both from a technical /interoperability standpoint and the legal standpoint as far as protection of personal data is concerned.

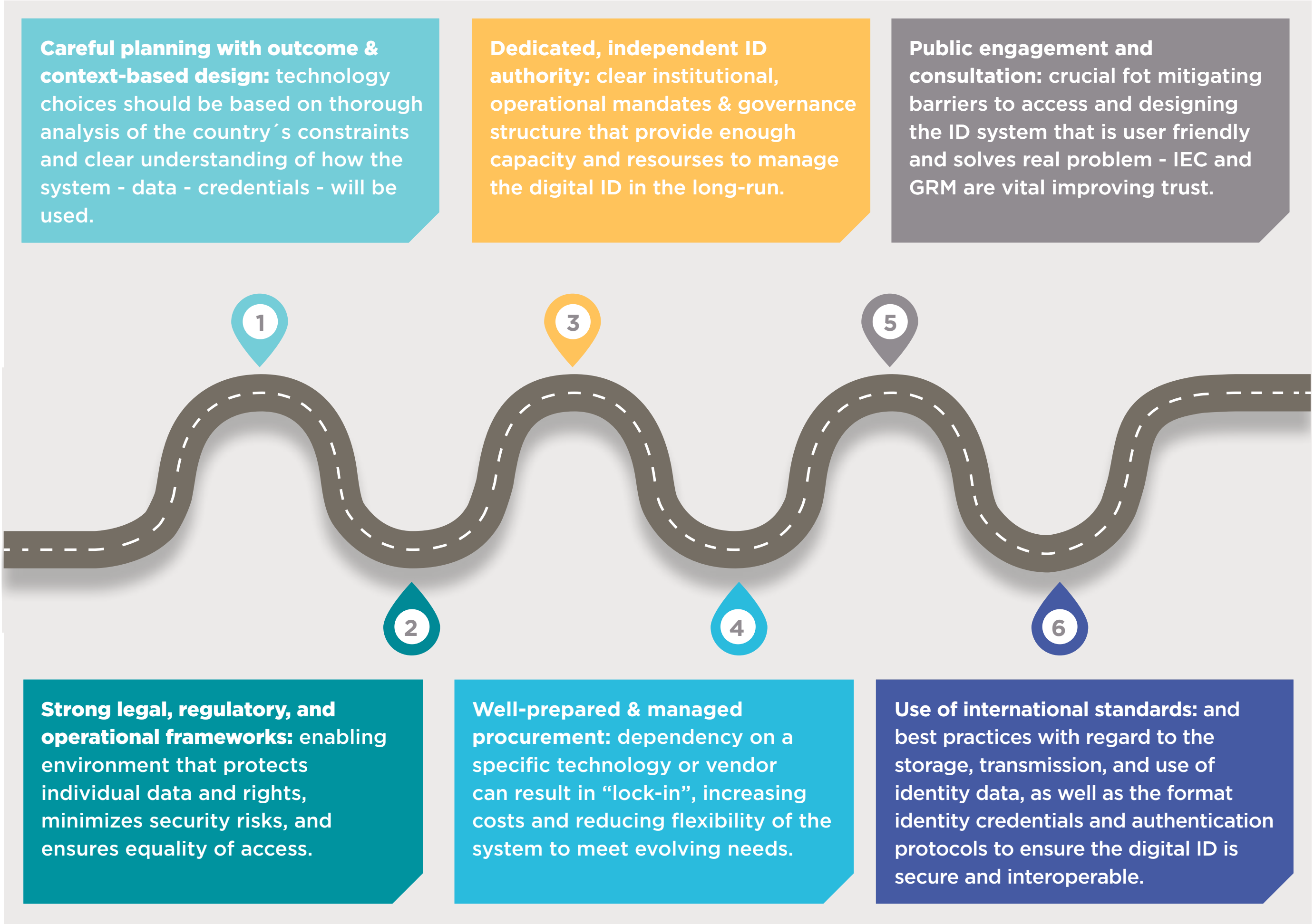
- Based on the above-mentioned review of the specific points of attention, finalize the design of the National ID system inclusive of interoperability platform and integrated identity verification services among public and private stakeholders.

- Develop Enrollment strategy and Identify strategic use cases with bigger impact to support the use and benefits of the National ID.

- Consider an accelerated procurement strategy if the need to support the launch of the National ID program in 2023 is confirmed, with two key components: the development of technical requirements for the RFP and the confirmation of a tentative budget

- Develop a legal framework with the drafting of a National ID bill and associated regulations as well as any update of existing legislation based on gaps identified (Personal Data Protection, Cybercrime, Data Sharing, all legislation related to other sectoral ID management activities as well as CRVS, etc.).

In summary, the following are the logical drivers to draft the planning of the National ID project :



Careful planning with outcome & context-based design: technology choices should be based on thorough analysis of the country´s constraints and clear understanding of how the system - data - credentials - will be used.

Strong legal, regulatory, and operational frameworks: enabling environment that protects individual data and rights, minimizes security risks, and ensures equality of access.

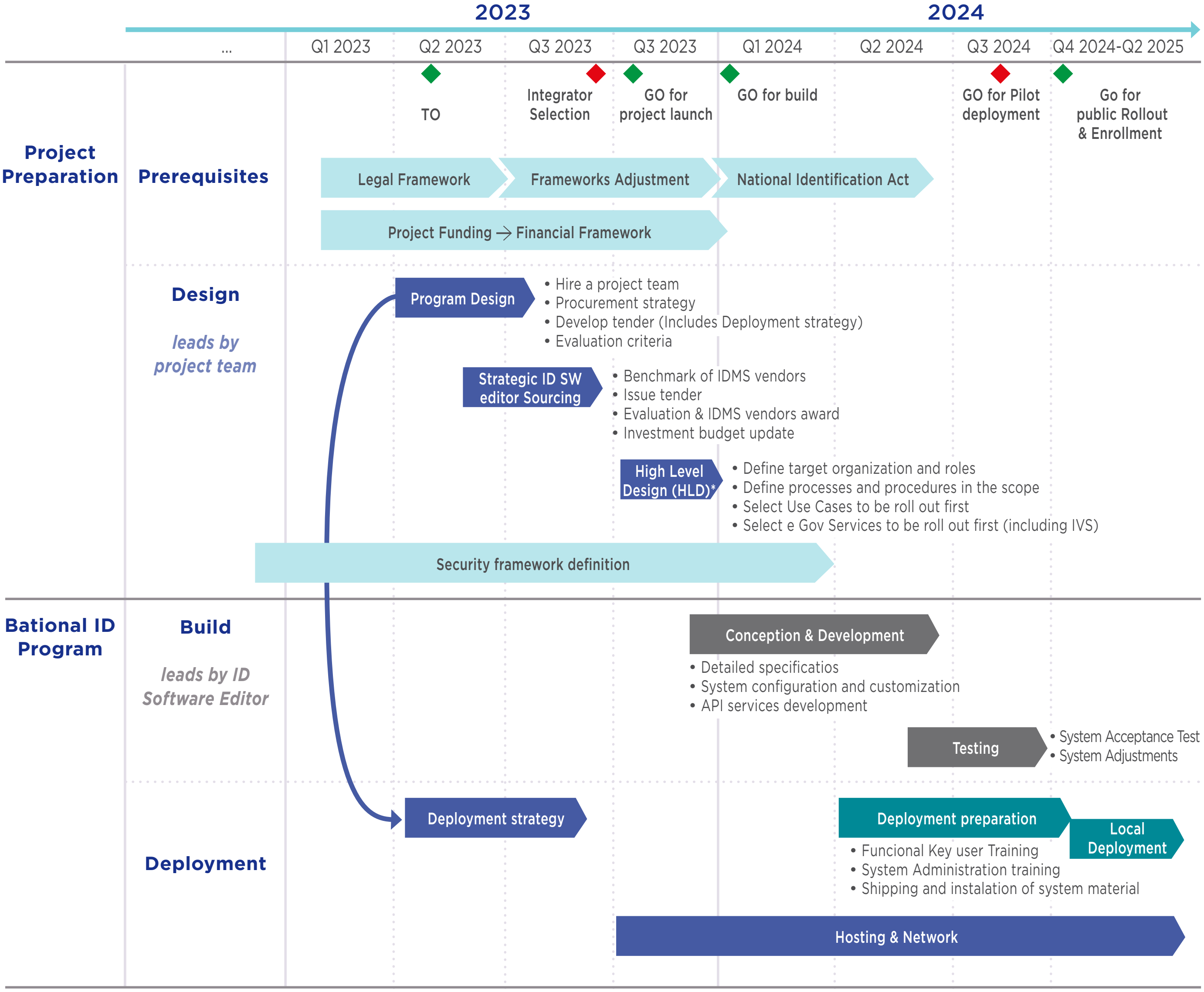
Dedicated, independent ID authority: clear institutional, operational mandates & governance structure that provide enough capacity and resourses to manage the digital ID in the long-run.

Well-prepared & managed procurement: dependency on a specific technology or vendor can result in "lock-in", increasing costs and reducing flexibility of the system to meet evolving needs.

Public engagement and consultation: crucial fot mitigating barriers to access and designing the ID system that is user friendly and solves real problem - IEC and GRM are vital improving trust.

Use of international standards: and best practices with regard to the storage, transmission, and use of identity data, as well as the format identity credentials and authentication protocols to ensure the digital ID is secure and interoperable.

Finally, the following timeline is recommended:


2023
2024
...
Q1 2023
Q2 2023
Q3 2023
Q3 2023
Q1 2024
Q2 2024
Q3 2024
Q4 2024-Q2 2025
TO
Integrator Selection
GO for project launch
GO for build
GO for Pilot deployment
Go for public Rollout & Enrollment
Project Preparation
Prerequisites
Legal Framework
Frameworks Adjustment
National Identification Act
Project Funding → Financial Framework
Design
leads by project team
Program Design
• Hire a project team
• Procurement strategy
• Develop tender (Includes Deployment strategy)
• Evaluation criteria
Strategic ID SW editor Sourcing
• Benchmark of IDMS vendors
• Issue tender
• Evaluation & IDMS vendors award
• Investment budget update
High Level Design (HLD)*
• Define target organization and roles
• Define processes and procedures in the scope
• Select Use Cases to be roll out first
• Select e Gov Services to be roll out first (including IVS)
Security framework definition
Bational ID Program
Build
leads by ID Software Editor
Conception & Development
• Detailed specificatios
• System configuration and customization
• API services development
Testing
• System Acceptance Test
• System Adjustments
Deployment
Deployment strategy
Deployment preparation
• Funcional Key user Training
• System Administration training
• Shipping and instalation of system material
Local Deployment
Hosting & Network