Introduction

Landscape analysis on digitalisation of CRVS systems

Fui Meng Liew, Chief of Digital Centre of Excellence

1 February 2024

Recap: Challenges with digitalisation of CRVS systems

Complicated, cumbersome, & inefficient business processes

Redundancies and complex procedures complicate the registration process, making it time consuming & error prone.

Lack of integration incl. with health and identity systems

Fragmented systems across government agencies lead to challenges in identification and service delivery, duplication of efforts and leave many behind

Vendor lock-in due to over-reliance on proprietary software

Governments might be locked into specific systems and in some cases do not even have unrestricted access to citizen data

Limited resources & capacity in government

Governments often lack the (technical) capacity to implement population-scale integrated digital CRVS systems

CRVS Landscape Analysis:
Overview

Objective and purpose

- Support UNICEF country offices and governments in **identifying CRVS platforms that comply** with minimum functional and non-functional requirements

Expected outcome

- Supports practitioners in **CVRS design and procurement**, and ensures solution selection follows good practices and design principles
- **Focused on solution procurement/selection,** complements other guidance on implementation

Scope

- Focus on solutions that **are available in the market** for deployment (no homegrown/ country solutions)
- **Covering open-source and proprietary solutions**
- **Focused on self-reported information** provided by the vendors and live demos for 11 use cases

unicef
for every child

CRVS platforms
Key Findings for Practitioners

https://unstats.un.org/legal-identity-agenda/documents/Paper/CRVS_Key%20Findings_for_Practitioners.pdf

Six step approach for digital solution analysis
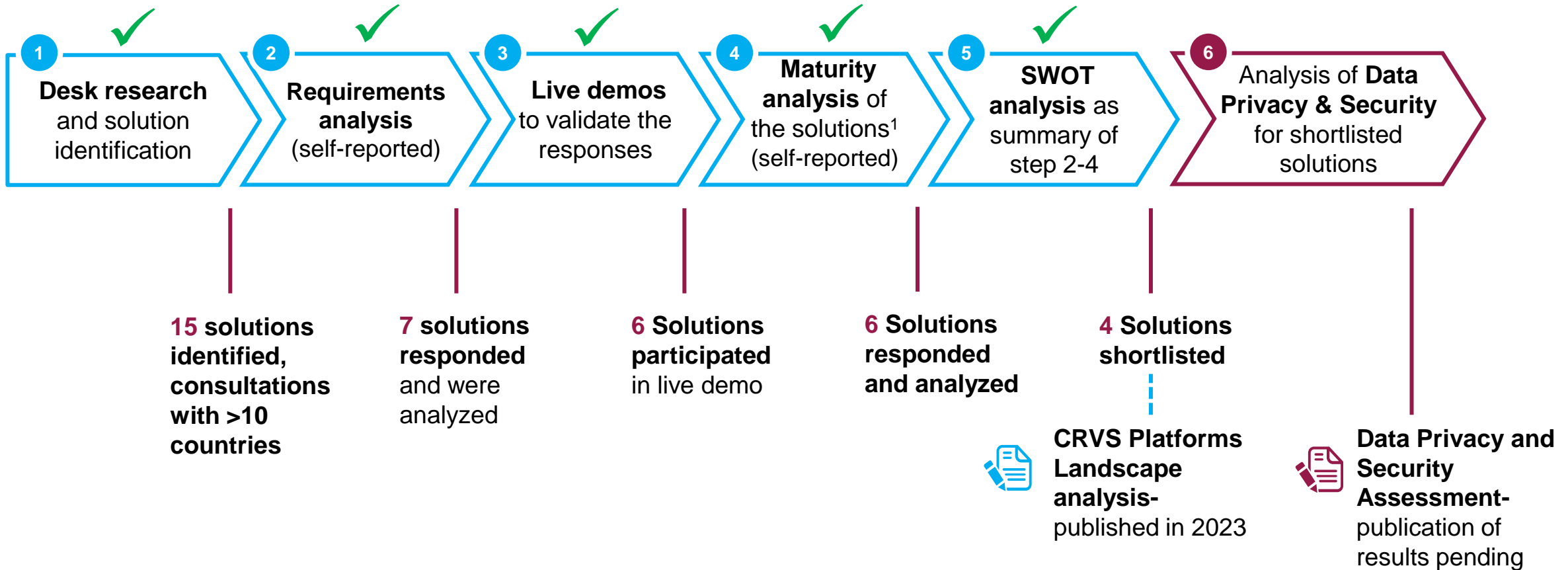
1 ✔ **Desk research** and solution identification

2 ✔ **Requirements analysis** (self-reported)

3 ✔ **Live demos** to validate the responses

4 ✔ **Maturity analysis** of the solutions[1] (self-reported)

5 ✔ **SWOT analysis** as summary of step 2-4

6 Analysis of **Data Privacy & Security** for shortlisted solutions

15 solutions identified, consultations with >10 countries

7 solutions responded and were analyzed

6 Solutions participated in live demo

6 Solutions responded and analyzed

4 Solutions shortlisted

CRVS Platforms Landscape analysis- published in 2023

Data Privacy and Security Assessment- publication of results pending

110 requirements analyzed

Refer to **page 35-40** for the full overview of requirements assessed

Functional requirements		Non-functional requirements (1/2)		Non-functional requirements (2/2)	
Category	**# of requirements**	**Category**	**# of requirements**	**Category**	**# of requirements**
Alerts	2	Interoperability	6	Authentication	1
Client Features	5	Scalability	4	Location	1
Registration	8	Portability	2	Language	1
Amendment	1	Performance	8	Security	14
Validation	5	Availability	2	Backup	1
Messaging	1	Traceability	1	Error-Handling	4
Searchability	2	Usability	4	Learning	1
Data Sharing	1	Flexibility	3		
Certification	3	Archiving	1		
Data	6	Data extraction	1		
Administrative	5	Messaging	1		
System monitoring	4	Data	6		
		Audit	5		

Requirements were assigned weight based on importance (good to have, optional, mandatory).

High-level insights

- **Fragmented market with no clearly recommended solution:** No digital CRVS solution has reached high adoption rates across a range of countries.

- **The Total cost of Ownership (TCO) varied widely**: TCO reported varies between USD 270,000 and USD 61.5mn – variations mostly due to some solution providers not considering all required cost drivers.

- **Online/Offline**: **3 of the 7 shortlisted** systems cannot comply with offline with requirements, significantly limiting their potential application in LMICs (though one is planning offline version until end of 2023)

- **Implementation of interoperability or data standards between digital solutions** and other solutions (health, identity) is inconsistent.

- **Security considerations, such as the encryption and decryption** of outgoing and incoming data, is not consistently implemented across most solutions, and the use of globally recognized benchmarks such as CIS is not applied.

LMIC: Low- and middle-income country   CIS: Center of Internet Security

Limitations

- Assessment as of May 2023, new version of the digital solutions might since have been released

- Results largely based on vendor self-reporting

- Not all available solutions participated in the assessment

- Home-grown solutions not assessed

Next Step

- **Knowledge product strengthening**

  o Functional and Non-functional requirements

- **Translation** to other languages

- **Establish synergy to better share and promote adoption** of the key recommendations and suggestions of the knowledge products

LMIC: Low- and middle-income country   CIS: Center of Internet Security

Fui Meng Liew
Chief, Digital Centre of Excellence
fliew@unicef.org

For every child,
a legal identity.

UNICEF/UN0286458/Sang Mooh