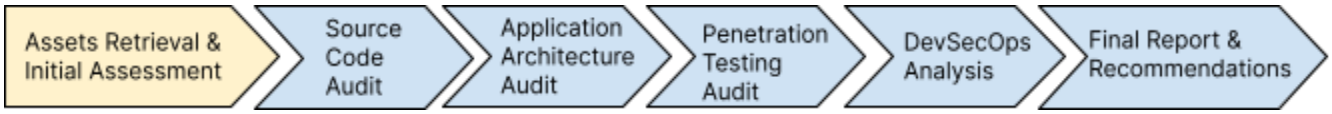
[insert vendor logo]

[vendorname] Evaluation Report

v0.0.X
Date Submitted

The report will be updated, iterated, and versioned as each stage of the evaluation is completed



Performed by Guardian Project
Report Last Updated: Mar 17, 2023
Solution Name and Version: XXXX vX.X.X

Introduction

Executive summary of current evaluation status

Table of Contents

Glossary of Terms

Listing of combined terminology from both general CRVS definition space, along with vendor and audit/evaluation specific terminology

- *Civil registration and vital statistics (CRVS): A well-functioning civil registration and vital statistics (CRVS) system registers all births and deaths, issues birth and death certificates, and compiles and disseminates vital statistics, including cause of death information. It may also record marriages and divorces.*
- *Software Bill of Materials (SBOM): list of all the open source and third-party components present in a codebase. An SBOM also lists the licenses that govern those components, the versions of the components used in the codebase, and their patch status, which allows security teams to quickly identify any associated security or license risks.*

Evaluation Summary

Solution Summary

Brief description of the solution from our evaluation perspective

- [ ] *version number, release history, cycle*
- [ ] *background on how long it has been developed*
- [ ] *other relevant history and details that have been documented, discovered through the evaluation process*

Elements of the Solution

- [ ] *High level summary of features, components, modules, capabilities, user stories and personas, and other*

Threat and Risk Assessment

Current understanding of the environment threats and risks that the evaluation is being considered within, with some examples of threats being considered under this evaluation

Threat	Likelihood	Impact	Severity	Mitigations
Describe the potential threat, attack vector, bad actor	How likely is it that this could happen?	What will happen if the threat/attack is successful?	How severely will the solution instance be impacted?	How can we reduce the risk, impact, and severity of the attack?
Example 1	Likely	Example Impact 1	Minor	Example Mitigation would go here
Example 2	Unlikely	Example Impact 2	Moderate	Example Mitigation would go here

Initial Assessment Results

Status: Not Started

Initial Thoughts

After meeting the team and reviewing the product here's what we think so far (our major takeaways)

- [ ] General impression
- [ ] Summary of interactions with vendor
- [ ] Identification of key vendor team members and roles
- [ ] High-level concerns and blockers

Review of Assets

An analysis of the discovered and received assets from both a quantitative and qualitative perspective

- [ ] *Product and architecture documents, diagrams, specifications*
- [ ] *User stories, personas, threat models, needs assessments, and other user experience and feature design inputs*
- [ ] *Source code for all tiers of the application*
- [ ] *Access to ticketing systems, discussion boards, wikis, and other public development infrastructure*
- [ ] *Inputs to and results from any other security audits*
- [ ] *Prerequisites for installation, use, access*
- [ ] *Operational deployment images, tools, and/or scripts for configuration management*

Questions to investigate further

Any major takeaways that stood out to us so far that we will be focusing on during the audits

- [ ] *Areas where we need more definition or additional inputs*
- [ ] *Consideration of alignment of threat / risk model to solution*

Source Code Security Audit

Status: Not Started

Status

- [ ] *Timeline review and updates*
- [ ] *High-level concerns, issues*
- [ ] *Summary of test environment setup, steps taken to complete analysis*
- [ ] *Summary of communication with vendor related to disclosures and direct feedback*
- [ ] *Status of any mitigations, patches, updated releases*

Outcomes

Outcome of the audit and disclosure of any vulnerabilities, bugs, typos, threats, etc that we've discovered (anything found will be shared with the vendor)

- [ ] *Flaws in the application (bugs, security weaknesses, extensibility,*
- [ ] *Readiness of the source code for being enhanced by a third party*
- [ ] *Open-Source Software (OSS) vulnerability scanning*
- [ ] *Static application security testing (SAST) scanning*
- [ ] *Research and document the complete "Software Bill of Materials" (SBOM)*

Feedback

Open questions or comments for the vendor or UNICEF

[vendorname] Evaluation Report

- [ ] *Specific request for feedback on discovered outcome*
- [ ] *Request for additional details or ideas on future mitigations*
- [ ] *Potential issues to address in future phase of work*

Application Architecture Audit

Status: Not Started

Status

- [ ] *Timeline review and updates*
- [ ] *High-level concerns, issues*
- [ ] *Summary of test environment setup, steps taken to complete analysis*
- [ ] *Summary of communication with vendor related to disclosures and direct feedback*
    - [ ] *Status of any mitigations, patches, updated releases*

Outcomes

Outcome of the audit and disclosure of any vulnerabilities, bugs, typos, threats, etc that we've discovered (anything found will be shared with the vendor)

- [ ] *Document a shared, holistic view of the structure of the application*
- [ ] *Research and document the complete "Software Bill of Materials" (SBOM) regarding components, database, APIs, and third-party libraries*
- [ ] *Ease of user interface for setting roles and status visibility*
- [ ] *Evaluation of maintainability, performance at scale, re-usability, flexibility.*

Feedback

Open questions or comments for the vendor or UNICEF

- [ ] *Request for more clarification regarding architecture, design, API, extensibility goals*
- [ ] *Listing of potential scenarios, configurations, alternative technologies*
- [ ] *Specific request for feedback on discovered outcome*
- [ ] *Potential issues to address in future phase of work*

Penetration Testing Audit

Status: Not Started

[vendorname] Evaluation Report

Status

- [ ] *Timeline review and updates*
- [ ] *Details of process, setup, tools utilized*
- [ ] *High-level concerns, issues*
- [ ] *Summary of test environment setup, steps taken to complete analysis*
- [ ] *Summary of communication with vendor related to disclosures and direct feedback*
- [ ] *Status of any mitigations, patches, updated releases*

Outcomes

- [ ] *Active and passive security scanning of vulnerabilities*
    - [ ] *Dynamic Application Security Testing (DAST)*
- [ ] *Evaluation of the holistic approach in terms of cyber security*
    - [ ] *Security policies analysis*
    - [ ] *Analysis of history of public vulnerabilities*
    - [ ] *CRVS product vendor response/management and communication to users*
    - [ ] *Analysis of the security of data at rest and in motion*
    - [ ] *Analysis of security guidelines/documentation (including resilience and recovery recommendations)*

Feedback

Open questions or comments for the vendor or UNICEF

- [ ] *Specific request for feedback on discovered outcome*
- [ ] *Request for additional details or ideas on future mitigations*
- [ ] *Potential issues to address in future phase of work*

DevSecOps Analysis

Status: Not Started

Status

- [ ] *Timeline review and updates*
- [ ] *Summary of test environment setup, steps taken to complete analysis*

Outcomes

- [ ] *Software development operation best practices*
- [ ] *Review of operations management from a system administrator perspective*
- [ ] *Guidance on production deployment*

[vendorname] Evaluation Report

Feedback

Open questions or comments for the vendor or UNICEF

- [ ] *Specific request for feedback on discovered outcome*
- [ ] *Request for additional details or ideas on future mitigations*
- [ ] *Potential issues to address in future phase of work*

Final Report and Recommendations

Status: Not Started

Overall Findings

Includes summary of work performed, any overall takeaways and a comprehensive statement of our evaluation

Area of Evaluation	**Readiness**	**Impact**	**Comments**
Evaluation Aspect	General readiness / fitness of solution in specific area	Affect that readiness has on viability of solution as part of this evaluation	Any summary thoughts on each area
Source Code Security			
Application Architecture			
Penetration Testing			
DevSecOps			

Actionable Recommendations

Major areas of concern and recommendations to mitigate

Closing

Final thoughts

Appendix

- [ ] *Links to relevant support content, tools, and other resources*