Samoa Finance Sector Resilience and Development Project

Terms of Reference for National Digital Identification System (NDIDS) Implementation Support & Technical Advisory Firm

1. Background

Samoa has a population of just over 200,000 people and covers approximately 3,000 square kilometres of land. This population is spread across four main islands and is organised into more than 330 villages. These villages are clustered in 51 districts, from which a representative is elected every five years to serve in the democratic Government of Samoa ('the Government'). In its conducive efforts to expand opportunities and reduce vulnerabilities for its citizens, the Government passed the National Digital Identification (NDID) Act after challenging years of affirming the Public of the initiative's inclusive gain for all. As of January 2024, national digital identification is mandatory for all citizens and residents of Samoa and is recognised as a legal form of identification.

The Samoa Bureau of Statistics ('the Bureau') of the Government is the primary implementing agency responsible for the National Digital Identification System ('the NDIDS'). The Government of Samoa has received a grant from the World Bank ('the Bank') through the Samoa Finance Sector Resilience and Development Project (SFSRDP 2025-2029) to develop the NDIDS. A dedicated division within the Bureau has been established for this purpose. The division's recruitment of permanent staff continues and is expected to be completed by July 2026. Technical and operational staff are scheduled for recruitment throughout the NDIDS development phases until its services are fully operational for public use.

For the next five years, development proceedings include: full system development; Public and staff awareness and capacity building; one-off mass registration of all eligible persons; and deployment of continuous registration and authentication services. The authentication services anticipate: the transition from physical to digital identity verification and authentication ensuring synchronous use of both; and deployment and integration of e-KYC functionalities to existing processes for public, private and financial services.

The Government approved the Strategic Implementation Plan for the National Digital Identity System for Samoa ('the Strategy'), which outlines the system's scope, key enablers, and the timeline for implementation, before enacting the principal act in January 2024. After analysing the gaps and needs, Samoa's context-specific Technical Requirements for the NDIDS have also been documented. However, restricted resources due to the COVID-19 pandemic consequentially limited progress within the strategised timeframe. This leads to an urgent prerequisite review of the Strategy and Technical Requirements. With the principal NDID Act enacted, the Government continues to strengthen the legal framework by having the Regulations and National Policy and Plan for Implementation drafted and approved by 2026.

2. National Digital Identification System (NDIDS)

The NDIDS is envisioned as a fully digitalized, forward-looking platform that establishes secure digital identities for all citizens and residents of Samoa. Upon enrolment, an individual's digital identity cycle commences with the issuance of a unique Samoa Digital Identification Number (SDIN). The SDIN is a unique ten-digit identifier that facilitates seamless access to digital services throughout an individual's lifecycle until deactivation. This NDIDS system is designed to support both one-off mass registration and continuous updates. The Civil Registration System (CRS) will be upgraded and will become a component of the NDIDS to ensure accurate synchronization of vital events such as birth and death

certification. The NDIDS, including CRS, should be designed to be able to issue standards-compliant verifiable credentials[1].

The NDIDS objectives are:

i) **Deploy an upgraded Civil Registration System (CRS)**, that ensures a coordinated digital process for registering births, deaths, adoption and marriages. This system will effectively collect, store and process statistics information for relevant ministries, authorised organisations and the Public. The upgrade is required, but not limited to:

(a) improve efficiency and quality of registration procedures and reduce risks for identity duplication via web and mobile services for submission of notifications and applications;

(b) provide a communication channel for authorised formal and informal informants; and

(c) secure the same quality and efficient services at all offices regardless of location. These include:

(i) Notification Services – handle notices from authorised informants who have witnessed the appearance of an event to be entered in the CRS and stored until applicants arrive with original documentation and request registration;

(ii) Registration Services – handle the collection of the application dossier to register an event, official data entry and uploading of scanned or photocopied annexes, data verification process, registration approval, process and issuance of the registration certificate; and

(iii) Digitised Information Services – enables easy online secure access to official identity documents to streamline verification when using available digital services, including issuance of CRS documents in verifiable credentials format.

ii) **Introduce the SDIN** assigned to eligible persons. This unique ten-digit is randomly generated with the addition of a checksum as the last 2-digits. This checksum value is a machine-encoded security feature to confirm the SDIN is entered correctly;

iii) **Develop and deploy the Identity Database** that serves as the central point of the NDIDS. In a nutshell, this database:

(a) generates the SDIN, associated security tokens and verifiable credentials;

(b) stores biographical data of registered persons identified with an SDIN, such as names, birth dates, places of birth, sex, home addresses, parent's names (including adoption) and death date;

(c) is fully integrated to the CRS and Biometric database on a system-to-system basis; and

(d) has limited system-to-system communication with the Passports system.

iv) **Develop and deploy the Biometric Database**, which handles the collection, registration and storage of biometric data associated with the SDIN generated by the Identity Database. The solution should be equipped with software, equipment and support services for an Automated Biometric Identification System (ABIS) configured and customised to Samoa's solution requirements for capturing and recognising biometric data to support deduplication and verification functions;

v) **Develop and deploy the Authentication Module** to handle authentication and verification services in accordance to the national policy and plan for implementation, regulations and principal act of the NDIDS.

vi) **Develop and deploy Online services** through web portals and mobile applications to allow government, citizen and third party, secure and controlled access to authentication and services for digital identity credential verification;

[1] Verifiable credentials are digital credentials that are cryptographically secure, privacy-respecting, and machine-verifiable. They enable individuals to present trusted identity information that can be independently verified without contacting the original issuer. Examples of relevant international standards include the W3C Verifiable Credentials Data Model and the ISO/IEC 18013-5 standard for Mobile Driving Licences (mDL).

vii) **Develop an Enrolment, and Printing Module** to handle registration of all eligible persons and printing of quality physical ID cards.

The NDIDS involves developing the following interoperable system: (i) **(upgraded) Civil Registration System (CRS) Database**, (ii) **Identity Database, (**iii**) Biometric Database,** (iv) **Authentication Module** (vi) **Online services,** and (v) **Enrolment and Printing Module**.

The desired NDIDS solution must consider the following design principles: ensure vendor neutrality in design provided; preferred use of open-source technologies to ensure compatibility; ease of integration; interoperability between databases and modules; ongoing sustainability; upgradability and future enhancement options. Open-source platforms are considered frameworks for building and customizing Samoa's solution, however, any better alternatives that enable the above conditions can be considered via a compare and contrast feasibility investigation. The system architecture and design will be developed to encompass the business requirements of the Bureau for the NDIDS, as part of a market approach to select a vendor's design proposal for the solution.

3. Objectives of the Assignment

The objectives of this assignment are to provide the Bureau with the following on-the-ground and day-to-day support to ensure all planned activities will be carried out in the most efficient, timely, cost-effective and well-coordinated manner for:

i) Advisory Services, including system design and architecture;
ii) Procurement Support, including preparation of documentation and contributing to evaluation;
iii) Technical Implementation Support, including vendor oversight and quality assurance;
iv) Contract Management; and
v) Capacity Building.

The Firm is expected to engage face-to-face with the Bureau for most of the contract's duration. The Firm will liaise directly with the Bureau, alongside the Bank's advisor, to ensure alignment with Samoa protocols and international donor standards.

4. Scope of Services

4.1 Advisory Services

4.1.1 Inception

The Firm will review existing project documents and consult adequately to submit an inception report. The report should demonstrate that all services to be provided are adequately resourced and executed. At a minimum, the inception report should include an overview of:

a) needs analysis of technical resources and capacity gaps for successful development and deployment of the NDIDS;
b) assessment of risks and mitigation measures regarding communication channel to the Passports System and roll out of the authentication module;
c) recommendation of international standards for proper implementation of digital and physical identity assurance frameworks, including aspects such as credential issuance and lifecycle management (e.g. use of verifiable credentials), biometrics, data security and protection, digital trust and interoperability frameworks, physical ID card quality, usage and retirement, and considerations for long-term system sustainability and public trust;
d) plan of necessary training and workshops;
e) plan for NDIDS and quality assurance testing outline;
f) engagement plan with key stakeholders on digital ID, biometrics, e-KYC and data exchange requirements, including high-level descriptions of priority use cases;

g) outline of key considerations for long-term sustainability of the NDIDS, including institutional arrangements, budgeting and financial planning, staffing and capacity needs, maintenance and upgrade pathways, and phased transition to local ownership and support;
h) trainings/workshops to be implemented for the Bureau throughout the contract. The Firm is to include a tentative schedule of in-house training/workshops that spreads across the full engagement of contract. A full capacity gaps report is to be prepared in completion of necessary scheduled in-house training/workshops and staff mentorship during working engagements implemented by the end of the contract. The firm may also recommend necessary overseas training or courses to build capacity of staff for continuity of the NDIDS; and
i) detailed work plan (including timelines and outputs), working arrangements (including mechanisms for coordinating with other consultants and cadence for meetings).

4.1.2 Review Technical Requirements and Functional Design for Procurement of NDIDS

There is an urgency to review the technical requirements for NDIDS components and its modules to reflect the Act and working Regulations and Policy. Under the review, updated technical requirements are to be included in an appropriately formatted Terms of Reference (TOR), as part of developing request for tender documents, for the Bureau, to be released to international market for responses, by appropriately qualified vendors in the provision of a Samoa NDIDS and CRS solution. At a minimum, the review, technical specification updates, TOR and any other procurement document, needs to cover:

a) objectives of the NDIDS;
b) high-level scope of work (NDIDS work breakdown structure, exclusions and stakeholder management);
c) functional and non-functional requirements for: (i) CRS (CRS database, Notification portal, data requirements, (ii) Enrolment, Automated Biometric Identification System (ABIS) (Multimodal SDK Component, Manual Adjudication and Manual Verification Module), (iii) Identity Database including SDIN generation and Authentication Module, ID card supply and personalisation modules, (iv) Mobile applications and web portal, (v) centralised and distributed digital ID, including using verifiable credentials (vi) Establishments of ICT infrastructure (equipment requirements for each component, ICT tools for cyber security, network infrastructure, cloud), and (vii) implementation requirements (deployment and roll-out service specifications, recurrent cost items – warranty defect recourse, technical support and capacity related requirements);
d) testing and quality assurance requirements;
e) implementation schedule;
f) technical responsiveness checklist for each component;
g) indicative processes and priority use cases; and
h) recommendations and high-level planning for technical integration with existing and future government systems and services, use of APIs, data exchange protocols, and secure interoperability standards, to enable reusability and scalability of the NDIDS.

In additions, to address any existing gaps, incorporation of measures to address: resilience to external shocks, interoperability of systems and sub systems, total cost of ownership, expansion on mobile and web portal functions, sustainability, onsite-and-cloud-hybrid network, migration to local cloud and change management support, are to be included as part of the drafted technical specification, TOR and RFT produced.

4.1.3 Exit Management

The Firm will develop and submit plans to the Bureau, detailing the provision of contingent support for the NDIDS and recommendations to support long-term operational sustainability and continuity of NDIDS. This Exit Management plan must be provided in writing to the Bureau or its designated agencies within 90 days before the end of the contract.

4.1.4 Final Report

The Firm is to submit a final report detailing progress, results, challenges, lessons learned, future work, recommendations, etc. 30 days before the contract end date.

4.2 Procurement Support

The Firm will serve as an advisor and support the Bureau in the procurement of goods, consulting services, and non-consulting services for the NDIDS. At a minimum, the Firm is to assist in:

a) developing the complete set of documents for procuring the Vendor, software and hardware (Requests for Proposals, Requests for Bids, etc.) and, when necessary, support with obtaining the World Bank's no-objection;
b) writing Scopes of Work, Terms of Reference, and/or Bills of Quantity, General Conditions of Contract, Special Conditions of contract, Instruction to Bidders, as well as evaluation criteria, for the procurement packages related to the NDIDS, and related goods and services, and support obtaining the World Bank's approval;
c) proposing potential goods and services solutions based on the market analysis;
d) evaluating expressions of interest and preparation of shortlist evaluation reports;
e) evaluating bids and proposals, preparation of evaluation reports to support obtaining approval by the Government and the World Bank, as necessary;
f) contract negotiations with the Vendor and other technical consultants, preparation of contract negotiation minutes and negotiated draft contracts initiated by both parties;
g) debriefing of complaints and vendor engagement;
h) preparing contracts for supply of goods and non-consulting services; and
i) optimizing the procurement plan to prioritise activities based on the complexity and nature of goods and services proposed.

The Firm is to submit recommendation reports during the approach to market for vendor's selection to support the final evaluation report. At a minimum, the reports should cover: (i)the firm's recommended and justification of shortlisted bids; (ii)necessary presentations for bidders' information; (iii)annexed responses to raised queries by bidders; (iv)meeting minutes of all bidder engagements; and (v)justification of recommendation, for the selected bidder for vendor.

4.3 Technical Implementation Support

4.3.1 Overseeing Supervisor of the Vendor

The Firm will be a technical resource to support the Bureau in onboarding and supervising the vendor and any supplier involved in the development and maintenance of the NDIDS. This includes but is not limited to, addressing questions about relevant deliverables from the design phase, participating in regular meetings, and advising the Bureau on vendor management to ensure the successful execution of contracts. Not only will the Firm partake during frequent progress meetings with the vendor, but will also assure the Bureau of the successful completion of the vendor's deliverables and validate the quality of all functions of the NDIDS to include in the quality assurance and validation reports.

4.3.2 Quality Assurance and Validation

The Firm is to validate the work of the selected vendor (system integrator). This service is split into (i) a quality assurance and validation report of system development, assuring all planned functions of the NDIDS have been included and developed; and (ii) a quality assurance and validation report of system deployment, assuring the usage of NDIDS services have met the requirements of the Bureau, relying parties and the public based on the national policy and other legal agreements. Full assessment of the NDIDS, including results of essential one-off system (prior and after deployment) tests, is to be detailed in these reports and submitted to the Bureau. At a minimum, the reports will cover:

a) results of system tests for risks, issues, discrepancies and omissions. Includes penetration testing of the vendor's solution;

b) system architecture assessment for scalability limitations, potential failure points, faults under increased loads, etc.;
c) assessment of network limitations, integrating and data compatibility issues, technical mismatches between systems and risk of service disruptions;
d) testing of potential risks of Biometric DB and ABIS for data inconsistencies, system performance, or failures;
e) version control and maintenance standards, to ensure a proper system and process is introduced by the vendor and adopted by the Bureau, and is user-friendly and efficient;
f) ID card printing system, physical card quality and durability;
g) external online access (web/app) portals and administration interface of the system (local and VPN);
h) enrolment kits suitability and durability;
i) scheduled inspections and emergency responses during the system development;
j) assurance assessment of the vendor pre-commissioning tests, security tests, and further operational acceptance test results; and
k) overall evaluation of quality of equipment and output service and validation approval.

All interactions with the vendor must occur alongside the Bureau. The Firm is to provide a plan of scheduled mandatory inspections of the progress of system development, to be discussed with the Bureau before system development.

4.3.3 Security Risk, Data Protection and Impact Assessment

The Firm will develop and implement frequent reporting for security risks, data protection and impact Assessment of the NDIDS to ensure the data collected is generated and used in compliance with the Samoa NDID Act 2024, applicable regulations, and relevant international standards. The production of these report will be continued on by the Bureau throughout the lifespan of the NDIDS. Essential tests to be frequently implemented on the NDIDS to sustain and ensure security and data protection measures are met, must be in detail with guidelines/templates for future implementations. The Firm is to produce the first three reports throughout the contract and train responsible staff to ensure the Bureau can independently take on the production of this report in the future. At a minimum, these reports should include:

a) information technology security protocols framework to safeguard user data, encryption methods, administration and user access control and secure storage;
b) data protection compliance with relevant national acts and international standards and data protection regulations to protect a registered person's sensitive information;
c) robust auditing mechanisms and monitoring procedures to detect and address vulnerabilities, potential data breaches and compliance gaps;
d) biometric technologies standards and their application in the systems;
e) mitigation actions to ensure fairness and trust in biometric data. Ensuring accuracy, false positives/negatives, privacy concerns and potential for discrimination; and
f) guideline/template and frequency for risk and DPIA assessment reports.

The combination of recommended frameworks must best suit systems and use in Samoa. The Firm is to train the Bureau in implementing this Security Risk, Data Protection Impact Assessment and developing the reports at a suggested frequency (no longer than a year).

4.3.4 Oversee Identity Proofing, Adjudication and Authentication Module Implementation

The Firm's role includes assisting the Bureau: (i) in developing procedures, in line with the Act and proposed National Policy, for identity proofing, adjudication, and biometric duplications for NDIDS enrolment and digital authentication services, and when used in support of e-KYC and other use cases; and (ii) oversee development and deployment of authentication portal access to relying parties and Public following proper protocols and procedures set under the National Policy.

4.3.5 Physical Identity Card

The Firm is to submit a recommendation report on details for the NDID physical ID card. The report, at a minimum, is to: (i) sample the design and oversee the development and supply of a secure physical identity card unique to Samoa and incorporate the Bureau themes and adequate security feature principles developed for the artistic layout of the physical card, incorporating associated digital seals; (ii) ensure the incorporation of internationally recognised standards and best practices for security design, security features, card material and construction technics, resistance to alteration, appendage and or substitution, to ensure a durable and wear-resistant physical identity card; and (iii) define and ensure appropriate test standards via a report that the physical identity card meets normal wear and tear for the card's validity period from the vendor.

4.3.6 Online access and Associated Digital Seals

Similar to 4.3.5, the Firm's recommendation report, at a minimum: (i) ensure the incorporation of internationally recognised standards and best practices for usability, security features, resistance to alteration, appendage and or substitution, for online access and issued digital seals; (ii) sample the user experience design output of the authentication portal and mobile app based on the needs stated in the National Policy; and (iii) define appropriate test cases to ensure the digital seal can be used in the authentication process and as part of government services.

4.4 Contract Management

The Advisor Firm is required to support the Bureau with contract management for vendor, licenses and supply of goods and services as well as ensure transfer of ownership to Samoa (source code, software, hardware, etc). The expected level of contract management support may vary throughout the assignment depending on the complexity and involvement of the vendor and other project stakeholders. The support may include, but not limited to:

a) ensure secured performance, advance payment, insurance and effective contract conditions;
b) if necessary, prepare and update contract management form;
c) monitoring contract performance
d) re-assess risk and mitigate in case of inevitable contract modification ensuring minimal disruption to operations
e) review and maintain quality reports and deliverables prepared by the vendor and advise the Bureau to approve;
f) review of technical documentation prepared by suppliers;
g) participate in acceptance and similar testing of the NDIDS by the vendor and advise the Bureau on acceptance for endorsement;
h) advise the Bureau when progressing invoices for payment the vendor and other suppliers;
i) manage warranty claims and arrange Service Level Agreements and/or Post Warranty Services, when necessary;
j) manage end of contacts (and relative assessments)
k) when necessary, train Bureau staff to effectively manage and maintain ongoing contracts and licenses for the operation of NDIDS.

4.5 Capacity Building

4.5.1 Knowledge Transfer

The Firm will transfer knowledge and capabilities to the Bureau for ongoing management, maintenance, and development of the solution based on the technical and other documentation produced during the period of engagement with the Bureau. Mentoring and building capacity of responsible staff of the Bureau is ensured during frequent engagements.

4.5.2 Training and Capacity Building

The Firm will: (i) conduct frequent in-house training workshops to ensure the Bureau can take on responsibly to ensure the continuity of the NDIDS; (ii)submit a report that concludes the

capacity gaps raised initially have been addressed as a result of mentoring and successful implementation of scheduled in-house training and possible recommended overseas training; (iii)participate in technical operational training for the Bureau by the vendor and ensure all necessary areas are covered, (iv) advise and prepare any necessary documentation for the Bureau (e.g. standard operating procedures (SOP), service flow, etc), and (v) assist and participate in training workshops by the Bureau for the Public and relying parties for the use of the NDIDS.

5. Deliverables

Deliverable	Due Date	Weight
1. Inception Report	28days after contract signed date	15%
2. NDIDS Technical Requirements and Function Design Review	30days after 'deliverable 1' approved date	5%
3. Deliver all procurement documents (RFP/RFB) for Procurement of: Design, Supply and Installation of the National Digital Identification System of Samoa and associated upgrade of the Civil Registry System	60days after 'deliverable 1' approved date	5%
4. Strategy Review for Development and Deployment of the NIDIDS	90days after 'deliverable 1' approved date	5%
5. Deliver all Procurement Evaluation Report(s) for the selection of the design, supply and installation for the NDIDS	within 30days after closing date of receiving bids/proposal/EOI documents	10%
6. Quality Assurance and Validation Report for System Development	14days after completion date of Vendor's pre-commission testing of NDIDS	5%
7. Quality Assurance and Validation Report for NDIDS Services Deployment	120days before end of contract date	5%
8. Deliver 3x reports on Security Risk, Data Protection and Impact Assessment	1st – 60days after 'deliverable 4' approved date 2nd – 21days after end date of mass registration 3rd – 90days after start date of continuous registration	12%
9. Delivery of Draft & Final Identity Proofing and Adjudication practice for Authentication	Draft – 120days before mass registration state date Final – 90days before launch of continuous registration	6%
10. Recommendation Report on Physical ID Card security, design, construction and testing results	30days before commence date of system development	5%

11. Recommendation Report for Online Access and Digital Seals	30days before commence date of system development	5%
12. Capacity Gaps Report plus at least 5 internal training/workshops carried out	120days before end of contract date	10%
13. Exit Management Plan	90days before end of contract date	10%
14. Final Report	30days before end of contract	2%

6. Requirements

6.1 Qualification Requirements as a Firm

The selected firm must be a licensed and qualified entity or consortium of firms with demonstrated experience in successfully executing digital identity projects on a national scale. The Firm should have:

a) a minimum of seven (7) years of experience in high-level advisory services to governments on national scale solutions for technical, procurement, resources and capacity issues, preferably projects related to identity information systems, digital authentication functions and similar initiatives;
b) completed at least two (2) contracts similar to managing the implementation of a digital identification system and facilitation of digital transition activities for improvements to national identification systems;
c) experience with complex projects implemented in small island developing states and/or within the Pacific region;
d) a detailed understanding of the process standards, data standards (field length, format, permissible values, code directories, etc) and technical standards (biometrics, IT security, cards and personal identification, verifiable credentials, telecommunications and information exchange between systems) for ID management, IT security frameworks and security compliance management for a robust, interoperable and sustainable national ID system in response to the rapid evolving technology;
e) experience working in a team with a designated Team Leader (TL) who will operate as the main point of contact with the Bureau. The Team Leader, and/or suggested key individuals, may work full-time initially to deliver the first five (5) contract deliverables. This role is preferred for an Enterprise Architecture Specialist with proven project management experience and skills. Alternative suggestions can be considered based on the Firm's performance history of success; and
f) experience in digital strategy, planning and execution in a government setting in at least one country across organizations in government considering architecture, design, and support requirements for delivery.

6.2 Team Composition

The Firm's team is expected to have an appropriate mix of key and non-key specialists to deliver the services specified in the Terms of Reference. Key individuals are as follows:

a) Enterprise Architecture Specialist (preferred Team Leader);
b) ICT Business and Systems Analyst;
c) User Experience and Service Design Specialist;
d) Digital Identification Specialist with Biometric Systems and CRVS knowledge and experience;
e) Cybersecurity Specialist: and

f) Procurement and Contract Management Specialist;

The team leader may advise on other technical expertise or individuals required to be part of the firm's team.

6.3 Qualification Requirements of Key Individuals

6.3.1 General

Key individuals must have:

a) proficiency in oral and written English;
b) strong diplomatic negotiation and meeting facilitation skills including reporting and presentation experience;
c) strong team collaboration, training and public speaking skills;
d) strong problem evaluating, analysis and adaptable solution skills;
e) practical experience in translating strategic and business requirements into successful procurements and developing successful operational roadmaps; and
f) practical experience in adaptations of international legal and ethical aspects related to information technology and rights to personal information.

6.3.2 Key Individuals

The list of Key Individuals whose CVs and experience to be evaluated include the following:

No. Staff	Key Position	Area of specific expertise required	Minimum qualification and professional experience required
	Enterprise Architecture Specialist - Team Leader;	a. A highly skilled technical leader with expertise in designing, developing, and securing civil registry, digital ID, and eKYC-linked systems. Proficient in architecting robust solutions that integrate multi-factor authentication (MFA) and biometric verification for identity assurance. b. Adept at drafting technical and functional requirements, including Terms of Reference (TOR), and leading penetration testing strategies to enhance system security. Experienced in guiding cross-functional teams, ensuring interoperability, scalability, and compliance with international standards for identity management and data protection. c. knowledgeable in API security, including threat protection, rate limiting, and encryption, ensuring seamless integration between identity systems and third-party services d. Expertise in RESTful APIs, GraphQL, SOAP, WebSockets, and API gateways	a. Master's degree in Computer Science, Software Engineering, Information Systems, or a related field. b. Certifications in enterprise architecture (e.g., TOGAF), cybersecurity (e.g., CISSP, CISM), or cloud computing (e.g., AWS, Azure, etc), project management (PMI, PRINCE2, PMBOK, AGILE), are an advantage. a. At least 10 years of experience in IT architecture, software development, or systems integration. With a focus on digital ID, civil registration, and or eKYC solutions preferred. b. Proven expertise in designing and implementing secure, scalable identity management systems, including multi-factor authentication (MFA) and biometric registration and verification functions. c. Experience in developing technical standards, system architecture, and Terms of Reference (TOR) for large-scale government or private sector identity projects.

No. Staff	Key Position	Area of specific expertise required	Minimum qualification and professional experience required
		e. Strong knowledge of API authentication and security (E.G., OAuth2, OpenID Connect, JWT, MTLS, rate limiting, WAF).	d. Proficient in API lifecycle management, authentication protocols (OAuth2, OpenID Connect, JWT, etc), and microservices architecture. e. Strong background in penetration testing, security assessments, and demonstrated compliance with implementing international standards, and best practices (e.g., ISO 27001, NIST, GDPR, ID4D principles) in Digital Identity systems. f. Leadership experience in managing cross-functional teams, with a minimum of 2 successfully delivered projects they have led. Demonstrated coordinating role with government agencies, private sector and public, ensuring interoperability between digital identity ecosystems for authentication and verification.
	ICT Business and Systems Analyst	a. A seasoned ICT Business and Systems Analyst specialising in national digital ID and civil registration systems. b. Expertise in analysing, designing, and optimizing identity management solutions, ensuring seamless integration with civil registry platforms. c. Skilled in defining business and functional requirements, developing Terms of Reference (TOR), and mapping workflows for digital ID, eKYC, and identity authentication and verification processes. d. Adept at translating policy and operational needs into scalable, secure, and user-centric digital identity solutions.	a. Bachelor's or Master's degree in Information Systems, Business Administration, Computer Science, or a related field b. Certifications in business analysis (e.g., CBAP, PMI-PBA) or digital identity using opensource solution are an advantage. c. At least 5 years of experience in business and systems analysis, with a focus on digital ID and civil registration solutions. d. Strong expertise in requirements gathering, process mapping, and workflow optimization for identity management and eKYC systems. e. Experience in developing business and functional specifications, Terms of Reference (TOR), and feasibility studies for digital identity projects. f. Experienced in stakeholder engagement, interoperability assessments, and compliance with legal and regulatory frameworks.

No. Staff	Key Position	Area of specific expertise required	Minimum qualification and professional experience required
			g. Familiarity with identity verification frameworks, data protection regulations, and interoperability standards
	Cybersecurity Specialist	a. A highly skilled cybersecurity professional specializing in analysing threats and securing ICT system solutions. This includes risks for digital ID, Civil registration, personal identifiable information, data protection and eKYC systems. b. Expertise in risk assessment, penetration testing, and security architecture to protect sensitive person identifiable information (identity data) and ensure system resilience against cyber threats. c. Proficient in designing and implementing multi-factor authentication (MFA), biometric security, encryption, and access control solutions. d. Strong knowledge of international cybersecurity standards, best practices (ISO 27001, NIST, GDPR) and regulatory compliance for identity management systems.	a. Bachelor's or Master's degree in Cybersecurity, Computer Science, Information Security, or a related field, or combination of extensive industry experience and certification in recognised cyber security programs. b. Industry-recognized certifications such as CISSP, CISM, CEH, OSCP, ISO 27001 Lead Implementer/Auditor, or equivalent are highly desirable c. At least 7 years of experience in IT security, cybersecurity risk management, or security architecture, preferably within civil registration, digital ID, or eKYC ecosystems. d. Expertise in security assessments, penetration testing, and vulnerability management to ensure the integrity and confidentiality of digital identity systems. e. Experienced in developing security policies, incident response plans, and threat mitigation strategies, ensuring the integrity and confidentiality of digital identity ecosystems. f. Experience in application of international cybersecurity frameworks and best practices, including ISO 27001, NIST, GDPR, ID4D, W3C verifiable credentials and OWASP. g. Ability to work with cross-functional teams, provide advice to government agencies, and technology providers to ensure security-by-design principles are used in system development

No. Staff	Key Position	Area of specific expertise required	Minimum qualification and professional experience required
	User Experience and Service Design Specialist	a. Expertise in Human human-centred design, service design for Digital Public Infrastructure (DPI), and user research to enhance front-end and back-end user experience for National Digital ID and CRVS System. b. Skilled in prototyping, accessibility compliance (WCAG), usability testing, and stakeholder engagement, to ensure inclusive and user-friendly service delivery across web, mobile, and assisted digital platforms.	a. A Bachelor's or Master's degree in Human-Computer Interaction (HCI), UX/UI Design, Service Design, Digital Transformation, Computer Science, Software Engineering, Information Systems, or a related field or combination of extensive experience of over 10 years in this field. b. Certifications or formal training in User Experience (UX) Design, Service Design, or Human-Centred Design c. At least 7 years of experience in UX/UI design, service design, or digital transformation projects, with a focus on government or large-scale public sector initiatives. d. Experience in leading user research and usability testing in digital ID, CRVS, or e-Government services. e. Experience working with developers, product owners, and system architects to ensure UX/UI best practices are implemented in the final system. f. Strong ability to analyse user feedback and performance metrics to drive continuous improvement in digital services. g. Knowledge of Digital ID and CRVS standards, such as those from ISO, ICAO, W3C, UNICEF, or the World Bank ID4D framework.
	Procurement and Contract Management Specialist	a. Solid experience in evaluating the bids/procurement by using the rated criteria, contract drafting, negotiation, and legal compliance b. Expertise in drafting and managing procurement processes for large-scale projects. E.G., civil, public, or nationally implemented ICT projects. c. In-depth knowledge of early market engagement and market	a. A Masters or Post-graduate degree in a relevant discipline (e.g., engineering, procurement, law, finance, business administration) or other relevant tertiary qualification(s). b. Minimum 10 years of relevant experience practical procurement activities following the World Bank, ADB or other similar institution procurement regulations or procedures

No. Staff	Key Position	Area of specific expertise required	Minimum qualification and professional experience required
		approach to identify the best procurement method. d. Expertise in regulatory compliance, risk assessment, and contract execution. e. Proven track record in managing service-level agreements (SLAs) and key performance indicators (KPIs).	c. Minimum 5 years recent experience of procuring IT systems, Digital system, contract management and implementation by using the World Bank or similar institution standard procurement documents and solid experience of international procurement practices d. Professional certifications (e.g., CIPS, CPPP, PMP) are preferred
	Digital Identification Specialists with Biometrics and CRVS knowledge and experience)	a. A highly skilled Digital ID Specialist with expertise in biometric identification technologies and secure identity management systems. b. Adept at designing, implementing, and optimizing solutions for national identity programs, civil registration systems, and digital transformation initiatives. c. expertise in design, implementation and ongoing operation of biometric systems and integrating biometric modalities with digital identity systems and eKYC platforms. d. Familiarity with international best practices in civil registration, as well as data protection, privacy and interoperability standards.	a. Bachelor's degree in Computer Science, Information Technology, Software Engineering, or equivalent. With relevant technical field experience of over 7 years, combined with extensive implementation and management of foundational or government national identity systems, that utilise biometric collection, storage, recognition and adjudication functions. b. Professional experience with relevant international standards and best practices for digital id and biometric solutions utilising, at a minimum, ISO-IEC 19794, ISO 39794 part 4 and part 5, ISO-IEC 24745, for biometric systems; ISO-IEC 29115 Security Techniques – Entity authentication and assurance framework. c. Knowledge and experience in the application of verifiable credentials utilising, ISO, W3C or distributed digital ID schemas is highly desirable.

7. Reporting and Supervision

The Advisor Firm will report to the Assistant Chief Executive Officer (ACEO) for the National ID Division of the Bureau. The ACEO, the responsible division and the World Bank advisor will provide guidance, oversight, and direction throughout the contract.

8. Duration and Location

The contract is expected to commence on 1st Sept 2025 and conclude by 1st Mar 2029 with a total expected duration of three and a half (3.5) years. The Advisor Firm will be based mainly in the Office of Samoa Bureau of Statistics, at the National ID Division, in the central town of the capital of Samoa

with the possibility of remote work, as agreed in the Firm's workplan and mutually accepted by the Bureau in the inception report.

9. Institutional and Organisational Arrangements

The Bureau will provide the necessary resources and access to relevant information to facilitate the consultancy.