Request for Proposals
Information Systems

Design, Supply and Installation

(Without Prequalification)

Procurement of:

Supply and Installation of the National Digital Identification System (NDIDS)

Purchaser: Government of Samoa, acting through the Samoa Bureau of Statistics (SBS)

Project: *Samoa Finance Sector Resilience and Development Project, World Bank Project P181456*

Contract title: *Supply and Installation of the National Digital Identification System (NDIDS)*

Country: *Samoa*

Loan No. /Credit No. / Grant No.: *Credit No. IDA-E3780*

RFP No: *WS-SBS-570867-NC-RFP*

Issued on: 23 October 2026

Table of Contents

Section I - Instructions to Proposers (ITP) **3**
Section II - Proposal Data Sheet (PDS) **41**
Section III - Evaluation and Qualification Criteria (Without Prequalification) **53**
Section IV - Proposal Forms **76**
Section V - Eligible Countries **149**
Section VI - Fraud and Corruption **150**
Section VII - Requirements of the Information System **153**
Section VIII - General Conditions of Contract **294**
Section IX - Special Conditions of Contract **375**
Section X - Contract Forms **394**

PART 1 – REQUEST FOR PROPOSALS PROCEDURES

SECTION I - INSTRUCTIONS TO PROPOSERS (ITP)

Contents

A. General....5

1. Scope of Proposal....5
2. Source of Funds....6
3. Fraud and Corruption....6
4. Eligible Proposers....6
5. Eligible Goods and Services....9

B. Contents of the Request for Proposals Document....10

6. Sections of the Request for Proposals Document....10
7. Clarification of Request for Proposals Document, Site Visit, Pre-Proposal Meeting....11
8. Amendment of Request for Proposals Document....12

C. Preparation of Proposals....12

9. Cost of Proposals....12
10. Language of Proposal....12
11. Documents Comprising the Proposal....12
12. Letters of Proposal and Price Schedules....14
13. Alternative Proposals....15
14. Documents Establishing the Eligibility of the Information System....15
15. Documents Establishing the Eligibility and Qualifications of the Proposer....15
16. Documents Establishing Conformity of the Information System....16
17. Proposal Prices....17
18. Currencies of Proposal and Payment....20
19. Period of Validity of Proposals....20
20. Proposal Security....20
21. Format and Signing of Proposal....22

D. Submission of Proposals....23

22. Submission, Sealing and Marking of Proposals....23
23. Deadline for Submission of Proposals....24
24. Late Proposals....24
25. Withdrawal, Substitution, and Modification of Proposals....24

E. Public Opening of Technical Parts of Proposals....25

26. Public Opening of Technical Parts of Proposals....25

F. Evaluation of Proposals- General Provisions....26

27. Confidentiality....26
28. Clarification of Proposals....27
29. Deviations, Reservations, and Omissions....27

G. Evaluation of Technical Part of Proposals....28

30. Determination of Responsiveness....28
31. Eligibility and Qualifications of the Proposer....28

32. …Detailed Evaluation of Technical Part 29

H. Notification of Evaluation of Technical Parts and Public Opening of Financial Parts 29

33. …Notification of Evaluation of Technical Parts and Public Opening of Financial Parts 29

I. Evaluation of Financial Part of Proposals 32

34. …Adjustments for Non-material Noconformities 32
35. …Correction of Arithmetic Errors 32
36. …Evaluation of Proposals Financial Part 32
37. …Abnormally Low Proposals 33
38. …Unbalanced or Front Loaded Proposals 34

J. Evaluation of Combined Technical and Financial Parts, Most Advantageous Proposal And Notification of Intention To Award 34

39. …Evaluation of combined Technical and Financial Parts, Most Advantageous Proposal 34
40. …Purchaser's Right to Accept Any Proposal, and to Reject Any or All Proposals.....36
41. …Standstill Period 36
42. …Notification of Intention to Award 36

K. Award of Contract 36

43. …Award Criteria 36
44. …Purchaser's Right to Vary Quantities at Time of Award 37
45. …Notification of Award 37
46. …Debriefing by the Purchaser 37
47. …Signing of Contract 38
48. …Performance Security 39
49. …Adjudicator 39
50. …Procurement Related Complaint 40

Section I - Instructions to Proposers

A. GENERAL

1. Scope of Proposal

1.1. The Purchaser, as indicated in the PDS, or its duly authorized Purchasing Agent if so specified in the PDS (interchangeably referred to as "the Purchaser" issues this request for proposals document for the supply and installation of the Information System as specified in Section VII, Purchaser's Requirements. The name, identification and number of lots (contracts) of this RFP are specified in the PDS.

1.2. Unless otherwise stated, throughout this request for proposals document definitions and interpretations shall be as prescribed in the Section VIII, General Conditions of Contract.

Throughout this request for proposals document:

(a) the term "in writing" means communicated in written form (e.g. by mail, e-mail, fax, including if specified in the PDS, distributed or received through the electronic-procurement system used by the Purchaser) with proof of receipt;

(b) if the context so requires, "singular" means "plural" and vice versa; and

(c) "Day" means calendar day, unless otherwise specified as "Business Day". A Business Day is any day that is an official working day of the Borrower. It excludes the Borrower's official public holidays.

(d) "ES" means environmental and social (including Sexual Exploitation and Abuse (SEA), and Sexual Harassment (SH));

(e) "Sexual Exploitation and Abuse" "(SEA)" means the following:

Sexual Exploitation is defined as any actual or attempted abuse of position of vulnerability, differential power or trust, for sexual purposes, including, but not limited to, profiting monetarily, socially or politically from the sexual exploitation of another;

Sexual Abuse is defined as the actual or threatened physical intrusion of a sexual nature, whether by force or under unequal or coercive conditions.

(f) "Sexual Harassment" "(SH)" is defined as unwelcome sexual advances, requests for sexual favors, and other verbal or physical conduct of a sexual nature by the Supplier's Personnel with other Supplier's Personnel or Purchaser's Personnel.

(g) "Supplier's Personnel" is as defined in GCC Clause 1.1; and

(h) "Purchaser's Personnel" is as defined in GCC Clause 1.1.

A non-exhaustive list of (i) behaviors which constitute SEA and (ii) behaviors which constitute SH is attached to the Code of Conduct form in Section IV

2. Source of Funds

2.1. The Borrower or Recipient (hereinafter called "Borrower") indicated in the PDS has applied for or received financing (hereinafter called "funds") from the International Bank for Reconstruction and Development or the International Development Association (hereinafter called "the Bank") in an amount specified in the PDS toward the project named in the PDS. The Borrower intends to apply a portion of the funds to eligible payments under the contract(s) for which this request for proposals document is issued.

2.2. Payments by the Bank will be made only at the request of the Borrower and upon approval by the Bank in accordance with the terms and conditions of the Loan (or other financing) Agreement between the Borrower and the Bank (hereinafter called the Loan Agreement), and will be subject in all respects to the terms and conditions of that Loan (or other financing) Agreement. The Loan (or other financing) Agreement prohibits a withdrawal from the loan account for the purpose of any payment to persons or entities, or for any import of equipment, materials or any other goods, if such payment or import is prohibited by a decision of the United Nations Security Council taken under Chapter VII of the Charter of the United Nations. No party other than the Borrower shall derive any rights from the Loan (or other financing) Agreement or have any claim to the funds.

3. Fraud and Corruption

3.1. The Bank requires compliance with the Bank's Anti-Corruption Guidelines and its prevailing sanctions policies and procedures as set forth in the WBG's Sanctions Framework, as set forth in Section VI.

3.2. In further pursuance of this policy, Proposers shall permit and shall cause their agents (where declared or not), subcontractors, subconsultants, service providers, suppliers, and personnel, to permit the Bank to inspect all accounts, records and other documents relating to any initial selection process, prequalification process, bid submission, proposal submission and contract performance (in the case of award), and to have them audited by auditors appointed by the Bank.

4. Eligible Proposers

4.1. A Proposer may be a firm that is a private entity, a state-owned enterprise or institution subject to ITP 4.6, or any combination of such entities in the form of a joint venture (JV) under an existing agreement or with the intent to enter into such an

agreement supported by a letter of intent. In the case of a joint venture, all members shall be jointly and severally liable for the execution of the Contract in accordance with the Contract terms. The JV shall nominate a Representative who shall have the authority to conduct all business for and on behalf of any and all the members of the JV during the procurement process and, in the event the JV is awarded the Contract, during contract execution. Unless specified in the PDS, there is no limit on the number of members in a JV.

4.2. A Proposer shall not have a conflict of interest. Any Proposer found to have a conflict of interest shall be disqualified. A Proposer may be considered to have a conflict of interest for the purpose of this procurement process, if the Proposer:

(a) directly or indirectly controls, is controlled by or is under common control with another Proposer; or

(b) receives or has received any direct or indirect subsidy from another Proposer; or

(c) has the same legal representative as another Proposer; or

(d) has a relationship with another Proposer, directly or through common third parties, that puts it in a position to influence the Proposal of another Proposer, or influence the decisions of the Purchaser regarding this procurement process; or

(e) any of its affiliates participates as a consultant in the preparation of the design or technical specifications of the Information System that are the subject of the Proposal; or

(f) or any of its affiliates has been hired (or is proposed to be hired) by the Purchaser or Borrower as Project Manager for the Contract implementation; or

(g) would be providing goods, works, or non-consulting services resulting from or directly related to consulting services for the preparation or implementation of the project specified in the PDS ITP 2.1 that it provided or were provided by any affiliate that directly or indirectly controls, is controlled by, or is under common control with that firm; or

(h) has a close business or family relationship with a professional staff of the Borrower (or of the project implementing agency, or of a recipient of a part of the loan) who: (i) are directly or indirectly involved in the preparation of the request for proposals document or specifications of the Contract, and/or the Proposal evaluation process of such Contract; or (ii) would be

involved in the implementation or supervision of such Contract unless the conflict stemming from such relationship has been resolved in a manner acceptable to the Bank throughout the procurement process and execution of the Contract.

4.3. A firm that is a Proposer (either individually or as a JV member) shall not participate as a Proposer or as JV member in more than one Proposal except for permitted alternative Proposals. Such participation shall result in the disqualification of all Proposals in which the firm is involved. However, this does not limit the participation of a Proposer as subcontractor in another Proposal or of a firm as a subcontractor in more than one Proposal.

4.4. A Proposer may have the nationality of any country, subject to the restrictions pursuant to ITP 4.8. A Proposer shall be deemed to have the nationality of a country if the Proposer is constituted, incorporated or registered in and operates in conformity with the provisions of the laws of that country, as evidenced by its articles of incorporation (or equivalent documents of constitution or association) and its registration documents, as the case may be. This criterion also shall apply to the determination of the nationality of proposed sub-contractors or sub-consultants for any part of the Contract including related Services.

4.5. A Proposer that has been sanctioned by the Bank, pursuant to the Bank's Anti-Corruption Guidelines, and in accordance with its prevailing sanctions policies and procedures as set forth in the WBG's Sanctions Framework as described in Section VI paragraph 2.2 d., shall be ineligible to be initially selected for, prequalified for, bid for, propose for, or be awarded a Bank-financed contract or benefit from a Bank-financed contract, financially or otherwise, during such period of time as the Bank shall have determined. The list of debarred firms and individuals is available at the electronic address specified in the PDS.

4.6. Proposers that are state-owned enterprises or institutions in the Purchaser's Country may be eligible to compete and be awarded a Contract(s) only if they can establish, in a manner acceptable to the Bank, that they (i) are legally and financially autonomous (ii) operate under commercial law, and (iii) are not under supervision of the Purchaser.

4.7. A Proposer shall not be under suspension from bidding or submitting proposals by the Purchaser as the result of the operation of a Bid–Securing Declaration or Proposal-Securing Declaration.

4.8. Firms and individuals may be ineligible if so indicated in Section V and (a) as a matter of law or official regulations, the Borrower's country prohibits commercial relations with that country, provided that the Bank is satisfied that such exclusion does not preclude effective competition for the supply of goods or the contracting of works or services required; or (b) by an act of compliance with a decision of the United Nations Security Council taken under Chapter VII of the Charter of the United Nations, the Borrower's country prohibits any import of goods or contracting of works or services from that country, or any payments to any country, person, or entity in that country.

4.9. This request for proposal process is open for all eligible Proposers, unless otherwise specified in ITP 15.2.

4.10. A Proposer shall provide such documentary evidence of eligibility satisfactory to the Purchaser, as the Purchaser shall reasonably request.

4.11. A firm that is under a sanction of debarment by the Borrower from being awarded a contract is eligible to participate in this procurement, unless the Bank, at the Borrower's request, is satisfied that the debarment; (a) relates to fraud or corruption, and (b) followed a judicial or administrative proceeding that afforded the firm adequate due process.

5. Eligible Goods and Services

5.1. The Information Systems to be supplied under the Contract and financed by the Bank may have their origin in any country in accordance with Section V, Eligible Countries.

5.2. For the purposes of this request for proposals document, the term "Information System" means all:

(a) the required information technologies, including all information processing and communications-related hardware, software, supplies, and consumable items that the Supplier is required to design, supply and install under the Contract, plus all associated documentation, and all other materials and goods to be designed, supplied, installed, integrated, and made operational; and

(b) the related software development, transportation, insurance, installation, customization, integration, commissioning, training, technical support, maintenance, repair, and other services necessary for proper operation of the Information System to be provided by the selected Proposer and as specified in the Contract.

5.3. For purposes of ITP 5.1 above, "origin" means the place where the goods and services making the Information System are produced in or supplied from. An Information System is deemed to be produced in a certain country when, in the territory of that country, through software development, manufacturing, or substantial and major assembly or integration of components, a commercially recognized product results that is substantially different in basic characteristics or in purpose or utility from its components.

B. CONTENTS OF THE REQUEST FOR PROPOSALS DOCUMENT

6. Sections of the Request for Proposals Document

6.1. The request for proposals document consists of Parts 1, 2, and 3, which include all the sections indicated below, and should be read in conjunction with any Addenda issued in accordance with ITP 8:

PART 1 - Request for Proposals Procedures

Section I - Instructions to Proposers (ITP)

Section II - Proposal Data Sheet (PDS)

Section III - Evaluation and Qualification Criteria

Section IV - Proposal Forms

Section V - Eligible Countries

Section VI - Fraud and Corruption

PART 2 - Purchaser's Requirements

Section VII - Requirements of the IS, including:

- Technical Requirements
- Implementation Schedule
- System Inventory Tables
- Background and Informational Materials

PART 3 - Contract

Section VIII - General Conditions of Contract

Section IX -Special Conditions of Contract

Section X - Contract Forms

6.2. The Specific Procurement Notice – Request for Proposals (RFP) issued by the Purchaser is not part of this request for proposals document.

6.3. Unless obtained directly from the Purchaser, the Purchaser is not responsible for the completeness of the document, responses to requests for clarification, the Minutes of the pre-Proposal meeting

(if any), or Addenda to the request for proposals document in accordance with ITP 8. In case of any contradiction, documents obtained directly from the Purchaser shall prevail.

6.4. The Proposer is expected to examine all instructions, forms, terms, and specifications in the request for proposals document and to furnish with its Proposal all information or documentation as is required by the request for proposals document.

7. Clarification of Request for Proposals Document, Site Visit, Pre-Proposal Meeting

7.1. A Proposer requiring any clarification of the request for proposals document shall contact the Purchaser in writing at the Purchaser's address specified in the PDS or raise its enquiries during the pre-Proposal meeting if provided for in accordance with ITP 7.4. The Purchaser will respond in writing to any request for clarification, provided that such request is received prior to the deadline for submission of Proposals within a period specified in the PDS. The Purchaser shall forward copies of its response to all Proposers who have acquired the request for proposals document in accordance with ITP 6.3, including a description of the inquiry but without identifying its source. If so specified in the PDS, the Purchaser shall also promptly publish its response at the web page identified in the PDS. Should the Purchaser deem it necessary to amend the request for proposals document as a result of a request for clarification, it shall do so following the procedure under ITP 8 and ITP 23.2.

7.2. The Proposer may wish to visit and examine the site where the Information System is to be installed and its surroundings and obtain for itself on its own responsibility all information that may be necessary for preparing the Proposal and entering into a contract. The costs of visiting the site shall be at the Proposer's own expense.

7.3. The Proposer and any of its personnel or agents will be granted permission by the Purchaser to enter upon its premises and lands for the purpose of such visit, but only upon the express condition that the Proposer, its personnel, and agents will release and indemnify the Purchaser and its personnel and agents from and against all liability in respect thereof, and will be responsible for death or personal injury, loss of or damage to property, and any other loss, damage, costs, and expenses incurred as a result of the inspection.

7.4. The Proposer's designated representative is invited to attend a pre-Proposal meeting and/or a site visit, if provided for in the PDS. The purpose of the meeting will be to clarify issues and to answer questions on any matter that may be raised at that stage.

7.5. The Proposer is requested, as far as possible, to submit any questions in writing, to reach the Purchaser not later than one week before the meeting.

7.6. Minutes of the pre-Proposal meeting, including the text of the questions raised without identifying the source, and the responses given, together with any responses prepared after the meeting, will be transmitted promptly to all Proposers who have acquired the request for proposals document in accordance with ITP 6.3. Any modification to the request for proposals document that may become necessary as a result of the pre-Proposal meeting shall be made by the Purchaser exclusively through the issue of an Addendum pursuant to ITP 8 and not through the minutes of the pre-Proposal meeting.

7.7. Nonattendance at the pre-Proposal meeting will not be a cause for disqualification of a Proposer.

8. Amendment of Request for Proposals Document

8.1. At any time prior to the deadline for submission of Proposals, the Purchaser may amend the request for proposals document by issuing addenda.

8.2. Any addendum issued shall be part of the request for proposals document and shall be communicated in writing to all who have obtained the request for proposals document from the Purchaser in accordance with ITP 6.3. The Purchaser shall also promptly publish the addendum on the Purchaser's web page in accordance with ITP 7.1.

8.3. To give prospective Proposers reasonable time in which to take an addendum into account in preparing their Proposals, the Purchaser may, at its discretion, extend the deadline for the submission of Proposals, pursuant to ITP 23.2.

C. PREPARATION OF PROPOSALS

9. Cost of Proposals

9.1. The Proposer shall bear all costs associated with the preparation and submission of its Proposal, and the Purchaser shall not be responsible or liable for those costs, regardless of the conduct or outcome of the Request for Proposals process.

10. Language of Proposal

10.1. The Proposal, as well as all correspondence and documents relating to the Proposal exchanged by the Proposer and the Purchaser, shall be written in the language specified in the PDS. Supporting documents and printed literature that are part of the Proposal may be in another language provided they are accompanied by an accurate translation of the relevant passages in the language specified in the PDS, in which case, for purposes of interpretation of the Proposal, such translation shall govern.

11. Documents Comprising the Proposal

11.1. The Proposal shall comprise two Parts, namely the Technical Part and the Financial Part. These two Parts shall be submitted simultaneously in two separate sealed envelopes (two-envelope procurement process). One envelope shall contain only information relating to the Technical Part and the other, only information relating to the Financial Part. These two envelopes

shall be enclosed in a separate sealed outer envelope marked "Original Proposal'.

11.2. The Technical Part shall contain the following:

(a) **Letter of Proposal**-Technical Part, prepared in accordance with ITP 12;

(b) **Proposal Security or Proposal-Securing Declaration** in accordance with ITP 20;

(c) **Alternative Proposal**- Technical Part**:** if permissible, in accordance with ITP 13, the Technical Part of any Alternative Proposal;

(d) **Authorization:** written confirmation authorizing the signatory of the Proposal to commit the Proposer, in accordance with ITP 21.3;

(e) **Eligibility of Information System:** documentary evidence established in accordance with ITP 14.1 that the Information System offered by the Proposer in its Proposal or in any alternative Proposal, if permitted, are eligible;

(f) **Proposer's Eligibility and qualifications:** documentary evidence in accordance with ITP 15 establishing the Proposer's eligibility and qualifications to perform the contract if its Proposal is accepted;

(g) **Conformity:** documentary evidence established in accordance with ITP 16 that the Information System offered by the Proposer conform to the **request for proposals** document;

(h) **Subcontractors:** list of subcontractors, in accordance with ITP 16.4;

(i) **Intellectual Property**: a list of: Intellectual Property as defined in GCC Clause 15;

(i) all Software included in the Proposal, assigning each item to one of the software categories defined in GCC Clause 1.1 (c):

a. System, General Purpose, and Application Software; or

b. Standard and Custom Software;

(ii) all Custom Materials, as defined in GCC Clause 1.1 (c), included in the Proposal;

All Materials not identified as Custom Materials shall be deemed Standard Materials, as defined in GCC Clause 1.1 (c);

Re-assignments among the Software and Materials categories, if necessary, will be made during the implementation of the Contract according to GCC Clause 39 (Changes to the Information System); and

(j) any other document required **in the PDS.**

11.3. **The Financial Part shall contain the following:**

(a) Letter of Proposal – Financial Part: prepared in accordance with ITP 12 and ITP 17;

(b) Schedule: Price Schedules completed in accordance with ITP 12 and ITP 17;

(c) Alternative Proposal - Financial Part: if permissible in accordance with ITP 13, the Financial Part of any Alternative Proposal; and

(d) any other document required in the PDS.

11.4. The Technical Part shall not include any information related to the Proposal price. Where material financial information related to the Proposal price is contained in the Technical Part the Proposal shall be declared non-responsive.

11.5. In addition to the requirements under ITP 11.2, Proposals submitted by a JV shall include in the Technical Part a copy of the Joint Venture Agreement entered into by all members indicating at least the parts of the Information System to be executed by the respective members. Alternatively, a letter of intent to execute a Joint Venture Agreement in the event of a successful Proposal shall be signed by all members and submitted with the Proposal, together with a copy of the proposed Agreement indicating at least the parts of the Information System to be executed by the respective members.

11.6. The Proposer shall furnish in the Letter of Proposal - Financial Part information on commissions and gratuities, if any, paid or to be paid to agents or any other party relating to this procurement process.

12. Letters of Proposal and Price Schedules

12.1. The Letter of Proposal - Technical Part, Letter of Proposal-Financial Part and Price Schedules shall be prepared using the relevant forms furnished in Section IV, Proposal Forms. The forms must be completed without any alterations to the text, and no substitutes shall be accepted except as provided under ITP 21.3. All blank spaces shall be filled in with the information requested.

13. Alternative Proposals

13.1. The PDS indicates whether alternative Proposals are allowed. If they are allowed, the PDS will also indicate whether they are permitted in accordance with ITP 13.3, or invited in accordance with ITP 13.2 and/or ITP 13.4.

13.2. When alternatives to the Time Schedule are explicitly invited, a statement to that effect will be included in the PDS, and the method of evaluating different time schedules will be described in Section III, Evaluation and Qualification Criteria.

13.3. Except as provided under ITP 13.4 below, Proposers wishing to offer technical alternatives to the Purchaser's requirements as described in the request for proposals document must also provide: (i) a price at which they are prepared to offer an Information System meeting the Purchaser's requirements; and (ii) all information necessary for a complete evaluation of the alternatives by the Purchaser, including drawings, design calculations, technical specifications, breakdown of prices, and proposed installation methodology and other relevant details. Only the technical alternatives, if any, of the Proposer with the Most Advantageous Proposal conforming to the basic technical requirements shall be considered by the Purchaser.

13.4. When Proposers are invited in the PDS to submit alternative technical solutions for specified parts of the system, such parts shall be described in Section VII, Purchaser's Requirements. Technical alternatives that comply with the performance and technical criteria specified for the Information System shall be considered by the Purchaser on their own merits, pursuant to ITP 32.

14. Documents Establishing the Eligibility of the Information System

14.1. To establish the eligibility of the Information System in accordance with ITP 5, Proposers shall complete the country of origin declarations in the Price Schedule Forms, included in Section IV, Proposal Forms.

15. Documents Establishing the Eligibility and Qualifications of the Proposer

15.1. To establish its eligibility and qualifications to perform the Contract in accordance with Section III, Evaluation and Qualification Criteria, the Proposer shall provide the information requested in the corresponding information sheets included in Section IV, Proposal Forms.

15.2. In the event that prequalification of potential Proposers has been undertaken as stated in the PDS, only Proposals from prequalified Proposers shall be considered for award of Contract. These qualified Proposers should submit with their Proposals any information updating their original prequalification applications or, alternatively, confirm in their Proposals that the originally

submitted prequalification information remains essentially correct as of the date of Proposal submission.

15.3. Any change in the structure or formation of a Proposer after being prequalified and invited to submit Proposals, if applicable, (including, in the case of a JV, any change in the structure or formation of any member and also including any change in any specialized subcontractor whose qualifications were considered to prequalify the Applicant) shall be subject to the written approval of the Purchaser prior to the deadline for submission of Proposals. Such approval shall be denied if (i) a Proposer proposes to associate with a disqualified Proposer or in case of a disqualified joint venture, any of its members; (ii) as a consequence of the change, the Proposer no longer substantially meets the qualification criteria; or (iii) in the opinion of the Purchaser, the change may result in a substantial reduction in competition. Any such change should be submitted to the Purchaser not later than fourteen (14) days after the date of the notice for RFP sent to the prequalified Proposers.

16. Documents Establishing Conformity of the Information System

16.1. Pursuant to ITP 11.2 (g), the Proposer shall furnish, as part of its Proposal, documents establishing the conformity to the request for proposals documents of the Information System that the Proposer proposes to design, supply and install under the Contract.

16.2. The documentary evidence of conformity of the Information System to the request for proposals documents including:

(a) Preliminary Project Plan describing, among other things, the methods by which the Proposer will carry out its overall management and coordination responsibilities if awarded the Contract, and the human and other resources the Proposer proposes to use. The Preliminary Project Plan must also address any other topics specified in the PDS. In addition, the Preliminary Project Plan should state the Proposer's assessment of what it expects the Purchaser and any other party involved in the implementation of the Information System to provide during implementation and how the Proposer proposes to coordinate the activities of all involved parties;

(b) written confirmation that the Proposer accepts responsibility for the successful integration and inter-operability of all components of the Information System as required by the request for proposals documents;

(c) an item-by-item commentary on the Purchaser's Technical Requirements, demonstrating the substantial responsiveness of the Information System offered to those requirements. In demonstrating responsiveness, the Proposer should use the Technical Responsiveness Checklist (or Checklist Format) in the Sample Proposal Forms (Section IV). The commentary shall include explicit cross-references to the relevant pages in

the supporting materials included in the Proposal. Whenever a discrepancy arises between the item-by-item commentary and any catalogs, technical specifications, or other preprinted materials submitted with the Proposal, the item-by-item commentary shall prevail;

(d) support material (e.g., product literature, white papers, narrative descriptions of technologies and/or technical approaches), as required and appropriate; and

(e) any separate and enforceable contract(s) for Recurrent Cost items which the PDS ITP 17.2 requires Proposers to propose.

16.3. References to brand names or model numbers or national or proprietary standards designated by the Purchaser in the request for proposals documents are intended to be descriptive and not restrictive. Except as specified in the PDS for specific items or standards, the Proposer may substitute alternative brand/model names or standards in its Proposal, provided that it demonstrates to the Purchaser's satisfaction that the use of the substitute(s) will result in the Information System being able to perform substantially equivalent to or better than that specified in the Technical Requirements.

16.4. For major items of the Information System as listed by the Purchaser in Section III, Evaluation and Qualification Criteria, which the Proposer intends to purchase or subcontract, the Proposer shall give details of the name and nationality of the proposed subcontractors, including manufacturers, for each of those items. In addition, the Proposer shall include in its Proposal information establishing compliance with the requirements specified by the Purchaser for these items. Quoted rates and prices will be deemed to apply to whichever subcontractor is appointed, and no adjustment of the rates and prices will be permitted.

16.5. The Proposer shall be responsible for ensuring that any subcontractor proposed complies with the requirements of ITP 4, and that any goods or services to be provided by the subcontractor comply with the requirements of ITP 5 and ITP 16.1.

17. Proposal Prices

17.1. All Goods and Services identified in the Supply and Installation Cost Sub-Tables in System Inventory Tables in Section VII, and all other Goods and Services proposed by the Proposer to fulfill the requirements of the Information System, must be priced separately and summarized in the corresponding cost tables in the Sample Proposal Forms (Section IV), in accordance with the instructions provided in the tables and in the manner specified below.

17.2. Unless otherwise specified in the PDS, the Proposer must also propose Recurrent Cost Items specified in the Technical Requirements, Recurrent Cost Sub-Table of the System Inventory Tables in Section VII (if any). These must be priced separately and summarized in the corresponding cost tables in the Sample

Proposal Forms (Section IV), in accordance with the instructions provided in the tables and in the manner specified below:

(a) if specified **in the PDS,** the Proposer must also propose separate enforceable contracts for the Recurrent Cost Items not included in the main Contract;

(b) prices for Recurrent Costs are all-inclusive of the costs of necessary Goods such as spare parts, software license renewals, labor, etc., needed for the continued and proper operation of the Information System and, if appropriate, of the Proposer's own allowance for price increases;

(c) prices for Recurrent Costs beyond the scope of warranty services to be incurred during the Warranty Period, defined in GCC Clause 29.4 and prices for Recurrent Costs to be incurred during the Post-Warranty Period, defined in SCC Clause 1.1. (e) (xiii), shall be quoted as Service prices on the Recurrent Cost Sub-Table in detail, and on the Recurrent Cost Summary Table in currency totals.

17.3. Unit prices must be quoted at a level of detail appropriate for calculation of any partial deliveries or partial payments under the contract, in accordance with the Implementation Schedule in Section VII), and with GCC and SCC Clause 12 – Terms of Payment. Proposers may be required to provide a breakdown of any composite or lump-sum items included in the Cost Tables

17.4. The price of items that the Proposer has left blank in the cost tables provided in the Sample Proposal Forms (Section IV) shall be assumed to be included in the price of other items. Items omitted altogether from the cost tables shall be assumed to be omitted from the Proposal and, provided that the Proposal is substantially responsive, an adjustment to the Proposal price will be made during Proposal evaluation in accordance with ITP 34.1.

17.5. The prices for Goods components of the Information System are to be expressed and shall be defined and governed in accordance with the rules prescribed in the edition of Incoterms specified in the PDS, as follows:

(a) Goods supplied from outside the Purchaser's country:

Unless otherwise specified **in the PDS**, the prices shall be quoted on a CIP (named place of destination) basis, exclusive of all taxes, stamps, duties, levies, and fees imposed in the Purchaser's country. The named place of destination and special instructions for the contract of carriage are as specified in the SCC for GCC 1.1 (e) (iii)**.** In quoting the price, the Proposer shall be free to use transportation through carriers registered in any eligible countries. Similarly, the Proposer may obtain insurance services from any eligible source country;

(b) Locally supplied Goods:

Unit prices of Goods offered from within the Purchaser's Country, shall be quoted on an EXW (ex factory, ex works, ex warehouse or off-the-shelf, as applicable) basis, including all customs duties, levies, fees, sales and other taxes incurred until delivery of the Goods, but excluding all VAT or sales and other taxes and duties/fees incurred for the Goods at the time of invoicing or sales transaction, if the Contract is awarded;

(c) Inland transportation.

17.6. Unless otherwise stated in the PDS, inland transportation, insurance and related local costs incidental to the delivery of the Goods to the designated Project Sites must be quoted separately as a Service item in accordance with ITP 17.5, whether the Goods are to be supplied locally or from outside the Purchaser's country, except when these costs are already included in the price of the Goods, as is, e.g., the case, when ITP 17.5 (a) specifies CIP, and the named places of destination are the Project Sites.

17.7. The price of Services shall be separated into their local and foreign currency components and where appropriate, broken down into unit prices. Prices must include all taxes, duties, levies and fees whatsoever, except only VAT or other indirect taxes, or stamp duties, that may be assessed and/or apply in the Purchaser's country on/to the price of the Services invoiced to the Purchaser, if the Contract is awarded.

17.8. Unless otherwise specified in the PDS, the prices must include all costs incidental to the performance of the Services, as incurred by the Supplier, such as travel, subsistence, office support, communications, translation, printing of materials, etc. Costs incidental to the delivery of the Services but incurred by the Purchaser or its staff, or by third parties, must be included in the price only to the extent such obligations are made explicit in these request for proposals documents (as, e.g., a requirement for the Proposer to include the travel and subsistence costs of trainees).

17.9. Unless otherwise specified in the PDS, prices quoted by the Proposer shall be fixed during the Proposer's performance of the Contract and not subject to increases on any account. Proposals submitted that are subject to price adjustment will be rejected.

18. Currencies of Proposal and Payment

18.1. The currency(ies) of the Proposal and currencies of payment shall be the same. The Proposer shall quote in the currency of the Purchaser's Country the portion of the Proposal price that corresponds to expenditures incurred in the currency of the Purchaser's Country, unless otherwise specified in the PDS.

18.2. The Proposer may express the Proposal price in any currency. If the Proposer wishes to be paid in a combination of amounts in different currencies, it may quote its price accordingly but shall use no more than three foreign currencies in addition to the currency of the Purchaser's Country.

19. Period of Validity of Proposals

19.1. Proposals shall remain valid until the date specified in the PDS or any extended date if amended by the Purchaser in accordance with ITP 8. A Proposal that is not valid until the date specified in the PDS, or any extended date if amended by the Purchaser in accordance with ITP 8, shall be rejected by the Purchaser as nonresponsive.

19.2. In exceptional circumstances, prior to the date of expiry of the Proposal validity, the Purchaser may request Proposers to extend the date of validity until a specified date. The request and the responses shall be made in writing. If a Proposal Security is requested in accordance with ITP 20, it shall also be extended for twenty-eight days (28) beyond the deadline of the extended validity period. A Proposer may refuse the request without forfeiting its Proposal Security. A Proposer granting the request shall not be required or permitted to modify its Proposal, except as provided in ITP 19.3.

19.3. If the award is delayed by a period exceeding fifty-six (56) days beyond the expiry of the initial Proposal validity specified in accordance with ITP 19.1, the Contract price shall be determined as follows:

(a) in case of fixed price contracts, the contract price shall be the Proposal price adjusted by a factor or factors specified **in the PDS**;

(b) in the case of an adjustable price contracts, no adjustments shall be made;

(c) in any case, Proposal evaluation shall be based on the Proposal Price without taking into consideration the applicable correction from those indicated above.

20. Proposal Security

20.1. The Proposer shall furnish as part of the Technical Part of its Proposal, either a Proposal-Securing Declaration or a Proposal Security as specified in the PDS, in original form and, in the case of a Proposal Security, in the amount and currency specified in the PDS.

20.2. A Proposal-Securing Declaration shall use the form included in Section IV, Proposal Forms.

20.3. If a Proposal Security is specified pursuant to ITP 20.1, the Proposal security shall be a demand guarantee in any of the following forms at the Proposer's option:

(a) an unconditional guarantee issued by a non-bank financial institution (such as an insurance, bonding or surety company);

(b) an irrevocable letter of credit;

(c) a cashier's or certified check; or

(d) another security indicated **in the PDS,**

from a reputable source from an eligible country. If an unconditional guarantee is issued by a non-bank financial institution located outside the Purchaser's Country the issuing non-bank financial institution shall have a correspondent financial institution located in the Purchaser's Country to make it enforceable unless the Purchaser has agreed in writing, prior to Proposal submission, that a correspondent financial institution is not required. In the case of a bank guarantee, the Proposal Security shall be submitted either using the Proposal Security Form included in Section IV, Proposal Forms or in another substantially similar format approved by the Purchaser prior to Proposal submission. In either case, the form must include the complete name of the Proposer. The Proposal Security shall be valid for twenty-eight (28) days beyond the original date of expiry of the Proposal validity, or beyond any extended date if requested under ITP 19.2.

20.4. If a Proposal Security or a Proposal-Securing Declaration is specified pursuant to ITP 20.1, any Proposal not accompanied by a substantially responsive Proposal Security or Proposal-Securing Declaration shall be rejected by the Purchaser as non-responsive.

20.5. If a Proposal Security is specified pursuant to ITP 20.1, the Proposal Security of unsuccessful Proposers shall be returned as promptly as possible upon the successful Proposer's furnishing of the Performance Security pursuant to ITP 48.

20.6. The Proposal Security of the successful Proposer shall be returned as promptly as possible once the successful Proposer has signed the Contract and furnished the required Performance Security.

20.7. The Proposal Security may be forfeited:

(a) if a Proposer withdraws its Proposal prior to the expiry date of Proposal validity specified by the Proposer on the Letter of Proposal or any extended date provided by the Proposer; or

(b) if the successful Proposer fails to**:**

(i) sign the Contract in accordance with ITP 47; or

(ii) furnish a performance security in accordance with ITP 48.

20.8. The Proposal Security or the Proposal-Securing Declaration of a JV shall be in the name of the JV that submits the Proposal. If the JV has not been legally constituted into a legally enforceable JV at the time of submission of Proposals, the Proposal Security or the Proposal-Securing Declaration shall be in the names of all future members as named in the letter of intent referred to in ITP 4.1 and ITP 11.5.

20.9. If a Proposal Security is not required in the PDS, and;

(a) if a Proposer withdraws its Proposal prior to the expiry date of the Proposal validity specified by the Proposer on the Letter of Proposal, or any extended date provided by the Proposer; or

(b) if the successful Proposer fails to: sign the Contract in accordance with ITP 47; or furnish a Performance Security in accordance with ITP 48;

the Purchaser may, if provided for **in the PDS**, declare the Proposer disqualified to be awarded a contract by the Purchaser for a period of time as stated **in the PDS**.

21. Format and Signing of Proposal

21.1. The Proposer shall prepare one original and copies/sets of the documents comprising the Proposal as described in ITP 11 and Proposer22.

21.2. Proposers shall mark as "CONFIDENTIAL" information in their Proposals which is confidential to their business. This may include proprietary information, trade secrets, or commercial or financially sensitive information.

21.3. The original and all copies of the Proposal shall be typed or written in indelible ink and shall be signed by a person duly authorized to sign on behalf of the Proposer. This authorization shall consist of a written confirmation as specified in the PDS and shall be attached to the Proposal. The name and position held by each person signing the authorization must be typed or printed below the signature. All pages of the Proposal where entries or amendments have been made shall be signed or initialed by the person signing the Proposal.

21.4. In case the Proposer is a JV, the Proposal shall be signed by an authorized representative of the JV on behalf of the JV, and so as to be legally binding on all the members as evidenced by a power of attorney signed by their legally authorized representatives.

21.5. Any interlineations, erasures, or overwriting shall be valid only if they are signed or initialed by the person signing the Proposal.

D. SUBMISSION OF PROPOSALS

22. Submission, Sealing and Marking of Proposals

22.1. The Proposer shall deliver the Proposal in two separate, sealed envelopes (the Technical Part and the Financial Part). These two envelopes shall be enclosed in a separate sealed outer envelope marked "Original PROPOSAL". In addition, the Proposer shall submit copies of the Proposal in the number specified in the PDS. Copies of the Technical Part shall be placed in a separate sealed envelope marked "COPIES: TECHNICAL PART". Copies of the Financial Part shall be placed in a separate sealed envelope marked "COPIES: FINANCIAL PART". The Proposer shall place both of these envelopes in a separate, sealed outer envelope marked "PROPOSAL COPIES". In the event of any discrepancy between the original and the copies, the original shall prevail.

22.2. If alternative Proposals are permitted in accordance with ITP 14, the alternative Proposals shall be submitted as follows: the original of the alternative Proposal Technical Part shall be placed in a sealed envelope marked "ALTERNATIVE PROPOSAL – TECHNICAL PART" and the Financial Part shall be placed in a sealed envelope marked "ALTERNATIVE PROPOSAL – FINANCIAL PART" and these two separate sealed envelopes then enclosed within a sealed outer envelope marked "ALTERNATIVE PROPOSAL – ORIGINAL", the copies of the alternative Proposal will be placed in separate sealed envelopes marked "ALTERNATIVE PROPOSAL – COPIES OF TECHNICAL PART", and "ALTERNATIVE PROPOSAL – COPIES OF FINANCIAL PART" and enclosed in a separate sealed outer envelope marked "ALTERNATIVE PROPOSAL - COPIES.

22.3. The envelopes marked "ORIGINAL PROPOSAL" and "PROPOSAL COPIES" (and, if appropriate, a third envelope marked "ALTERNATIVE PROPOSAL") shall be enclosed in a separate sealed outer envelope for submission to the Purchaser.

22.4. The inner and outer envelopes shall:

(a) bear the name and address of the Proposer;

(b) be addressed to the Purchaser in accordance with ITP 23.1;

(c) bear the specific identification of this request for proposals process indicated in accordance with ITP 1.1; and

(d) bear a warning not to open before the time and date for Proposal opening.

22.5. If all envelopes are not sealed and marked as required, the Purchaser will assume no responsibility for the misplacement or premature opening of the Proposal.

23. Deadline for Submission of Proposals

23.1. Proposals must be received by the Purchaser at the address and no later than the date and time indicated in the PDS. When so specified in the PDS, Proposers shall have the option of submitting their Proposals electronically. Proposers submitting Proposals electronically shall follow the electronic Proposal submission procedures specified in the PDS.

23.2. The Purchaser may, at its discretion, extend this deadline for submission of Proposals by amending the request for proposals documents in accordance with ITP 8, in which case all rights and obligations of the Purchaser and Proposers will thereafter be subject to the deadline as extended.

24. Late Proposals

24.1. The Purchaser shall not consider any Proposal that arrives after the deadline for submission of Proposals, in accordance with ITP 23. Any Proposal received by the Purchaser after the deadline for submission of Proposals shall be declared late, rejected, and returned unopened to the Proposer.

25. Withdrawal, Substitution, and Modification of Proposals

25.1. A Proposer may withdraw, substitute, or modify its Proposal after it has been submitted by sending a written notice, duly signed by an authorized representative, and shall include a copy of the authorization in accordance with ITP 21.3, (except that withdrawal notices do not require copies). The corresponding substitution or modification of the Proposal must accompany the respective written notice. All notices must be:

(a) prepared and submitted in accordance with ITP 21 and ITP 22 (except that withdrawals notices do not require copies), and in addition, the respective envelopes shall be clearly marked "WITHDRAWAL," "SUBSTITUTION," "MODIFICATION;" and

(b) received by the Purchaser prior to the deadline prescribed for submission of Proposals, in accordance with ITP 23.

25.2. Proposals requested to be withdrawn in accordance with ITP 25.1 shall be returned unopened to the Proposers.

No Proposal may be withdrawn, substituted, or modified in the interval between the deadline for submission of Proposals and the date of expiry of the Proposal validity specified by the Proposer on the Letter of Proposal or any extended date thereof.

E. PUBLIC OPENING OF TECHNICAL PARTS OF PROPOSALS

26. Public Opening of Technical Parts of Proposals

26.1. Except as in the cases specified in ITP 24 and ITP 25.2, the Purchaser shall conduct the Proposal opening in public, in the presence of Proposers` designated representatives and anyone who chooses to attend, and at the address, date and time specified in the PDS. Any specific electronic Proposal opening procedures required if electronic submission of proposals is permitted in accordance with ITP 23.1, shall be as specified in the PDS.

26.2. First, envelopes marked "Withdrawal" shall be opened and read out and the envelope with the corresponding Proposal shall not be opened but returned to the Proposer. No Proposal withdrawal shall be permitted unless the corresponding withdrawal notice contains a valid authorization to request the withdrawal and is read out at Proposal opening.

26.3. Next, envelopes marked "Substitution" shall be opened and read out and exchanged with the corresponding Proposal being substituted, and the substituted Proposal shall not be opened, but returned to the Proposer. No Proposal substitution shall be permitted unless the corresponding substitution notice contains a valid authorization to request the substitution and is read out at Proposal opening.

26.4. Envelopes marked "Modification" shall be opened and read out with the corresponding Proposal. No Proposal modification shall be permitted unless the corresponding modification notice contains a valid authorization to request the modification and is read out at Proposal opening. Only Proposals that are opened and read out at Proposal opening shall be considered further.

26.5. Next, all other envelopes marked "Technical Part" shall be opened one at a time. All envelopes marked "Second Envelope: Financial Part" shall remain sealed and kept by the Purchaser in safe custody until they are opened at a later public opening, following the evaluation of the Technical Part parts of the Proposals. On opening the envelopes marked "Technical Part" the Purchaser shall read out: the name of the Proposer, the presence or the absence of a Proposal Security, or Proposal-Securing Declaration, if required, and whether there is a modification; and Alternative Proposal - Technical Part; and any other details as the Purchaser may consider appropriate.

26.6. Only Technical Parts of Proposals and Alternative Proposal - Technical Parts that are read out at Proposal opening shall be considered further for evaluation. The Letter of Proposal-Technical Part and the separate sealed envelope marked "Second Envelope: Financial Part" are to be initialed by representatives of the Purchaser attending Proposal opening in the manner specified in the PDS.

26.7. The Purchaser shall neither discuss the merits of any Proposal nor reject any Proposal (except for late Proposals, in accordance with ITP 24.1).

26.8. The Purchaser shall prepare a record of the Proposal opening that shall include, as a minimum:

(a) the name of the Proposer and whether there is a withdrawal, substitution, or modification;

(b) any alternative Proposals; and

(c) the presence or absence of a Proposal Security or a Proposal-Securing Declaration.

26.9. The Proposers' representatives who are present shall be requested to sign the record. The omission of a Proposer's signature on the record shall not invalidate the contents and effect of the record. A copy of the record shall be distributed to all Proposers.

F. EVALUATION OF PROPOSALS- GENERAL PROVISIONS

27. Confidentiality

27.1. Information relating to the evaluation of the Technical Part shall not be disclosed to Proposers or any other persons not officially concerned with the procurement process until the notification of evaluation of the Technical Part in accordance with ITP 33. Information relating to the evaluation of Financial Part, the evaluation of combined Technical Part and Financial Part, and recommendation of contract award shall not be disclosed to Proposers or any other persons not officially concerned with the RFP process until the Notification of Intention to Award the Contract is transmitted to Proposers in accordance with ITP 42ProposerProposer.

27.2. Any effort by a Proposer to influence the Purchaser in the evaluation of the Proposals or Contract award decisions may result in the rejection of its Proposal.

27.3. Notwithstanding ITP 27.2, from the time of Proposal opening to the time of Contract award, if any Proposer wishes to contact the Purchaser on any matter related to the procurement process, it should do so in writing.

28. Clarification of Proposals

28.1. To assist in the examination, evaluation, and comparison of the Proposals, and qualification of the Proposers, the Purchaser may, at its discretion, ask any Proposer for a clarification of its Proposal. Any clarification submitted by a Proposer that is not in response to a request by the Purchaser shall not be considered. The Purchaser's request for clarification and the response shall be in writing. No change in the prices or substance of the Proposal shall be sought, offered, or permitted, except to confirm the correction of arithmetic errors discovered by the Purchaser in the evaluation of the Proposals, in accordance with ITP 35.

28.2. If a Proposer does not provide clarifications of its Proposal by the date and time set in the Purchaser's request for clarification, its Proposal may be rejected.

29. Deviations, Reservations, and Omissions

29.1. During the evaluation of Proposals, the following definitions apply:

(a) "Deviation" is a departure from the requirements specified in the request for proposals document;

(b) "Reservation" is the setting of limiting conditions or withholding from complete acceptance of the requirements specified in the request for proposals document; and

(c) "Omission" is the failure to submit part or all of the information or documentation required in the request for proposals document.

29.2. Provided that a Proposal is substantially responsive, the Purchaser may waive any nonmaterial nonconformities in the Proposal.

Provided that a Proposal is substantially responsive, the Purchaser may request that the Proposer submit the necessary information or documentation, within a reasonable period of time, to rectify nonmaterial nonconformities in the Proposal related to documentation requirements. Requesting information or documentation on such nonconformities shall not be related to any aspect of the price of the Proposal. Failure of the Proposer to comply with the request may result in the rejection of its Proposal.

G. EVALUATION OF TECHNICAL PART OF PROPOSALS

30. Determination of Responsiveness

30.1. The Purchaser's determination of the Technical Part's responsiveness shall be based on the contents of the Proposal, as specified in ITP 11.

30.2. Preliminary examination of the Technical Part shall be carried out to identify proposals that are incomplete, invalid or substantially nonresponsive to the requirements of the request for proposals documents. A substantially responsive Proposal is one that materially confirms to the requirements of the request for proposals document without material deviation, reservation, or omission. A material deviation, reservation, or omission is one that,

(a) if accepted, would:

(i) affect in any substantial way the scope, quality, or performance of the Works specified in the Contract; or

(ii) limit in any substantial way, inconsistent with the request for proposals document, the Purchaser's rights or the Proposer's obligations under the proposed Contract;or

(iii)limit in any substantial way, inconsistent with the request for proposals document, the Purchaser's rights or the Proposer's obligations under the proposed Contract; or

(b) if rectified, would unfairly affect the competitive position of other Proposers presenting substantially responsive Proposals.

30.3. If the Technical Part is not substantially responsive to the requirements of the request for proposals document, it shall be rejected by the Purchaser and may not subsequently be made responsive by correction of the material deviation, reservation, or omission.

31. Eligibility and Qualifications of the Proposer

31.1. The Purchaser shall determine to its satisfaction whether the Proposers that have been assessed to have submitted substantially responsive Proposals are eligible, and either continue to meet (if prequalification applies) or meet (if prequalification has not been carried out), the qualifying criteria specified in Section III, Evaluation and Qualification Criteria.

31.2. The determination shall be based upon an examination of the documentary evidence of the Proposer's eligibility and qualifications submitted by the Proposer, pursuant to ITP 15. The determination shall not take into consideration the qualifications of other firms such as the Proposer's subsidiaries, parent entities, affiliates, subcontractors (other than Specialized Subcontractors if

permitted in the request for proposals document), or any other firm.

31.3. Prior to Contract award, the Purchaser will verify that the successful Proposer (including each member of a JV) is not disqualified by the Bank due to noncompliance with contractual SEA/SH prevention and response obligations. The Purchaser will conduct the same verification for each subcontractor proposed by the successful Proposer. If any proposed subcontractor does not meet the requirement, the Purchaser will require the Proposer to propose a replacement subcontractor.

31.4. Only substantially responsive Proposals submitted by eligible and qualified Proposers shall proceed to the detailed technical evaluation specified in ITP 32.

31.5. The Purchaser's evaluation of Technical Part will be carried out as specified in Section III, Evaluation and Qualification Criteria.

32. Detailed Evaluation of Technical Part

32.1. The scores and weightings to be given to Rated Criteria (including technical and non-price factors and sub factors) are specified in the PDS.

H. NOTIFICATION OF EVALUATION OF TECHNICAL PARTS AND PUBLIC OPENING OF FINANCIAL PARTS

33. Notification of Evaluation of Technical Parts and Public Opening of Financial Parts

33.1. Following the completion of the evaluation of the Technical Parts of the Proposals, the Purchaser shall notify in writing those Proposers whose Proposals were considered substantially non-responsive to the request for proposals document or failed to meet the eligibility and qualification requirements, advising them of the following information:

(a) the grounds on which their Technical Part of Proposal failed to meet the requirements of the request for proposals document;

(b) their envelopes marked "SECOND ENVELOPE: FINANCIAL PART" will be returned to them unopened after the completion of the selection process and the signing of the Contract; and

(c) Option 1: when BAFO or negotiations is not to be applied notify them of the date, time and location of the public opening of the envelopes marked 'Financial Part", or;

Option 2: **when BAFO or negotiations apply as specified in the PDS,** notify them that: (i) the envelopes marked 'Financial Part' will not be opened in public, but in the presence of a probity auditor appointed by the Purchaser, and that (ii) the announcement of the names of the Proposers whose Financial Parts will be opened and the total Proposal

prices will be deferred to the time that the Notification of Intention to Award the contract is issued.

33.2. The Purchaser shall, simultaneously, notify in writing those Proposers whose Technical Part have been evaluated as substantially responsive to the request for proposals document and met the eligibility and qualification requirements, advising them of the following information:

33.3. their Proposal has been evaluated as substantially responsive to the request for proposals document and met the eligibility and qualification requirements;

33.4. Option 1: when BAFO or negotiations is not to be applied notify them of the date, time and location of the public opening of the envelopes marked 'Financial Part", or;

Option 2: when BAFO or negotiations apply as specified in the PDS, notify them that: (i) the envelopes marked 'Financial Part' will not be opened in public, but in the presence of a probity auditor appointed by the Purchaser, and that (ii) the announcement of the names of the Proposers whose Financial Parts will be opened and the total Proposal prices will be deferred to the time that the Notification of Intention to Award the contract is issued**.**

33.5. When BAFO or negotiations do not apply as specified in the PDS, the Financial Part of the Proposal shall be opened publicly in the presence of Proposers' designated representatives and anyone who chooses to attend.

33.6. The opening date shall be not less than ten (10) Business Days from the date of notification of the results of the technical evaluation, specified in ITP 33.1 and 33.2. However, if the Purchaser receives a complaint on the results of the technical evaluation within the ten (10) Business Days, the opening date shall be subject to ITP 50.1.

33.7. At this public opening, the Financial Parts will be opened by the Purchaser in the presence of Proposers, or their designated representatives and anyone else who chooses to attend. Proposers who met the eligibility and qualification requirements and whose Proposals were evaluated as substantially responsive will have their envelopes marked "SECOND ENVELOPE: FINANCIAL PART" opened at the second public opening. Each of these envelopes marked "SECOND ENVELOPE: FINANCIAL PART" shall be inspected to confirm that they have remained sealed and unopened. These envelopes shall then be opened by the Purchaser. The Purchaser shall read out the names of each Proposer, the technical score and the total Proposal prices, per lot (contract) if applicable, including any discounts and Alternative Proposal - Financial Part, and any other details as the Purchaser may consider appropriate.

33.8. Only envelopes of Financial Part of Proposals, Financial Parts of Alternative Proposals and discounts that are opened and read out at Proposal opening shall be considered further for evaluation. The Letter of Proposal – Financial Part and the Price Schedules are to be initialed by a representative of the Purchaser attending the Proposal opening in the manner specified in the PDS.

33.9. The Purchaser shall neither discuss the merits of any Proposal nor reject any envelopes marked "SECOND ENVELOPE: FINANCIAL PART" at this public opening.

33.10. The Purchaser shall prepare a record of the Financial Part of the Proposal opening that shall include, as a minimum: (a) the name of the Proposer whose Financial Part was opened; (b) the Proposal price, per lot (contract) if applicable, including any discounts; and (c) if applicable, any Alternative Proposal – Financial Part.

33.11. The Proposers whose envelopes marked "SECOND ENVELOPE: FINANCIAL PART" have been opened or their representatives who are present shall be requested to sign the record. The omission of a Proposer's signature on the record shall not invalidate the contents and effect of the record. A copy of the record shall be distributed to all Proposers.

33.12. When, as specified in the PDS, BAFO or negotiations apply the Financial Parts will not be opened in public and will be opened in the presence of a probity auditor appointed by the Purchaser.

33.13. At the opening each of the envelopes marked "Financial Part" shall be inspected to confirm that they have remained sealed and unopened. These envelopes shall then be opened by the Purchaser. The Purchaser shall record the names of each Proposer, and the total Proposal prices and any other details as the Purchaser may consider appropriate. The Letter of Proposal - Financial Part and the Price Schedules are to be initialed by a representative of the Purchaser attending the opening and by the probity auditor.

33.14. The Purchaser shall prepare a record of the opening of the Financial Part envelopes that shall include, as a minimum:

(a) the name of the Proposers whose Financial Part was opened;

(b) the Proposal prices including any discounts. and

(c) The Probity Auditor's report of the opening of the Financial Part.

33.15. The probity auditor shall sign the record. The contents of the envelopes marked 'Financial Part' and the record of the opening shall be kept in safe custody by the Purchaser and not disclosed to anyone until the time of the transmission of the Notification of Intention to Award the contract.

I. EVALUATION OF FINANCIAL PART OF PROPOSALS

34. Adjustments for Non-material Noconformities

34.1. Provided that a Proposal is substantially responsive, the Purchaser shall rectify quantifiable nonmaterial nonconformities related to the Proposal Price. To this effect, the Proposal Price shall be adjusted, for comparison purposes only, to reflect the price of a missing or non-conforming item or component by adding the average price of the item or component quoted by substantially responsive Proposers. If the price of the item or component cannot be derived from the price of other substantially responsive Proposers, the Purchaser shall use its best estimate.

35. Correction of Arithmetic Errors

35.1. In evaluating the Financial Part of each Proposal, the Purchaser shall correct arithmetical errors on the following basis:

(a) where there are errors between the total of the amounts given under the column for the price breakdown and the amount given under the Total Price, the former shall prevail and the latter will be corrected accordingly;

(b) where there are errors between the total of the amounts of Schedule Nos. 1 to 5 and the amount given in Schedule No. 6 (Grand Summary), the former shall prevail and the latter will be corrected accordingly; and

(c) if there is a discrepancy between words and figures, the amount in words shall prevail, unless the amount expressed in words is related to an arithmetic error, in which case the amount in figures shall prevail subject to (a) and (b) above.

35.2. Proposers shall be requested to accept correction of arithmetical errors. Failure to accept the correction in accordance with ITP 35.1, shall result in the rejection of the Proposal.

36. Evaluation of Proposals Financial Part

36.1. To evaluate the Financial Part, the Purchaser shall consider the following:

(a) the Proposal price, excluding provisional sums and the provision, if any, for contingencies in the Price Schedules;

(b) price adjustment for correction of arithmetic errors in accordance with ITP 35.1;

(c) price adjustment due to discounts offered in accordance with ITP 26;

(d) price adjustment due to quantifiable nonmaterial nonconformities in accordance with ITP 34.1;

(e) converting the amount resulting from applying (a) to (c) above, if relevant, to a single currency in accordance with ITP 36.2; and

(f) the evaluation factors indicated in the PDS and detailed in Section III, Evaluation and Qualification Criteria.

36.2. For evaluation and comparison purposes, the currency(ies) of the **Proposal** shall be converted into a single currency **as specified in the PDS**.

36.3. No margin of domestic preference shall apply**.**

36.4. If price adjustment is allowed in accordance with ITP 17.7, the estimated effect of the price adjustment provisions of the Conditions of Contract, applied over the period of execution of the Contract, shall not be taken into account in Proposal evaluation.

36.5. If this request for proposals document allows Proposers to quote separate prices for different lots (contracts), each lot will be evaluated separately to determine the Most Advantageous Proposal using the methodology specified in Section III, Evaluation and Qualification Criteria. Discounts that are conditional on the award of more than one lotor slice shall not be considered for Proposal evaluation.

36.6. The Purchaser will evaluate and compare the Proposals. The evaluation will be performed assuming either that:

(a) the Contract will be awarded to the Most Advantageous Proposal for the entire Information System; or

(b) if specified **in the PDS**, Contracts will be awarded to the Proposers for each individual Subsystem, lot, or slice defined in the Technical Requirements whose Proposals result in the Most Advantageous Proposal/Proposals for the entire System.

In the latter case, discounts that are conditional on the award of more than one Subsystem, lot, or slice may be offered in Proposals. Such discounts will be considered in the evaluation of Proposals as specified **in the PDS**.

37. Abnormally Low Proposals

37.1. An Abnormally Low Proposal is one where the Proposal price in combination with other constituent elements of the Proposal appears unreasonably low to the extent that the Proposal price raises material concerns as to the capability of the Proposer to perform the Contract for the offered Proposal Price.

37.2. In the event of identification of a potentially Abnormally Low Proposal, the Purchaser shall seek written clarifications from the Proposer, including detailed price analyses of its Proposal price in relation to the subject matter of the contract, scope, proposed methodology, schedule, allocation of risks and responsibilities and any other requirements of the request for proposals document.

37.3. After evaluation of the price analyses, in the event that the Purchaser determines that the Proposer has failed to demonstrate

its capability to perform the Contract for the offered Proposal Price, the Purchaser shall reject the Proposal.

38. Unbalanced or Front Loaded Proposals

38.1. If the Proposal that is evaluated as the lowest evaluated cost is, in the Purchaser's opinion, seriously unbalanced or front loaded the Purchaser may require the Proposer to provide written clarifications. Clarifications may include detailed price analyses to demonstrate the consistency of the Proposal prices with the scope of information systems, installations, proposed methodology, schedule and any other requirements of the request for proposals document.

38.2. After the evaluation of the information and detailed price analyses presented by the Proposer, the Purchaser may:

(a) accept the Proposal; or

(b) if appropriate, require that the total amount of the Performance Security be increased, at the expense of the Proposer, to a level not exceeding twenty percent (20%) of the Contract Price; or

(c) reject the Proposal.

J. EVALUATION OF COMBINED TECHNICAL AND FINANCIAL PARTS, MOST ADVANTAGEOUS PROPOSAL AND NOTIFICATION OF INTENTION TO AWARD

39. Evaluation of combined Technical and Financial Parts, Most Advantageous Proposal

39.1. The Purchaser's evaluation of responsive Proposals will take into account technical factors, in addition to cost factors in accordance with Section III Evaluation and Qualification Criteria. The weight to be assigned for the Technical factors and cost is specified in the PDS. The Purchaser will rank the Proposals based on the evaluated Proposal score (B).

39.2. Best and Final Offer (BAFO): After completion of the combined technical and financial evaluation of proposals, If specified in the PDS, the Purchaser may invite those Proposers to submit their BAFOs. The procedure for submitting BAFOs will be specified in the PDS. BAFO is a final opportunity for Proposers to improve their Proposals without changing the specified business function and performance requirements in accordance with the invitation to Submit Second Stage Combined Technical and Financial Proposals, Proposers are not obliged to submit a BAFO. Where BAFO is used there will be no negotiation after BAFO**.**

39.3. BAFO will apply a two envelope procurement process. The submission of BAFOs, opening of the Technical Parts and Financial Parts and the evaluation of Proposals will follow the

procedures described for the Technical, Financial and Combined evaluation above, as appropriate**.**

39.4. The Purchaser shall determine the Most Advantageous Proposal. The Most Advantageous Proposal is the Proposal of the Proposer that meets the Qualification Criteria and whose Proposal has been determined to be substantially responsive to the request for proposals document and is the Proposal with the highest combined technical and financial score.

39.5. If specified in the PDS, the Purchaser may conduct negotiations following the evaluation of the proposals and before the final contract award. The procedure of the negotiations will be specified in the PDS.

39.6. Negotiations shall be held in the presence of probity auditor appointed by the Purchaser.

39.7. Negotiations may address any aspect of the contract so long as they do not materially change the specified business function and performance requirements.

39.8. The Purchaser may negotiate first with the Proposer that has the Most Advantageous Proposal. If the negotiations are unsuccessful the Purchaser may negotiate with the Proposer that has the next best Most Advantageous Proposal, and so on down the list until a successful negotiated outcome is achieved.

39.9. Unless otherwise specified in the PDS, the Purchaser will NOT carry out tests prior to Contract award, to determine that the performance or functionality of the Information System offered meets those stated in the Technical Requirements. However, if so specified in the PDS the Purchaser may carry out such tests as detailed in the PDS.

39.10. Proposer.

39.11. Prior to Contract award, the Purchaser may carry out visits or interviews with the Proposer's clients referenced in its Proposal and site inspections.

39.12. The capabilities of the manufacturers and subcontractors proposed by the Proposer that is determined to have offered the Most Advantageous Proposal for identified major items of supply or services will also be evaluated for acceptability in accordance with Section III, Evaluation and Qualification Criteria. Their participation should be confirmed with a letter of intent between the parties, as needed. Should a manufacturer or subcontractor be determined to be unacceptable, the Proposal will not be rejected, but the Proposer will be required to substitute an acceptable manufacturer or subcontractor without any change to the Proposal price. Prior to signing the Contract, the corresponding Appendix to the Contract Agreement shall be completed, listing the

approved manufacturers or subcontractors for each item concerned.

40. Purchaser's Right to Accept Any Proposal, and to Reject Any or All Proposals

40.1. The Purchaser reserves the right to accept or reject any Proposal, and to annul the procurement process and reject all Proposals at any time prior to contract award, without thereby incurring any liability to Proposers. In case of annulment, all Proposals submitted and specifically, Proposal securities, shall be promptly returned to the Proposers.

41. Standstill Period

41.1. The Contract shall not be awarded earlier than the expiry of the Standstill Period. The Standstill Period shall be ten (10) Business Days unless extended in accordance with ITP 46. The Standstill Period commences the day after the date the Purchaser has transmitted to each Proposer the Notification of Intention to Award the Contract. Where only one Proposal is submitted, or if this contract is in response to an emergency situation recognized by the Bank, the Standstill Period shall not apply.

42. Notification of Intention to Award

42.1. The Purchaser shall send to each Proposer the Notification of Intention to Award the Contract to the successful Proposer. The Notification of Intention to Award shall contain, at a minimum, the following information:

(a) the name and address of the Proposer submitting the successful Proposal;

(b) the Contract price of the successful Proposal;

(c) the total combined score of the successful Proposal;

(d) the names of all Proposers who submitted Proposals, and their Proposal prices as readout and as evaluated prices and technical scores;

(e) a statement of the reason(s) the Proposal (of the unsuccessful Proposer to whom the notification is addressed) was unsuccessful;

(f) the expiry date of the Standstill Period; and

(g) instructions on how to request a debriefing or submit a complaint during the standstill period;

K. AWARD OF CONTRACT

43. Award Criteria

43.1. Subject to ITP 40, the Purchaser shall award the Contract to the successful Proposer. This is the Proposer whose Proposal has been determined to be the Most Advantageous Proposal..

Proposer.

44. Purchaser's Right to Vary Quantities at Time of Award

44.1. The Purchaser reserves the right at the time of Contract award to increase or decrease, by the percentage(s) for items as indicated in the PDS.

45. Notification of Award

45.1. Prior to the date of expiry of the Proposal validity and upon expiry of the Standstill Period, specified in ITP 41.1 or any extension thereof, and, upon satisfactorily addressing any complaint that has been filed within the Standstill Period, the Purchaser shall notify the successful Proposer, in writing, that its Proposal has been accepted. The notification letter (hereinafter and in the Contract Forms called the "Letter of Acceptance") shall specify the sum that the Purchaser will pay the Supplier in consideration of the execution of the Contract (hereinafter and in the Conditions of Contract and Contract Forms called "the Contract Price").

45.2. Within ten (10) Business days after the date of transmission of the Letter of Acceptance, the Purchaser shall publish the Contract Award Notice which shall contain, at a minimum, the following information:

(a) name and address of the Purchaser;

(b) name and reference number of the contract being awarded, and the selection method used;

(c) names of all Proposers that submitted Proposals, and their Proposal prices as read out at Proposal opening, and as evaluated;

(d) name of Proposers whose Proposals were rejected and the reasons for their rejection;

(e) the name of the successful Proposer, the final total contract price, the contract duration and a summary of its scope; and

(f) successful Proposer's Beneficial Ownership Disclosure Form.

45.3. The Contract Award Notice shall be published on the Purchaser's website with free access if available, or in at least one newspaper of national circulation in the Purchaser's Country, or in the official gazette.

45.4. Until a formal contract is prepared and executed, the Notification of Award shall constitute a binding Contract.

46. Debriefing by the Purchaser

46.1. On receipt of the Purchaser's Notification of Intention to Award referred to in ITP 42, an unsuccessful Proposer has three (3) Business Days to make a written request to the Purchaser for a debriefing. The Purchaser shall provide a

debriefing to all unsuccessful Proposers whose request is received within this deadline.

46.2. Where a request for debriefing is received within the deadline, the Purchaser shall provide a debriefing within five (5) Business Days, unless the Purchaser decides, for justifiable reasons, to provide the debriefing outside this timeframe. In that case, the standstill period shall automatically be extended until five (5) Business Days after such debriefing is provided. If more than one debriefing is so delayed, the standstill period shall not end earlier than five (5) Business Days after the last debriefing takes place. The Purchaser shall promptly inform, by the quickest means available, all Proposers of the extended standstill period.

46.3. Where a request for debriefing is received by the Purchaser later than the three (3) Business Day deadline, the Purchaser should provide the debriefing as soon as practicable, and normally no later than fifteen (15) Business Days from the date of publication of Public Notice of Award of contract. Requests for debriefing received outside the three (3)-day deadline shall not lead to extension of the standstill period.

46.4. Debriefings of unsuccessful Proposers may be done in writing or verbally. The Proposer shall bear their own costs of attending such a debriefing meeting.

47. Signing of Contract

47.1. The Purchaser shall send to the successful Proposer the Letter of Acceptance including the Contract Agreement, and a request to submit the Beneficial Ownership Disclosure Form providing additional information on its beneficial ownership. The Beneficial Ownership Disclosure Form shall be submitted within eight (8) Business Days of receiving this request.

47.2. The successful Proposer shall sign, date and return to the Purchaser, the Contract Agreement within twenty-eight (28) days of its receipt.

47.3. Notwithstanding ITP 47.2 above, in case signing of the Contract Agreement is prevented by any export restrictions attributable to the Purchaser, to the country of the Purchaser, or to the use of the Information System to be supplied, where such export restrictions arise from trade regulations from a country supplying those Information System, the Proposer shall not be bound by its Proposal, always provided, however, that the Proposer can demonstrate to the satisfaction of the Purchaser and of the Bank that signing of the Contract Agreement has not been prevented by any lack of diligence on the part of the Proposer in completing any formalities, including applying for permits, authorizations and licenses

necessary for the export of the Information System under the terms of the Contract.

48. Performance Security

48.1. Within twenty-eight (28) days of the receipt of the Letter of Acceptance from the Purchaser, the successful Proposer shall furnish the performance security in accordance with the General Conditions, subject to ITP 38.2 (b), using for that purpose the Performance Security Form included in Section X, Contract Forms, or another form acceptable to the Purchaser. If the Performance Security furnished by the successful Proposer is in the form of a bond, it shall be issued by a bonding or insurance company that has been determined by the successful Proposer to be acceptable to the Purchaser. A foreign institution providing a Performance Security shall have a correspondent financial institution located in the Purchaser's Country.

48.2. Failure of the successful Proposer to submit the above-mentioned Performance Security or sign the Contract shall constitute sufficient grounds for the annulment of the award and forfeiture of the Proposal Security. In that event the Purchaser may award the Contract to the Proposer offering the next Most Advantageous Proposal.

49. Adjudicator

49.1. Unless the PDS states otherwise, the Purchaser proposes that the person named in the PDS be appointed as Adjudicator under the Contract to assume the role of informal Contract dispute mediator, as described in GCC Clause 43.1. In this case, a résumé of the named person is attached to the PDS. The proposed hourly fee for the Adjudicator is specified in the PDS. The expenses that would be considered reimbursable to the Adjudicator are also specified in the PDS. If a Proposer does not accept the Adjudicator proposed by the Purchaser, it should state its non-acceptance in its Proposal Form and make a counterproposal of an Adjudicator and an hourly fee, attaching a résumé of the alternative. If the successful Proposer and the Adjudicator nominated in the PDS happen to be from the same country, and this is not the country of the Purchaser too, the Purchaser reserves the right to cancel the Adjudicator nominated in the PDS and propose a new one. If by the day the Contract is signed, the Purchaser and the successful Proposer have not agreed on the appointment of the Adjudicator, the Adjudicator shall be appointed, at the request of either party, by the Appointing Authority specified in the SCC clause relating to GCC Clause 43.1.4, or if no Appointing Authority is specified there, the Contract will be implemented without an Adjudicator.

50. Procurement Related Complaint

50.1. The procedures for making a Procurement-related Complaint are as specified in the PDS.

SECTION II - PROPOSAL DATA SHEET (PDS)

The following specific data for the Information System to be procured shall complement, supplement, or amend the provisions in the Instructions to Proposers (ITP). Whenever there is a conflict, the provisions in the PDS shall prevail over those in ITP.

ITP Reference	A. General
ITP 1.1	The reference number of the Request for Proposals is: *WS-SBS-570867-NC-RFP* The Purchaser is: The Government of Samoa, acting through the Samoa Bureau of Statistics (SBS). The name of the RFP is: *Supply and Installation of the National Digital Identification System* The Purchaser ***shall not*** accept Proposal for multiple lots under this request for proposals document.
ITP 1.3 (a)	Electronic Procurement *shall* be applicable to this procurement. The Purchaser shall use the following electronic-procurement system to manage this bidding process: ***https://portal.tenderlink.com/mof_samoa/login*** The electronic-procurement system shall be used to manage the following aspects of the bidding process: ***issuing requests for Proposal documents, Addendums, Clarifications and submissions of Proposals.***
ITP 2.1	The Borrower is: The Government of Samoa. The Samoa Bureau of Statistics is one of the implementing agencies of this project and acts for the Government of Samoa as the Purchaser under this Contract. Loan or Financing Agreement amount: *USD 21,000,000 (Credit No. IDA-E3780)* The name of the Project is: *Samoa Finance Sector Resilience and Development Project , World Bank Project P181456*
ITP 4.1	Maximum number of members in the JV shall be: *four (4)*
ITP 4.5	A list of debarred firms and individuals is available on the Bank's external website: http://www.worldbank.org/debarr.
B. Request for proposals Document	
ITP 7.1	For Clarification of Proposal purposes only, the Purchaser's address is:

	Attention: *Leota Aliielua Salani, Government Statistician (GS)* Address: *Level 1, Government FMFMII Building, 04 Apia City Boulevard, APIA, SAMOA* Floor/ Room number*: Level 1* City: *Apia* Postal Code: *not applicable* Country: *Samoa* Telephone: *+685 62000* Facsimile number: *not applicable* Electronic mail address: *nid@sbs.gov.ws* Requests for clarification should be received by the Purchaser no later than: *twenty one (21) days prior to the deadline for submission of Proposals in accordance with ITP 23.*
ITP 7.1	Web page: *Ministry of Finance https://www.mof.gov.ws/tender-adverisements and the Government of Samoa e-Tendering portal for submissions, https://portal.tenderlink.com/mof_samoa/login* and Samoa Bureau of Statistics National ID resources webpage https://www.sbs.gov.ws/samoa-nid-resources/
ITP 7.4	A Pre-Proposal meeting *shall* take place at the following date, time and place: Date: *10 November 2026* Time:*10:00 hours, Samoan time* Address: *by videoconference; the connection details are sent to every Proposer that requests to the Purchaser 10 days before the above scheduled date via nid@sbs.gov.ws* Floor/ Room number*: not applicable* City: *Apia* Country: *Samoa* A site visit conducted by the Purchaser *will not be* organized.
C. Preparation of Proposals	
ITP 10.1	The language of the Proposal is: *English.* All correspondence exchange shall be in ***English*** language. Language for translation of supporting documents and printed literature is ***English***.
ITP 11.2 (j)	The Proposer shall submit with its Proposal the following additional documents for the Technical Part of its Proposal: **Code of Conduct for Supplier's Personnel (ES)**

	The Proposer shall submit its Code of Conduct that will apply to the Supplier's Personnel (as defined in GCC Clause 1.1) employed in the execution of the Contract at the Project Site/s to ensure compliance with the Supplier's Environmental and/or Social obligations under the Contract, as applicable. The Proposer shall use for this purpose the Code of Conduct form provided in Section IV. No substantial modifications shall be made to this form, except that the Proposer may introduce additional requirements, including as necessary to take into account specific Contract issues/risks. **Management Strategies and Implementation Plans (MSIP) to manage the (ES) risks** No Management Strategies and Implementation Plans are required for environmental and social risks other than the Code of Conduct above; the environmental and social obligations of the Supplier are those of the General Conditions of Contract. **Cyber security management strategies and implementation plans** The Proposer shall submit method statements, management strategies and implementation plans and innovations to manage cyber security risks, responding to the cyber security chapter of Section VII, the Contract having been assessed as presenting cyber security risks. **Skills transfer and capacity building approach** The Proposer shall submit its skills transfer and capacity building approach responding to the capacity building annex of Section VII, including the pairing model, the target depth of skill per role and the approach to the Purchaser repository and continuous integration. **Technical Responsiveness Checklist** The Proposer shall submit the completed Technical Responsiveness Checklist workbook, returned in its spreadsheet format, with one line per requirement of Section VII, the compliance statement, the technical justification and the cross reference to the Technical Part, as stated in Section III and Section IV.

ITP 11.3(d)	The Proposer shall submit the following additional documents in the Financial Part of its Proposal: ***(a) the Options Schedule, priced separately and never included in the base totals;*** ***(b) the Unit Rates Schedule, giving the rates that apply to any variation of quantity under ITP 44;*** ***(c) the Country of Origin Code Table;*** ***(d) a written statement confirming that the right to use all software is acquired once with the System, is priced in the Supply and Installation Schedules, and carries no fee, royalty or charge per transaction or per registered person to keep it alive. The Financial Part shall contain no technical information beyond what is needed to identify the priced item.***
ITP 13.1	*Alternative Proposals are not permitted.*
ITP 13.2	Alternatives to the Time Schedule *are not* permitted. The Implementation Schedule of Section VII is fixed by the Purchaser and no credit is given for earlier completion.
ITP 13.4	Alternative technical solutions shall not be permitted.
ITP 15.2	Prequalification *has not* been undertaken.
ITP 16.2 (a)	In addition to the topics described in ITP Clause 16.2 (a), the Preliminary Project Plan must address the following topics: (i) ***Project Organization and Management Sub-Plan, including management authorities, responsibilities, and contacts, as well as task, time and resource-bound schedules (in GANTT format), aligned with milestones M1 to M12 of the Implementation Schedule;*** (ii) ***Implementation Sub-Plan, covering release V1 and release V2 separately;*** (iii) ***Training and Skills Transfer Sub-Plan, responding to the capacity building annex of Section VII;*** (iv) ***Testing and Quality Assurance Sub-Plan;*** (v) ***Data Migration and Civil Registration Preloading Sub-Plan;*** (vi) ***Risk Management Sub-Plan, addressing at least the enrolment kit procurement lead time, the Purchaser legal prerequisites and power supply continuity;*** (vii) ***Warranty Defect Repair and Technical Support Service Sub-Plan, responding to the service levels of Section VII.***

ITP 16.3	In the interest of effective integration, cost-effective technical support, and reduced re-training and staffing costs, Proposers shall offer the following items: *the open standards listed in Section VII, in particular OpenID Connect, OAuth 2.0, the credential format selected under SAM-ARC-027, OpenID4VCI and OpenID4VP, and ISO/IEC 19794 and ISO/IEC 39794 for biometric data interchange. No brand name or model is imposed.*
ITP 17.2	The Proposer *must* propose Recurrent Cost Items *They cover support, maintenance and updates, card personalisation consumables and the post acceptance service levels of Section VII, quoted per year in the Recurrent Cost Schedules for two (2) years of post acceptance support for each release, with years three and four quoted separately as options.*
ITP 17.2	The Proposer *must not* propose for contracts for Recurrent Cost Items not included in the main Contract.
ITP 17.5	The Incoterms edition is: *Incoterms 2020.*
ITP 17.5 (a)	Named place of destination is: *SBS Premises, Apia, Samoa*
ITP 17.6	Named place of final destination (or Project site) is: *each of the sites listed in the Site Table of Section VII: the SBS building in Apia, being the main server room and the supervision cell; the Apia card personalisation centre; the Apia registration, adjudication and investigation offices; the Salelologa site on Savai'i; the Vodafone data centre acting as the disaster recovery site; and the itinerant enrolment sites on Upolu and Savai'i.*
ITP 17.8	ITP 17.8 is modified as follows: *There are no modifications to ITP 17.8*
ITP 17.9	The prices quoted by the Proposer *shall not* be subject to adjustment during the performance of the Contract.
ITP 18.1	The Proposer *is* required to quote in the currency of the Purchaser's Country the portion of the Proposal price that corresponds to expenditures incurred in that currency. *The currency of the Purchaser's Country is the Samoan Tala (WST).* Note: this quote-currency requirement is distinct from the evaluation currency; for evaluation purposes, all Proposal prices are converted to USD in accordance with ITP 36.2.
ITP 19.1	The Proposal shall be valid until: 1 June 2027.
ITP 19.3 (a)	The Proposal price shall be adjusted by the following factor(s): *not applicable*

ITP 20.1	A *Proposal Security shall not be* required. A Proposal-Securing Declaration *shall be* required. Any proposal not accompanied by a signed Proposal-Securing Declaration shall be rejected by the Purchaser as non-responsive.
ITP 20.3 (d)	Other types of acceptable securities: *None*
ITP 20.9	If the Proposer performs any of the actions prescribed in ITP 20.9 (a) or (b), the Purchaser will declare the Proposer ineligible to be awarded contracts by the Purchaser for a period of *two (2)* years starting from the date the Proposer performs any of the actions.
ITP 21.3	The written confirmation of authorization to sign on behalf of the Proposer shall consist of: *a power of attorney, or a resolution of the board of directors or equivalent governing body, naming the signatory and stating the extent of the authority, signed and dated within the twelve months preceding the deadline for submission; and, for a joint venture, the joint venture agreement or a letter of intent to form a joint venture signed by all members, naming the lead member and authorising it to sign, incur obligations and receive instructions on behalf of all members*
D. Submission and Opening of Proposals	
ITP 22.1	In addition to the original of the Proposal, the number of copies is: none. Proposals are submitted only through the Government of Samoa e-Tendering Portal, and the files uploaded constitute the original. The files uploaded shall be in PDF generated directly from the source files, not scanned from paper, so that the text is searchable. The Technical Responsiveness Checklist workbook is uploaded in its spreadsheet format with the Technical Part.
ITP 23.1	For Proposal submission purposes only, the Purchaser's address is: Attention: *Ministry of Finance, Tenders Board Secretary* Street Address: *Central Bank of Samoa Building, 02 Apia City Boulevard* Floor/Room number: *Level 4* City: *Apia* Postal Code: *not applicable* Country: *Samoa* The deadline for Proposal submission is:

	Date: *21 December 2026* Time: *11:00 a.m., Samoan time* The deadline is set eight (8) weeks after the date of issue of this request for proposals. Proposers *shall submit their Proposals electronically, only via the Government of Samoa (GoS) e-Tendering Portal Link: https://portal.tenderlink.com/mof_samoa/login*. The electronic bid submission procedures shall be: as set as in and through the Government of Samoa (GoS) e-Tendering Portal which is administered and managed by the Ministry of Finance and can be accessed via the link: https://portal.tenderlink.com/mof_samoa/. Any procurement notices, minutes to the Prebid meeting, clarifications and/or addenda/addendum will be published on the e-portal before the closing date. The e-portal shall automatically expire on the submission deadline, as specified in this ITP. The request for proposals is published on the portal in two separate e-tender boxes, one for the Technical Part and one for the Financial Part. A Proposer submitting through the portal shall upload the Technical Part in the e-tender box for technical proposals and the Financial Part in the e-tender box for financial proposals, as two separate submissions. A Proposal that combines both Parts in a single submission, or that places any element of the Financial Part in the e-tender box for technical proposals, does not comply with ITP 22 and shall be rejected.

E. Public Opening of Technical Parts of Proposals	
ITP 26.1	The Proposal opening shall take place at: Street Address: *Ministry of Finance, Level 4, Central Bank of Samoa Building, 02 Apia City Boulevard* Floor/Room number: *Floor 4, Conference room* City : *Apia* Country: *Samoa* Date: *21 December 2026* Time: *11:10 a.m., Samoan time*
ITP 26.1	The electronic Proposal opening procedures shall be: as procedure set out in the Government of Samoa (GoS) e-Tendering Portal via link *https://portal.tenderlink.com/mof_samoa/login* The Proposal opening is conducted by the Procurement Division of the Ministry of Finance, as Administrator of the Government of Samoa e-Tendering Portal.

	The portal closes automatically at the deadline for Proposal submission. The electronic keys giving access to the e-tender boxes are issued by the portal to the Procurement Division upon that deadline and not before, and are unique to this procurement. The e-tender box for technical proposals is opened on the submission deadline. The e-tender box for financial proposals remains sealed and unopened until the opening of Financial Parts under ITP 33. Technical Parts received through the portal are opened and read out in the same session, in the presence of the Tenders Board Sub-Committee, the representatives of the Purchaser and the Proposers who attend. The Purchaser may make a videoconference link available so that Proposers may attend the opening remotely. Attendance, in person or by videoconference, is not compulsory and is at the Proposer's own cost. Minutes of the Technical Part opening shall be shared with all Proposers by email.
	G. Evaluation of Technical Part of Proposals
ITP 32.2	The weighting to be given for Rated Criteria (including technical and non-price factors) is: *seventy percent (70 %)* The technical factors (including sub-factors if any), which for purposes of this document carry the same meaning as Rated Criteria, and the corresponding weight out of 100% are: Technical Factor — Weight in percentage A. Technical and functional solution — 30 B. Enrolment operations — 15 C. Card, credentials and production chain — 15 D. Skills transfer, capacity building and local anchoring — 20 E. Preliminary Project Plan — 10 F. Key personnel

	10 Total 100 The technical proposal scoring methodology is specified in Section III-Evaluation and Qualification Criteria. The qualification requirements of Section III, part 1 (Qualification), are assessed on a pass or fail basis and are not scored. A Proposer that fails any of them is rejected, whatever its technical score. A Proposal shall be considered further only if it obtains a total technical score of at least sixty (60) points out of one hundred (100), and, in each of the six rated categories A to F, a score of at least fifty percent (50 %) of the points available for that category. A Proposal that fails either condition shall not be considered further and its envelope marked Financial Part shall be returned unopened. The mandatory requirements whose satisfaction conditions a determination of substantial responsiveness under both ITP 30 and Section III, paragraph 2.1 are those listed in Section III, paragraph 2.1, which states that list to be complete in itself. A deviation on a requirement that is not identified as mandatory is not in itself a ground for a determination of non responsiveness: it is scored under the rated criteria. The sub factors within each category, their points and the scoring method are specified in Section III. The rated criteria include the method statement, management strategies and implementation plans to manage cyber security risks.
H. Notification of Evaluation of Technical Parts and Public Opening of Financial Parts	
ITP 33.8	The representatives of the Purchaser conducting Proposal opening are the members of the Tenders Board Sub-Committee, which acts on behalf of the Government of Samoa. The Letter of Proposal – Financial Part and the Price Schedules shall be initialed by the members of the Tenders Board Sub-Committee attending the opening of Financial Parts. The read out prices and any discounts shall be recorded in the opening record, signed by the attending members of the Tenders Board Sub-Committee. The opening of Financial Parts is broadcast by videoconference. The connection link is prepared by the Samoa Bureau of Statistics and made available to Proposers who so request.
I. Evaluation of Financial Part of Proposals	
36.1(f)	The adjustments shall be determined using the following criteria, from amongst those set out in Section III, Evaluation and Qualification Criteria: (a) Deviation in Time for Completion: ***No;***

	(b) Present value of Recurrent Costs ***: Yes, discounted over two (2) years of post acceptance support at the discount rate stated for ITP 39.1, by the method set out in Section III;*** (c) Functional Guarantees of the Facilities ***: No*** (d) Work, services, facilities, etc., to be provided by the Purchaser ***Yes, for training only. The Purchaser makes available the training facilities described at item 0.5 of Section VII.;***
ITP 36.2	The currency(ies) of the Proposal shall be converted into a single currency as follows: *United States Dollars (USD)* The currency that shall be used for Proposal evaluation and comparison purposes to convert all Proposal prices expressed in various currencies into a single currency is: *United States Dollars (USD)* The source of exchange rate shall be: *the selling rate published by the Central Bank of Samoa.* The date for the exchange rate shall be: *the deadline for submission of Proposals.* Note: this evaluation-currency conversion is distinct from the quote-currency requirement at ITP 18.1, which requires the local-expenditure portion of the Proposal price to be quoted in Samoan Tala (WST); the two requirements are complementary.
J. Evaluation of Combined Technical and Financial Parts and Most Advantageous Proposal	
ITP 39.1	The weight to be given for cost is: 0.30 (thirty percent), the weight given to the total technical score being 0.70 (seventy percent). Discount Rate (I) for net present value calculations of recurrent costs (if any) is *six (6)* percent per annum.
ITP 39.2	Best And Final Offer (BAFO) does not apply.
ITP 39.5	Negotiation does not apply.
ITP 39.9	As additional qualification measures, the Information System (or components/parts of it) offered by the Proposer with the Most Advantageous Proposal may be subjected to the following tests and performance benchmarks prior to Contract award*:* *The Information System offered by the Proposer with the Most Advantageous Proposal may be subjected, before Contract award, to a demonstration of the card production chain limited to the security features of the card. The Proposer shall present physical card samples produced on the equipment and with the materials it has offered, and shall demonstrate that the security features offered are present, reproducible and not proprietary, meaning that the Purchaser can obtain them from more than one supplier at the end of the Contract. The demonstration is conducted by the evaluation committee, assisted by its*

	technical adviser, at the Purchaser premises in Apia or by videoconference with the samples sent in advance, at the option of the Purchaser. It lasts no more than one working day and the Purchaser gives at least ten (10) days notice. No price information shall be presented, requested or discussed at the demonstration. The demonstration verifies the conformity of what was offered in the Technical Part, does not change the technical score and shall not be used to introduce any change to the Proposal. It is successful if the samples carry the security features stated in the Technical Part and the Proposer evidences that each of them can be sourced from at least two suppliers. If it is not successful the Purchaser may reject the Proposal and proceed to the next ranked Proposal. No other test, benchmark or reference site visit applies.
K. AWARD OF CONTRACT	
ITP 44	The maximum percentage by which quantities may be increased is: *fifteen percent (15 %)* The maximum percentage by which quantities may be decreased is: *fifteen percent (15 %)* The items for which the Purchaser may increase or decrease the quantities are the following. *(a) enrolment equipment, kits and tablets; (b) the number of persons to register and the associated enrolment operations support and consumables; (c) the number of National ID Cards and the associated personalisation consumables, the baseline being two hundred and fifty thousand (250,000) cards delivered once; (d) card production and delivery sites, print and quality control stations, the Salelologa production line remaining a separately priced option not affected by this clause; (e) civil registration offices and registration points. The variation applies item by item and in the aggregate, is exercised once at the time of Contract award, and is given effect through the Unit Rates Schedule.*
ITP 49	The proposed Adjudicator is: ***To be appointed by mutual agreement between the Purchaser and the Contractor during contract finalization. The hourly rate shall also be agreed upon during these same contract finalization. If an adjudicator is not agreed upon, the Appointing Authority designated in the SCC shall make the appointment upon request of either party. Adjudicator fees and expense shall be shared equally (50/50) between parties.***
ITP 50.1	The procedures for making a Procurement-related Complaint are detailed in the "Procurement Regulations for IPF Borrowers (Annex

	III).” A Procurement-related Complaint may challenge any of the following: 1. The terms of the request for proposals document; 2. the Purchaser’s decision to exclude a Proposer from the procurement process prior to the award of contract; and 3. The Purchaser’s decision to award the contract. If a Proposer wishes to make a Procurement-related Complaint, the Proposer should submit its complaint following these procedures, in writing (by the quickest means available, that is either by email or fax), to: For the attention: Mr. *Leota Aliielua Salani* Title/position: *Government Statistician (GS)* Purchaser: Government of Samoa, acting through the Samoa Bureau of Statistics Email address*: nid@sbs.gov.ws* Fax number: *Not applicable* A copy of the complaint can be sent for the Bank’s information and monitoring to: **procurementcomplaints@worldbank.org**

SECTION III - EVALUATION AND QUALIFICATION CRITERIA (WITHOUT PREQUALIFICATION)

This Section contains all the criteria that the Purchaser shall use to evaluate Proposals and qualify Proposers. No other factors, methods or criteria shall be used. The Proposer shall provide all the information requested in the forms included in Section IV, Proposal Forms.

1. Qualification

1.1 Qualification Requirements

The Proposer's qualification shall be assessed in accordance with the Qualification table included in this section.

1.2 Financial Resources

Using the relevant Form, FIN 1.3.3 in Section IV, Proposal Forms, the Proposer must demonstrate access to, or availability of, financial resources such as liquid assets, unencumbered real assets, lines of credit, and other financial means, other than any contractual advance payments to meet:

(i) the following cash-flow requirement: USD 1,500,000 (one million five hundred thousand United States Dollars), net of the Proposer's other contractual commitments, as stated in the Qualification table, sub factor 1.3.3;

and

(ii) the overall cash flow requirements for this contract and its current supply and services' commitment.

1.3 Key Personnel

The Proposer must demonstrate that it will have suitably qualified key personnel. The Proposer shall complete the relevant Forms in Section IV, Proposal Forms. The Contract has been assessed as presenting cyber security risks and **the Key Personnel include a Cyber Security and Data Protection Expert. The six key positions, the reference experience that scores 2 under criterion F and the elements valued in the score are the following:**

#	Position	Reference experience (score 2 under criterion F)	Valued in the score	Sub weight
1	Project Manager (dedicated)	10 years, including 2 identity or government IS projects of comparable size	Degree in a relevant field; PMP, PRINCE2 or equivalent project management certification	2

2	ID Solution Architect and Biometrics / ABIS Specialist	10 years, including 8 years in biometrics and at least 2 similar projects, one of them with a national ABIS deployment; demonstrated open standards (OIDC, digital credential formats). A similar project is the design or integration of a national identity or civil registration system	Degree in computer science or a related field	2.5
3	Cyber Security and Data Protection Expert	8 years, including securing a system holding sensitive data and 1 DPIA of an identity or health system	Recognised security certification (CISSP, CISM, ISO 27001 LA or equivalent); legal training or DPO certification; critical infrastructure experience	1.5
4	Enrolment Operations Manager	8 years of field operations, including 1 mass enrolment campaign	Degree	1
5	Card Personalisation Manager	8 years in secure document personalisation, including 1 set up of a production centre	Technical degree	1
6	Deputy Local Project Manager (dedicated, based in Samoa for the whole duration of the Contract)	5 years, including at least 1 experience in project management of a digital project; fluent English	Degree; project management certification; being a staff member of the member established in Samoa	2

Scope of the Deputy Local Project Manager. Deputy to the Project Manager on site. Leads local capacity building and acts as Training and Skills Transfer Lead: training plan, delivery of training, transfer of skills to the Purchaser and to the local ecosystem, and evidence of what stays after the Contract. Mobilised from the Effective Date to the end of the support period. Based in Samoa refers to the place of work, never to nationality. Replacement is subject to the approval of the Purchaser (Special Conditions of Contract for GCC 9.20 (b)).

Reference experience, not a gate. The reference experience is the level that scores 2 under criterion F. Degrees and professional certifications are not minimum requirements for any position; they are taken into account in the score, above the reference. No position is pass or fail: a position left without a candidate scores zero under criterion F and is never a ground for rejection of the Proposal. Other experts of the Supplier's team, such as the integration engineer, are non key experts: their CVs are not requested at proposal stage, they are not evaluated, and they are never a ground for rejection of the Proposal.

Combination of positions. A candidate may be proposed for two positions at most, provided the time commitments of the two positions are compatible over the schedule. The Project Manager and the Deputy Local Project Manager are dedicated positions and are not combined with another. The typical combination is the Enrolment Operations Manager with the Card Personalisation Manager. The Cyber Security and Data Protection Expert is not combined with the ID Solution Architect and Biometrics / ABIS Specialist, so that the security review stays independent of the design. Each position is scored on its own under criterion F.

1.4 **Subcontractors/vendors/manufacturers**

Subcontractors/vendors/manufacturers for major items of supply or services identified in the prequalification document must meet or continue to meet the minimum criteria specified therein for each item.

Subcontractors for the following additional major items of supply or services must meet the following minimum criteria, herein listed for that item:

Item No.	Description of Item	Minimum Criteria to be met
1	No additional major item is specified.	Not applicable.

Failure to comply with this requirement will result in the rejection of the subcontractor.

1.5 Manufacturer's authorization

For all powered (active) hardware and/or software components of the Information System which the Proposer does not itself produce, by submission of documentary evidence in its Proposal, the Proposer must establish to the Purchaser's satisfaction that it is not prohibited to supply those components in the Purchaser's country under the Contract(s) that may result from this procurement.

(i) In the case of powered (active) hardware and other powered equipment, this must be documented by including Manufacturer's Authorizations in the Proposal (based on the sample found in the Sample Proposal Forms in Section IV.);

(ii) In the case of proprietary commercial software (i.e., excluding open source or "freeware" software) that the Proposer does not manufacture itself and for which the Proposer has or will establish an Original Equipment Manufacturer (OEM) relationship with the manufacture, the Proposer must provide Manufacture's Authorizations;

(iii) In the case of proprietary commercial software (i.e., excluding open source or "freeware" software) that the Proposer does not manufacture itself and for which the Proposer does not or will not establish an OEM relationship with the manufacturer, the Proposer must document to the Purchaser's satisfaction that the Proposer is not excluded from sourcing these items from the manufacturer's distribution channels and proposing offering these items for supply in the Borrower's Country.

(iv) In the case of open source software, the Proposer must identify the software item as open source and provide copies of the relevant open source license(s).

The Proposer is responsible for ensuring that the manufacturer or producer complies with the requirements of ITP 4 and ITP 5 and meets the minimum criteria listed above for that item.

For this Contract, this applies in particular to the biometric enrolment kits, the personalisation printers, the hardware security modules, the servers and storage, and the proprietary OEM software. Open source licences are attached with the Software List of the Intellectual Property Forms of Section IV.

1.6 Local Representative

In the case of a Proposer not doing business within the Purchaser's country, the Proposer shall submit documentary evidence in its Proposal to establish to the Purchaser's satisfaction that it is or will be (if awarded the Contract) represented by an agent in that country who is equipped and able to carry out / manage the Proposer's maintenance, technical support, training, and warranty repair obligations specified in the Purchaser's Requirements (including any response time, problem-resolution norms or other aspects that may be specified in the Contract).

Experience of delivery in a small or remote operating environment is described by the Proposer and taken into account under criterion D2, where the relevant capability is rated.

2. Technical Evaluation

2.1 Assessment of adequacy of Technical Proposal with Requirements in accordance with ITP 32.1

1. The requirements of Section VII listed below are mandatory. They are assessed pass or fail and they are not scored. A requirement passes where the Proposal meets it as written; a clarification that does not qualify the requirement does not prevent a pass. A requirement fails where the Proposal does not meet it, or meets it only in part: partial compliance is a fail in the same way as non compliance, and a conditional or qualified acceptance is a fail. A Proposal that fails one mandatory requirement shall be considered non responsive, and no score obtained under the rated criteria can compensate for that failure. A deviation on any other requirement of Section VII is not in itself a ground for a determination of non responsiveness: it is evaluated under the rated criteria of

Each mandatory requirement is stated in full in Section VII, which governs; the list below identifies them by reference and subject.

SAM-LEG-003. The Identity Database contains in digital form only the nine data items listed in section 27(3) of the Act.

SAM-LEG-004. The Identity Database contains no biometric data and no data directly identifying race, religion, ethnicity or language.

SAM-LEG-005. The Identity Database, the Biometric Database and the records of use of the authentication function are held separately, as required by section 38(4) of the Act.

SAM-IDM-018. Deduplication accuracy is expressed and contracted as measurable outcomes.

SAM-IDM-019. Deduplication throughput absorbs the daily intake of the mass enrolment wave as sized in VII.1.5.

SAM-IDM-020. The proportion of applications sent to manual adjudication that prove to be false duplicates is measured monthly and capped.

SAM-IDM-022. The SDIN is generated by a standalone, government controlled unique number generator delivered with its source code.

SAM-IDM-137. The Purchaser can operate, modify and replace each component without dependence on the Supplier, through the route stated in the Proposal for each component: delivery of the full source code; escrow for packaged software specific to the System; or, for the biometric identification system, the exit guarantees of SCC GCC 15.5.

SAM-CRD-025. The national identity card is a polycarbonate card without a chip, ID-1 format, no thicker than 0.76 mm, monoblock at end of manufacture, with non proprietary security features.

SAM-CRD-068. The blank cards supplied conform to the same construction and to the same security features.

SAM-ARC-022, read with SAM-LEG-029. The reference registries, the biometric data and the cryptographic keys remain hosted in Samoa, on infrastructure owned and controlled by the Purchaser, for the duration of the Contract.

SAM-ARC-027. Federation, authentication and consented data sharing implement OpenID Connect and OAuth 2.0; digital credentials held on the phone and presented online are issued in the families of SAM-CRD-002, the IETF SD-JWT VC and the ISO/IEC 18013-5 mobile document (mdoc); the signed QR code of the card follows SAM-CRD-046.

SAM-ARC-028. Biometric data is captured, stored and exchanged in the formats of ISO/IEC 19794 and ISO/IEC 39794, no proprietary format being the reference.

SAM-ARC-032. Interoperability between the components of the System relies on open, published standards.

SAM-ARC-033. The implemented standards are kept at current, supported versions throughout the Contract, with a standards roadmap.

SAM-CYB-001. The System is designed, implemented, documented and operated as Critical Information Infrastructure of Samoa.

SAM-TRF-001. The skills transfer brings the SBS teams to the point where they can operate, support, maintain and evolve the System.

SAM-INF-002. The hosting infrastructure supports all components of the System.

SAM-SLA-008. The ABIS operational accuracy service level is met.

A finding of failure on a mandatory requirement shall be recorded by reference to the passage of the Proposal relied on, and shall be confirmed by the evaluation committee as a whole.

The Technical Responsiveness Checklist issued with Section IV must be completed and returned by the Proposer. Failure to do so increases significantly the risk that the Technical Part will be declared technically non responsive. It is a supporting document for the evaluation and is not itself a scoring mechanism, and the list above is complete in itself.

Points 2 to 6 below recall features that the mandatory requirements above and the rated criteria already cover; they add no pass or fail condition. Point 7 is the minimum technical score, also stated in the Proposal Data Sheet.

2. Card: chipless polycarbonate; non proprietary security features demonstrated in the proposal (SAM-CRD, model clause C.1.7); card personalisation operated locally at the Apia production site of the base scope, the design allowing the second production line at Salelologa to be installed if the option is exercised.

3. Architecture: IDMS and IDVS separated; 1:1 performed by the IDVS; three separate databases (NDID Act s.38(4)); documented open APIs; compliance with the standards of VII.1.3 (OIDC, OAuth 2.0, IETF SD-JWT VC and ISO/IEC 18013-5 mdoc, OpenID4VCI/VP, ISO/IEC 19794/39794).

4. Cyber security risk management plan present (PDS 11.2(j)).

5. Response to the capacity building annex present (preliminary transfer plan).

6. SDIN generator proposed as a standalone component with a commitment to deliver the source code.

7. Minimum overall technical score: 60/100; no category score from A to F strictly below 50 % of its weight. This threshold and these floors are also stated in the Proposal Data Sheet.

2.2 Technical Evaluation (ITP 32.2)

The technical features to be evaluated are generally defined below and specifically identified in the PDS:

(i) to which extent that the performance, capacity, or functionality features meet or exceed the levels specified in the performance / functional requirements and/or influence the life-cycle cost and effectiveness of the Information System;

(ii) usability features, such as ease of use, ease of administration, or ease of expansion, which influence the life-cycle cost and effectiveness of the Information System;

(iii) quality of the Proposer's Preliminary Project Plan as evidenced by the thoroughness, reasonableness, and responsiveness of: (a) the task and resource schedules, both general and specific, and (b) the proposed arrangements for management and coordination, training, quality assurance, technical support, logistics, problem resolution, and transfer of

knowledge, and other such activities as specified by the Purchaser or proposed by the Proposer based on the Proposer's experience;

(iv) Any sustainable procurement requirement if specified in Section VII- Requirements of the Information System.

The total technical points assigned to each Proposal in the Evaluated Proposal Formula will be determined by adding and weighting the scores assigned by an evaluation committee to technical features of the Proposal **in accordance with the PDS** and the scoring methodology below.

The technical factors (categories), their features and their points out of one hundred (100) are the following. The weight of each category is its total of points.

SPD scale per feature: 0 absent, 1 present with deficiencies, 2 compliant, 3 marginally exceeds, 4 significantly exceeds. Each level converts into a share of the points of the feature: 0 percent for level 0, 30 percent for level 1, 60 percent for level 2, 80 percent for level 3 and 100 percent for level 4. Category score = sum of the feature points obtained, scaled to the category weight. **Overall technical weight 70 %** in the combined evaluation.

Cat.	Feature	Points
A. Technical and functional solution		**30**
A1	Enrolment functional coverage (including family enrolment in a single visit, minors without biometrics, offline mode)	4
A2	IDMS and ABIS: approach, quantified FPIR and FNIR and throughput commitments, adjudication	4
A3	IDVS and relying party management: privacy by design partitioning (individual encryption), 1:1 in the IDVS, RP application owned by SBS, billing through an established ERP or billing platform, open source or commercial, pluggable (SAM-IDV-079), the invoicing chain itself being an option (SAM-IDV-074)	5
A4	CRVS DPI: 3 components, interoperability gateway, digital only, stock V1 / flow V2	4
A5	Credentials: digital first VC, wallet + cloud wallet, signed QR verifiable offline	4
A6	Assurance levels framework: configurable mechanism, alignment with Policy Annex A	3
A7	Architecture and ICT Infrastructure component: separations, PKI trust services consumed by all components (SAM-INF-040 to 048), central supervision and monitoring platform covering the whole System, power protection, reversibility, absence of lock in, standalone SDIN generator	4
A8	Security by design and critical infrastructure readiness (including the proposal's cyber plan)	2
B. Enrolment operations		**15**
B1	Deployment plan for 50 kits + 10 tablets, two island logistics	4

B2	Commitment on kit delivery lead time (the number one schedule lever)	4
B3	Operator training, throughput and quality in real conditions	3
B4	CRVS preloading approach and exception handling	2
B5	Offline robustness and synchronisation	2
C. Card, credentials and production chain		**15**
C1	Quality of the proposition against the requirements, and the card and consumables economy: construction, consumable consumption, reject rate and the design choices that keep the personalised unit cost within the Purchaser target of USD 2 at the contract volume, demonstrated without stating any price in the Technical Part	4
C2	Demonstration of the non proprietary security features (samples, proof of reproducibility)	4
C3	Local production autonomy plan (the Apia production site of the base scope, the Salelologa line if the option is exercised, progressive transition to local operation)	4
C4	Quality of the signed QR and of offline verification; 10 year durability proven	3
D. Skills transfer, capacity building and local anchoring		**20**
D1	Quality of the response to the annex: plan, pairing, target depth per role, immersion, knowledge base	6
D2	Quality and credibility of the in country support arrangement: on site response times, staff based in Samoa, local spare parts holding, and the support capability that remains in Samoa after the contract. Any arrangement may score in full (a local branch of the Proposer, a Local Entity or a subcontractor). No points are given for nationality, ownership or length of establishment.	5
D3	Client repo + CI practice, acceptance through deployment by SBS	4
D4	Relying party pilot and 5 co developed use cases	3
D5	Exit, reversibility and living documentation	2
E. Preliminary Project Plan		**10**
E1	Realism of the schedule against milestones M1 to M12 of the Implementation Schedule, including the sixty thousand persons enrolled and processed before 31 December 2027, and the final skills transfer assessment.	4
E2	Risk management (kit lead time, regulatory prerequisites, power)	3
E3	Testing and quality plan; migration plan	3
F. Key personnel		**10**
F1 to F6	Scoring of the six key personnel against the reference experience of 1.5, each position on its own sub weight: Project Manager 2, ID Solution Architect and Biometrics / ABIS	10

	Specialist 2.5, Deputy Local Project Manager 2, Cyber Security and Data Protection Expert 1.5, Enrolment Operations Manager 1, Card Personalisation Manager 1, ten points in total. Degrees and certifications count above the reference experience. A candidate proposed for two positions is scored under each.	
Total		**100**

Mapping of the Rated Criteria to the requirement families of Section VII

Rated Criterion (weight)	Requirement families of Section VII covered (SAM-* codes)	Where stated in Section VII
A. Technical and functional solution (30)	SAM-LEG, SAM-IDM, SAM-IDV, SAM-CRV, SAM-ARC, SAM-ADM, SAM-PER, SAM-CYB, SAM-INF; SAM-ENR-001 to 070 for the enrolment functional coverage scored at feature A1; the digital credential requirements of SAM-CRD scored at feature A5	VII.1 B, 1.1, 1.2.1, 1.2.2, 1.2.3, 1.2.4, 1.2.6, 1.3, 1.4, 1.5 and 1.6; VII.1 D (ICT Infrastructure component)
B. Enrolment operations (15)	SAM-ENR-071 to 144 (kit composition, ultra mobile tablets, central enrolment services, deployment and logistics, spares and maintenance, fleet delivery commitment); SAM-SVC for data migration and preloading; SAM-PER for enrolment throughput	VII.1 D (Enrolment kits and central enrolment services); VII.1 C, 2.5; VII.1 B, 1.5
C. Card, credentials and production chain (15)	SAM-CRD-001 to 092 (card body and security features, card data content and layout, personalisation chain, signed QR and offline verification, durability); SAM-TST for card chain acceptance	VII.1 B, 1.2.4; VII.1 E, 4.9
D. Skills transfer, capacity building and local anchoring (20)	SAM-TRF-001 to 040; SAM-SVC for training delivery, documentation and the Supplier's team; SAM-ARC-038 to 040 for reversibility and exit	VII.1 C, Annex to 2.4; VII.1 C, 2.4, 2.6 and 2.7; VII.1 B, 1.3
E. Preliminary Project Plan (10)	SAM-SVC (analysis and detailed design, development and integration, project management, warranty and post acceptance support); SAM-TST (test strategy, performance, security, disaster recovery and acceptance testing); SAM-SLA; the Implementation Schedule	VII.1 C, 2.0 to 2.3, 2.8 and 2.9; VII.1 E; VII.1 F; VII.2 (a)
F. Key personnel (10)	The six key personnel positions and their reference experience; SAM-SVC for the composition of the Supplier's team	Section III, 1.5; VII.1 C, 2.7

Technical proposal scoring methodology

(a) During the evaluation process, the evaluation committee will assign each desirable/preferred feature a whole number score from 0 to 4, where 0 means that the feature is absent, and 1 to 4 either represent predefined values for desirable features amenable to an objective way of rating (as is the case for, e.g., extra memory, or extra mass storage capacity, etc., if these extras would be conducive for the utility of the system), or if the feature represents a desirable functionality (e.g., of a software package) or a quality improving the prospects for a successful implementation (such as the strengths of the proposed project staff, the methodology, the elaboration of the project plan, etc., in the proposal), the scoring will be 1 for the feature being present but showing deficiencies; 2 for meeting the requirements; 3 for marginally

exceeding the requirements; and 4 for significantly exceeding the requirements.

(b) The score for each feature (i) within a category (j) will be combined with the scores of features in the same category as a weighted sum to form the Category Technical Score using the following formula:

$$S_j \equiv \sum_{i=1}^{k} t_{ji} * w_{ji}$$

where:

t_{ji} = the technical score for feature "i" in category "j"

w_{ji} = the weight of feature "i" in category "j"

k = the number of scored features in category "j"

and $\sum_{i=1}^{k} w_{ji} = 1$

(c) The Category Technical Scores will be combined in a weighted sum to form the total Technical Proposal Score using the following formula:

$$T \equiv \sum_{j=1}^{n} S_j * W_j$$

where:

S_j = the Category Technical Score of category "j"

W_j = the weight of category "j" as specified in the PDS

n = the number of categories

and $\sum_{j=1}^{n} W_j = 1$

3. Technical alternatives

If invited in accordance with ITP 13.4, will be evaluated as follows: *none*

4. Financial Evaluation

The following factors and methods will apply:

(a) Time Schedule:

The number of weeks, from the effective date specified in Article 3 of the Contract Agreement, to achieve Operational Acceptance must be no more than: ***the weeks stated in the Implementation Schedule of Section VII for each Operational Acceptance, that is thirty six (36) weeks for release V1 (milestone M4) and seventy (70) weeks for release V2 (milestone M8)***.

A Proposal offering to achieve Operational Acceptance earlier than the maximum number of weeks *shall not* be given credit for proposal evaluation purposes.

(b) Recurrent Costs

Since the operation and maintenance of the system being procured form a major part of the implementation, the resulting recurrent costs will be evaluated according to the principles given hereafter, including the cost of recurrent cost items for the initial period of operation stated below, based on prices furnished by each Proposer in Price Schedule Nos. 3.3 and 3.5.

The Recurrent Costs (R) are reduced to net present value and determined using the following formula:

$$R \equiv \sum_{X=1}^{N} \frac{R_x}{(1+I)^x}$$

where

N = number of years of evaluated recurrent costs

x = an index number 1, 2, 3, ... N.

R_x = total Recurrent Costs for year "x," as recorded in the Recurrent Cost Sub-Table.

I = discount rate to be used for the Net Present Value calculation, as specified **in the PDS for ITP 39.1.**

(c) Specific additional criteria

The relevant evaluation method, if any, shall be as follows:

Not Applicable

5. Combined Evaluation

The Purchaser will evaluate and compare the Proposals that have been determined to be substantially responsive.

An Evaluated Proposal Score (B) will be calculated for each responsive Proposal using the following formula, which permits a comprehensive assessment of the evaluated cost and the technical merits of each Proposal:

$$B \equiv \frac{Clow}{C} * X * 100 + \frac{T}{Thigh} * (1 - X) * 100$$

where

C = Evaluated Proposal Price

C_{low} = the lowest of all Evaluated Proposal Prices among responsive Proposals

T = the total Technical Score awarded to the Proposal

T_{high} = the Technical Score achieved by the Proposal that was scored best among all responsive Proposals

X = weight for the Cost as specified in the PDS

The Proposal with the best evaluated Proposal Score (B) among responsive Proposals shall be the Most Advantageous Proposal provided the Proposer was prequalified and/or it was found to be qualified to perform the Contract

1. Qualification

Factor	1.1 ELIGIBILITY					
Sub-Factor	Criteria					Documentation Required
	Requirement	Proposer				
		Single Entity	Joint Venture (existing or intended)			
			All members combined	Each member	At least one member	
1.1.1 Nationality	Nationality in accordance with ITP 4.4.	Must meet requirement	Must meet requirement	Must meet requirement	N / A	Form ELI –1.1 and 1.2, with attachments
1.1.2 Conflict of Interest	No- conflicts of interests as described in ITP 4.2.	Must meet requirement	Must meet requirement	Must meet requirement	N / A	Letter of Proposal
1.1.3 Bank Ineligibility	Not having been declared ineligible by the Bank as described in ITP 4.5.	Must meet requirement	Must meet requirement	Must meet requirement	N / A	Letter of Proposal
1.1.4 State owned Entity of the Borrower country	Compliance with conditions of ITP 4.6	Must meet requirement	Must meet requirement	Must meet requirement	N / A	Form ELI –1.1 and 1.2, with attachments

Factor	1.1 ELIGIBILITY					
Sub-Factor	Criteria					Documentation Required
	Requirement	Proposer				
		Single Entity	Joint Venture (existing or intended)			
			All members combined	Each member	At least one member	
1.1.5 United Nations resolution or Borrower's country law	Not having been excluded as a result of prohibition in the Borrower's country laws or official regulations against commercial relations with the Proposer's country, or by an act of compliance with UN Security Council resolution, both in accordance with ITP 4.8	Must meet requirement	Must meet requirement	Must meet requirement	N / A	Letter of Proposal

<table>
<tr><td>Factor</td><td colspan="6">1.2 HISTORICAL CONTRACT NON-PERFORMANCE</td></tr>
<tr><td rowspan="4">Sub-Factor</td><td colspan="5">Criteria</td><td rowspan="3">Documentation Required</td></tr>
<tr><td rowspan="3">Requirement</td><td colspan="4">Proposer</td></tr>
<tr><td rowspan="2">Single Entity</td><td colspan="3">Joint Venture (existing or intended)</td></tr>
<tr><td>All members combined</td><td>Each member</td><td>At least one member</td></tr>
</table>

1.2.1 History of non-performing contracts	Non-performance of a contract[1] did not occur as a result of Proposer's default since 1st January *2022*.	Must meet requirement by itself or as member to past or existing JV	N / A	Must meet requirement[2]	N / A	Form CON - 2
1.2.2 Suspension	Not under suspension based on execution of a Proposal Securing Declaration or Proposal Securing Declaration pursuant to ITP 4.7 and ITP 20.10	Must meet requirement	N / A	Must meet requirement	N / A	Letter of Proposal
1.2.3 Pending Litigation	All pending litigation shall in total represent not more than fifty percent (50%) of the Proposer's net worth.	Must meet requirement by itself or as member to past or existing JV	N / A	Must meet requirement	N / A	Form CON – 2
1.2.4 Litigation History	No consistent history of court/arbitral award decisions against the Proposer[3]since 1st January *2022*	Must meet requirement	Must meet requirement	Must meet requirement	N/A	Form CON – 2

[1] Nonperformance, as decided by the Purchaser, shall include all contracts where (a) nonperformance was not challenged by the contractor, including through referral to the dispute resolution mechanism under the respective contract, and (b) contracts that were so challenged but fully settled against the contractor. Nonperformance shall not include contracts where Purchaser decision was overruled by the dispute resolution mechanism. Nonperformance must be based on all information on fully settled disputes or litigation, i.e. dispute or litigation that has been resolved in accordance with the dispute resolution mechanism under the respective contract and where all appeal instances available to the applicant have been exhausted.

[2] This requirement also applies to contracts executed by the Applicant as JV member.

[3] The Proposer shall provide accurate information on the related Letter of Proposal about any litigation or arbitration resulting from contracts completed or ongoing under its execution over the last five years. A consistent history of awards against the Proposer or any member of a joint venture may result in failure of the Proposal.

1.2.5 Bank's SEA and/or SH Disqualification[4]	At the time of Contract Award, not subject to disqualification by the Bank for non-compliance with SEA/ SH obligations	Must meet requirement (including each subcontractor proposed by the Proposer)	N/A	Must meet requirement (including each subcontractor proposed by the Proposer)	N/A	Letter of Proposal, Form CON-3

Factor	1.3 FINANCIAL SITUATION					
Sub-Factor	Criteria					Documentation Required
	Requirement	Proposer				
		Single Entity	Joint Venture (existing or intended)			
			All members combined	Each member	At least one member	
1.3.1 Historical Financial Performance	Submission of audited balance sheets or if not required by the law of the Proposer's country, other financial statements acceptable to the Purchaser, for the last three (3) years to demonstrate the current soundness of the Proposers financial position and its prospective long term profitability.	Must meet requirement	N / A	Must meet requirement	N / A	Form FIN – 1.3.1 with attachments
1.3.2 Average Annual Turnover	Minimum average annual turnover of USD 8,000,000 (eight million United States Dollars), calculated as total certified payments received for contracts in progress or completed, within the last three (3) years	Must meet requirement	Must meet requirement	Must meet an amount at least equal to the annual value of the part of the Information System that the member executes	Must meet sixty percent (60%) of the requirement (the lead member)	Form FIN –1.3.2

Factor	1.3 FINANCIAL SITUATION					
Sub-Factor	Criteria					Documentation Required
	Requirement	Proposer				
		Single Entity	Joint Venture (existing or intended)			
			All members combined	Each member	At least one member	
				under the Joint Venture Agreement, which shall state the share of each member in value (ITP 11.2)		
1.3.3 Financial Resources	The Proposer must demonstrate access to, or availability of, financial resources such as liquid assets, unencumbered real assets, lines of credit, and other financial means, other than any contractual advance payments to meet the following cash-flow requirement: USD 1,500,000 (one million five hundred thousand United States Dollars), net of other contractual commitments.	Must meet requirement	Must meet requirement	N / A, the resources are assessed on all members combined	Must meet sixty percent (60%) of the requirement (the lead member)	Form FIN –1.3.3 and Form CCC

Factor	1.4 EXPERIENCE					
Sub-Factor	Criteria					Documentation Required
	Requirement	Proposer				
		Single Entity	Joint Venture (existing or intended)			
			All members combined	Each member	At least one member	
1.4.1 General Experience	Experience under Information System contracts in the role of supplier or integrator for at least five (5) years prior to the proposal submission deadline.	Must meet requirement	N / A	Must meet requirement	N / A	Form EXP-1.4.1
1.4.2 Specific Experience	Participation as supplier or integrator in at least two (2) contracts of national or sectoral biometric identity scope, each of a value of at least USD 3,000,000, successfully completed within the last eight (8) years. The required capabilities (enrolment, ABIS deduplication, credential issuance, identity card personalisation, handover of operations to the client) may be demonstrated across the two cited contracts taken together and across JV members, no single contract being required to cover the full chain alone. The successfully completed similar contracts shall be	Must meet requirement	Must meet requirements	N / A	Must meet the following requirement: the lead member must have delivered at least one of the cited contracts covering the enrolment and biometric core at national scale	Form EXP 1.4.2

Factor	1.4 EXPERIENCE					
Sub-Factor	Criteria					Documentation Required
	Requirement	Proposer				
		Single Entity	Joint Venture (existing or intended)			
			All members combined	Each member	At least one member	
	documented by a copy of an Operational acceptance certificate (or equivalent documentation satisfactory to the Purchaser) issued by the purchaser(s).					
1.4.3 Card Personalisation and Handover	At least one of the cited contracts covering identity card personalisation and at least one including a handover of operations to the client.	Must meet requirement	Must meet requirement	N / A	N / A	Form EXP 1.4.2
1.4.4 Local Support Capability	A Proposer not operating or registered in Samoa designates a local representative or local partner established in Samoa, with a real first level support capability: trained staff, a spare parts buffer with local storage, locally based technical staff, and customs and inter island logistics. The Local Entity shall be operating in Samoa at the proposal submission deadline, as evidenced by permanent staff based in Samoa, premises in	Must meet requirement	Must meet requirement	N / A	N / A	Description of the in country support arrangement proposed. No signed commitment from a local entity is required at proposal stage.

Factor	1.4 EXPERIENCE					
Sub-Factor	Criteria					Documentation Required
	Requirement	Proposer				
		Single Entity	Joint Venture (existing or intended)			
			All members combined	Each member	At least one member	
	Samoa, and at least one reference for information technology services delivered in Samoa. No minimum period of registration is required. The Proposal shall include a local capability plan for the Local Entity, stating its role, the staff assigned, the support services it delivers and the skills it acquires during the Contract; the plan is assessed on a pass or fail basis against these elements. The arrangement with the local representative or local partner is described in the Proposal. The signed commitment of that entity is a condition of award, furnished by the successful Proposer before the Contract is signed. The obligations themselves are set out in the Special Conditions of Contract, and the capability is also rated under criterion D2. Local Entity refers to a company, partnership or sole trader lawfully registered or licensed to do					

Factor	1.4 EXPERIENCE					
Sub-Factor	Criteria					Documentation Required
	Requirement	Proposer				
		Single Entity	Joint Venture (existing or intended)			
			All members combined	Each member	At least one member	
	business in Samoa, with an established place of business in Samoa, designated by the Proposer as its local representative or local partner. Evidence: for a company, its certificate of incorporation and a current extract of the Companies Registry (Ministry of Commerce, Industry and Labour); for a partnership or a sole trader, its current business licence (Ministry for Revenue), with the names of the partners for a partnership; in all cases, its taxpayer identification number (TIN) and proof of its business address in Samoa. A Local Entity engaged as subcontractor or local representative may support more than one Proposer; only a Local Entity that is a member of a Proposer's joint venture is limited to one Proposal (ITP 4.3).					

SECTION IV - PROPOSAL FORMS

Table of Forms

Letter of Proposal- Technical Part **77**

FORM ELI 1.1.1- PROPOSER INFORMATION FORM **80**

FORM ELI 1.1.2- PROPOSER'S JV MEMBERS INFORMATION FORM **82**

FORM CON – 2- HISTORICAL CONTRACT NON-PERFORMANCE, PENDING LITIGATION AND LITIGATION HISTORY **83**

FORM CON – 3 ..... **83**

SEXUAL EXPLOITATION AND ABUSE (SEA) AND/OR SEXUAL HARASSMENT PERFORMANCE DECLARATION **85**

FORM EXP 1.4.1- GENERAL EXPERIENCE **86**

FORM EXP 1.4.2- SPECIFIC EXPERIENCE **87**

FORM EXP 1.4.2 (CONT.)- SPECIFIC EXPERIENCE (CONT.) **88**

FORM CCC- SUMMARY SHEET: CURRENT CONTRACT COMMITMENTS / WORK IN PROGRESS **89**

FORM FIN 1.3.1- FINANCIAL SITUATION: HISTORICAL FINANCIAL PERFORMANCE **89**

FORM FIN 1.3.2- AVERAGE ANNUAL TURNOVER **91**

FORM FIN 1.3.3- FINANCIAL RESOURCES **92**

PERSONNEL CAPABILITIES- KEY PERSONNEL **93**

CODE OF CONDUCT FOR SUPPLIER'S PERSONNEL FORM **96**

TECHNICAL CAPABILITIES **100**

MANUFACTURER'S AUTHORIZATION **101**

SUBCONTRACTOR'S AGREEMENT **102**

INTELLECTUAL PROPERTY FORMS **104**

CONFORMANCE OF INFORMATION SYSTEM MATERIALS **107**

FORM OF PROPOSAL SECURITY (BANK GUARANTEE) **111**

FORM OF PROPOSAL SECURITY (PROPOSAL BOND) **113**

FORM OF PROPOSAL-SECURING DECLARATION **115**

PRICE SCHEDULE FORMS **119**

LETTER OF PROPOSAL- TECHNICAL PART

INSTRUCTIONS TO PROPOSERS: DELETE THIS BOX ONCE YOU HAVE COMPLETED THE DOCUMENT

The Proposer must prepare this Letter of Proposal on stationery with its letterhead clearly showing the Proposer's complete name and business address.

Note: All italicized text is to help Proposers in preparing this form.

Date of this Proposal submission: *[insert **date (as day, month and year) of Proposal submission**]*

RFP No.: *[insert **number of RFP process**]*

Alternative No.: *[insert **identification No if this is a Proposal for an alternative,** otherwise state **"not applicable"**]*

We, the undersigned, declare that:

To: *[insert **complete name of Purchaser**]*

(a) **No reservations:** We have examined and have no reservations to the request for proposals document, including Addenda issued in accordance with Instructions to Proposers (ITP 8);

(b) **Eligibility**: We meet the eligibility requirements and have no conflict of interest in accordance with ITP 4;

(c) **Proposal-Securing Declaration:** We have not been suspended nor declared ineligible by the Purchaser based on execution of a Proposal-Securing Declaration or Proposal-Securing Declaration in the Purchaser's Country in accordance with ITP 4.7;

(d) **Sexual Exploitation and Abuse (SEA) and/or Sexual Harassment (SH):** [*select the appropriate option from (i) to (v) below and delete the others. In case of JV members and/or subcontractors, indicate the status of disqualification by the Bank of each JV member and/or subcontractor]*.

We, including any of our subcontractors:

(i) [have not been subject to disqualification by the Bank for non-compliance with SEA/ SH obligations.]

(ii) [are subject to disqualification by the Bank for non-compliance with SEA/ SH obligations.]

(iii) [had been subject to disqualification by the Bank for non-compliance with SEA/ SH obligations, and were removed from the disqualification list. An arbitral award on the disqualification case has been made in our favor.]

(e) **Conformity:** We offer to provide design, supply and installation services in conformity with the request for proposals document of the following: [*insert a brief description of the IS Design, Supply and Installation Services*];

(f) **Proposal Validity:** Our Proposal shall be valid until *[insert day, month and year in accordance with ITP 19.1]*, and it shall remain binding upon us and may be accepted at any time before the expiration of that period;

(g) **Performance Security:** If our Proposal is accepted, we commit to obtain a Performance Security in accordance with the request for proposals document;

(h) **One Proposal Per Proposer:** We are not submitting any other Proposal(s) as an individual Proposer, and we are not participating in any other Proposal(s) as a Joint Venture member, and meet the requirements of ITP 4.3, other than alternative Proposals submitted in accordance with ITP 13;

(i) **Suspension and Debarment**: We, along with any of our subcontractors, suppliers, consultants, manufacturers, or service providers for any part of the contract, are not subject to, and not controlled by any entity or individual that is subject to, a temporary suspension or a debarment imposed by the World Bank Group or a debarment imposed by the World Bank Group in accordance with the Agreement for Mutual Enforcement of Debarment Decisions between the World Bank and other development banks. Further, we are not ineligible under the Purchaser's Country laws or official regulations or pursuant to a decision of the United Nations Security Council;

(j) **State-owned enterprise or institution**: [*select the appropriate option and delete the other*: ***We are not a state-owned enterprise or institution*** / ***We are a state-owned enterprise or institution but meet the requirements of ITP 4.6***];

(k) **Commissions, gratuities and fees**: We have paid, or will pay the following commissions, gratuities, or fees with respect to the procurement process or execution of the Contract: *[insert* ***complete name of each Recipient, its full address, the reason for which each commission or gratuity was paid and the amount and currency of each such commission or gratuity****]*

Name of Recipient	Address	Reason	Amount

*[If none has been paid or is to be paid, indicate "****none****."]*

(l) **Binding Contract**: We understand that this Proposal, together with your written acceptance thereof included in your Letter of Acceptance, shall constitute a binding contract between us, until a formal contract is prepared and executed;

(m) **Not Bound to Accept:** We understand that you are not bound to accept the lowest evaluated cost Proposal, the Most Advantageous Proposal or any other Proposal that you may receive; and

(n) **Fraud and Corruption:** We hereby certify that we have taken steps to ensure that no person acting for us or on our behalf engages in any type of Fraud and Corruption.

Name of the Proposer: *[*insert* ***complete name of the Proposer****]*

Name of the person duly authorized to sign the Proposal on behalf of the Proposer: **[*insert* ***complete name of person duly authorized to sign the Proposal****]*

Title of the person signing the Proposal: *[insert* ***complete title of the person signing the Proposal****]*

Signature of the person named above: *[insert* ***signature of person whose name and capacity are shown above****]*

Date signed *[insert* ***number****]* day of *[insert* ***month****]*, *[insert* ***year****]*

*****: In the case of the Proposal submitted by joint venture specify the name of the Joint Venture as Proposer

**: Person signing the Proposal shall have the power of attorney given by the Proposer to be attached with the Proposal

FORM ELI 1.1.1- PROPOSER INFORMATION FORM

*[**Note**: The Proposer shall fill in this Form in accordance with the instructions indicated below. No alterations to its format shall be permitted and no substitutions shall be accepted.]*

Date: *[insert **date (as day, month and year) of Proposal submission***]

RFP No.: *[insert **number of Request for Proposals process**]*

Alternative No.: *[insert **identification No if this is a Proposal for an alternative]** otherwise state **"not applicable"***

Page _____ of_ _____ pages

1. Proposer's Name *[insert **Proposer's legal name**]*
2. In case of JV, legal name of each member : *[insert **legal name of each member in JV**]*
3. Proposer's actual or intended country of registration: *[insert **actual or intended country of registration**]*
4. Proposer's year of registration: *[insert **Proposer's year of registration**]*
5. Proposer's Address in country of registration: *[insert **Proposer's legal address in country of registration**]*
6. Proposer's Authorized Representative Information Name: *[insert **Authorized Representative's name**]* Address: *[insert **Authorized Representative's Address**]* Telephone/Fax numbers: *[insert **Authorized Representative's telephone/fax numbers**]* Email Address: *[insert **Authorized Representative's email address**]*
7. Attached are copies of original documents of *[check the box(es) of the attached original documents]* ☐ Articles of Incorporation (or equivalent documents of constitution or association), and/or documents of registration of the legal entity named above, in accordance with ITP 4.4. ☐ In case of JV, letter of intent to form JV or JV agreement, in accordance with ITP 4.1. ☐ In case of state-owned enterprise or institution, in accordance with ITP 4.6 documents establishing: ● Legal and financial autonomy ● Operation under commercial law ● Establishing that the Proposer is not under the supervision of the Purchaser

8. Included are the organizational chart, a list of Board of Directors, and the beneficial ownership. *[The successful Proposer shall provide additional information on beneficial ownership, using the Beneficial Ownership Disclosure Form.]*

FORM ELI 1.1.2- PROPOSER'S JV MEMBERS INFORMATION FORM

[The Proposer shall fill in this Form in accordance with the instructions indicated below. The following table shall be filled in for the Proposer and for each member of a Joint Venture].

Date: *[insert **date (as day, month and year) of Proposal submission***]

RFP No.: *[insert **number of Request for Proposals process**]*

Alternative No.: *[insert **identification No if this is a Proposal for an alternative,** otherwise state **"not applicable"**]*

Page _____ of_ _____ pages

1. Proposer's Name: *[insert **Proposer's legal name**]*
2. Proposer's JV Member's name: *[insert **JV's Member legal name**]*
3. Proposer's JV Member's country of registration: *[insert **JV's Member country of registration**]*
4. Proposer's JV Member's year of registration: *[insert **JV's Member year of registration**]*
5. Proposer's JV Member's legal address in country of registration: *[insert **JV's Member legal address in country of registration**]*
6. Proposer's JV Member's authorized representative information Name: *[insert **name of JV's Member authorized representative**]* Address: *[insert **address of JV's Member authorized representative**]* Telephone/Fax numbers: *[insert **telephone/fax numbers of JV's Member authorized representative**]* Email Address: *[insert **email address of JV's Member authorized representative**]*
7. Attached are copies of original documents of *[check the box(es) of the attached original documents]* ☐ Articles of Incorporation (or equivalent documents of constitution or association), and/or registration documents of the legal entity named above, in accordance with ITP 4.4. ☐ In case of a state-owned enterprise or institution, documents establishing legal and financial autonomy, operation in accordance with commercial law, and they are not under the supervision of the Purchaser in accordance with ITP 4.6. 8. Included are the organizational chart, a list of Board of Directors, and the beneficial ownership. *[The successful Proposer shall provide additional information on beneficial ownership for each JV member using the Beneficial Ownership Disclosure Form.]*

FORM CON – 2- HISTORICAL CONTRACT NON-PERFORMANCE, PENDING LITIGATION AND LITIGATION HISTORY

In case a prequalification process was conducted this form should be used only if the information submitted at the time of prequalification requires updating

Proposer's Legal Name: *[insert **Proposer's Legal Name**]*

Date: _____*[insert **date**]*

JV member Legal Name: *[insert **JV Member Legal Name**]*

RFP No.: *[insert **RFP number**]*

Page _____ of _____ pages

Non-Performed Contracts in accordance with Section III, Evaluation and Qualification Criteria			
☐ Contract non-performance did not occur since 1st January *2022* specified in Section III, Evaluation and Qualification Criteria, Sub-Factor 1.2.1. ☐ Contract(s) not performed since 1st January *2022* specified in Section III, Evaluation and Qualification Criteria, requirement 1.2.1			
Year	**Non-performed portion of contract**	**Contract Identification**	**Total Contract Amount (current value, currency, exchange rate and US$ equivalent)**
*[insert **year**]*	*[insert **amount and percentage**]*	Contract Identification: *[indicate **complete contract name/ number, and any other identification**]* Name of Employer: *[insert **full name**]* Address of Employer: *[insert **street/city/country**]* Reason(s) for nonperformance: *[indicate **main reason(s)**]*	*[insert **amount**]*
Pending Litigation, in accordance with Section III, Evaluation and Qualification Criteria			
☐ No pending litigation in accordance with Sub-Factor 1.2.3. ☐ Pending litigation in accordance with Sub-Factor 1.2.3 as indicated below.			

Year of dispute	**Amount in dispute (currency)**	**Contract Identification**	**Total Contract Amount (currency), USD**

			Equivalent (exchange rate)
*[specify **year**]*	*[specify **amount and currency**]*	Contract Identification: *[insert **Contract ID**]* Name of Employer: *[insert **Name of Employer**]* Address of Employer: *[insert **Address of Employer**]* Matter in dispute: *[describe **Matter of dispute**]* Party who initiated the dispute: *[specify **Initiator of dispute**]* Status of dispute: *[specify **Status of dispute**]*	*[specify **total contract amount and currency, USD equivalent and exchange rate**]*
*[specify **year**]*	*[specify **amount and currency**]*	Contract Identification: *[insert **Contract ID**]* Name of Employer: *[insert **Name of Employer**]* Address of Employer: *[insert **Address of Employer**]* Matter in dispute: *[describe **Matter of dispute**]* Party who initiated the dispute: *[specify **Initiator of dispute**]* Status of dispute: *[specify **Status of dispute**]*	*[specify **total contract amount and currency, USD equivalent and exchange rate**]*
Litigation History in accordance with Section III, Evaluation and Qualification Criteria			
☐ No Litigation History in accordance with Sub-Factor 1.2.4. ☐ Litigation History in accordance with Sub-Factor 1.2.4 as indicated below.			
Year of award	**Outcome as percentage of Net Worth**	**Contract Identification**	**Total Contract Amount (currency), USD Equivalent (exchange rate)**
*[specify **year**]*	*[specify **percentage of net worth**]*	Contract Identification: *[insert **Contract ID**]* Name of Employer: *[insert **Name of Employer**]* Address of Employer: *[insert **Address of Employer**]*	*[specify **total contract amount and currency, USD equivalent and exchange rate**]*

FORM CON – 3 - SEXUAL EXPLOITATION AND ABUSE (SEA) AND/OR SEXUAL HARASSMENT PERFORMANCE DECLARATION

[The following table shall be filled in by the Proposer, each member of a Joint Venture and each subcontractor proposed by the Proposer]

Proposer's Name: *[insert full name]*
Date: *[insert day, month, year]*
Joint Venture Member's or Subcontractor's Name: *[insert full name]*
RFP No. and title: *[insert RFP number and title]*
Page *[insert page number]* of *[insert total number]* pages

SEA and/or SH Declaration **in accordance with Section III, Qualification Criteria, and Requirements**
We: ☐ (a) have not been subject to disqualification by the Bank for non-compliance with SEA/ SH obligations ☐ (b) are subject to disqualification by the Bank for non-compliance with SEA/ SH obligations ☐ (c) had been subject to disqualification by the Bank for non-compliance with SEA/ SH obligations, and were removed from the disqualification list. An arbitral award on the disqualification case has been made in our favor.
[*If (c) above is applicable, attach evidence of an arbitral award reversing the findings on the issues underlying the disqualification.]*

FORM EXP 1.4.1- GENERAL EXPERIENCE

Proposer's Legal Name: *[insert **Proposer's Legal Name**]*

Date: *[insert **Date**]*

JV Member Legal Name: *[insert **JV Member Legal Name**]*

RFP No.: *[insert **RFP number**]*

Page _____ of _____ pages

Starting Month / Year	Ending Month / Year	Years *	Contract Identification	Role of Proposer
*[insert **month / year**]*	*[insert **month / year**]*	*[insert **number of years**]*	Contract name: *[insert **Name of Contract**]* Brief Description of the Information System performed by the Proposer: *[describe **Information System**]* Name of Purchaser: *[insert **Name of Purchaser**]* Address: *[insert **Address of Purchaser**]*	*[describe **role of Proposer under the contract**]*
*[insert **month / year**]*	*[insert **month / year**]*	*[insert **number of years**]*	Contract name: *[insert **Name of Contract**]* Brief Description of the Information System performed by the Proposer: *[describe **Information System**]* Name of Purchaser: *[insert **Name of Purchaser**]* Address: *[insert **Address of Purchaser**]*	*[describe **role of Proposer under the contract**]*
*[insert **month / year**]*	*[insert **month / year**]*	*[insert **number of years**]*	Contract name: *[insert **Name of Contract**]* Brief Description of the Information System performed by the Proposer: *[describe **Information System**]* Name of Purchaser: *[insert **Name of Purchaser**]* Address: *[insert **Address of Purchaser**]*	*[describe **role of Proposer under the contract**]*
*[insert **month / year**]*	*[insert **month / year**]*	*[insert **number of years**]*	Contract name: *[insert **Name of Contract**]* Brief Description of the Information System performed by the Proposer: *[describe **Information System**]* Name of Purchaser: *[insert **Name of Purchaser**]* Address: *[insert **Address of Purchaser**]*	*[describe **role of Proposer under the contract**]*

*List calendar year for years with contracts with at least nine (9) months activity per year starting with the earliest year

FORM EXP 1.4.2- SPECIFIC EXPERIENCE

Proposer's Legal Name: *[insert **Proposer's Legal Name**]*

Date: *[insert **Date**]*

JV Member Legal Name: *[insert **JV Member Legal Name**]*

RFP No.: *[insert **RFP number**]*

Page _____ of _____ pages

Similar Contract Number: ___ of ___ required.	**Information**		
Contract Identification	*[insert **Contract ID**]*		
Award date Completion date	*[insert **Date of Award*** *[insert **Date of Completion***		
Role in Contract	• Prime Supplier	• Management Contractor	• Subcontractor
Total contract amount			
If member in a JV or subcontractor, specify participation of total contract amount			
Purchaser's Name:	_____		
Address: Telephone/fax number: E-mail:	_____ _____ _____		

FORM EXP 1.4.2 (CONT.)- SPECIFIC EXPERIENCE (CONT.)

Proposer's Legal Name: *[insert **Proposer's Legal Name**]*

Date: *[insert **Date**]*

JV Member Legal Name: *[insert **JV Member Legal Name**]*

RFP No.: *[insert **RFP number**]*

Page _____ of _____ pages

Similar Contract No. *[insert **specific number**]* **of** *[**insert total number of contracts**]* **required**	**Information**
Description of the similarity in accordance with Sub-Factor 1.4.2 of Section III:	
Amount	*[insert **contract amount and currency and USD equivalent and exchange rate**]*
Geographical Scope	*[describe **geographic scope of the users of the information system**]*
Functional Scope	*[describe **the functionalities provided by the information system**]*
Methods/Technology	*[describe **methodologies and technologies used to implement the information system**]*
Key Activities	*[describe **the key activities of the Proposer under the contract**]*

FORM CCC- SUMMARY SHEET: CURRENT CONTRACT COMMITMENTS / WORK IN PROGRESS

[Proposers and each partner to a Joint Venture should provide information on their current commitments on all contracts that have been awarded, or for which a letter of intent or acceptance has been received, or for contracts approaching completion, but for which an unqualified, full completion certificate has yet to be issued.]

Proposer's Legal Name: *[insert **Proposer's Legal Name**]*

Date: *[insert **Date**]*

JV Member Legal Name: *[insert **JV Member Legal Name**]*

RFP No.: *[insert **RFP number**]*

Page _____ of _____ pages

Name of contract	Purchaser, contact address/tel./fax	Value of outstanding Information System (current US$ equivalent)	Estimated completion date	Average monthly invoicing over last six months (US$ equivalent/month)
1. *[insert **Name o Contract**]*	*[insert **Name of Purchaser, contact address, telephone / fax number**]*	*[insert **Total Outstanding Contract Value of the information system in USD equivalent and exchange rate**]*	*[insert **Estimated completion date**]*	*[insert **Average monthly invoices in USD equivalent and exchange rate**]*
2. *[insert **Name o Contract**]*	*[insert **Name of Purchaser, contact address, telephone / fax number**]*	*[insert **Total Outstanding Contract Value of the information system in USD equivalent and exchange rate**]*	*[insert **Estimated completion date**]*	*[insert **Average monthly invoices in USD equivalent and exchange rate**]*
3. *[insert **Name o Contract**]*	*[insert **Name of Purchaser, contact address, telephone / fax number**]*	*[insert **Total Outstanding Contract Value of the information system in USD equivalent and exchange rate**]*	*[insert **Estimated completion date**]*	*[insert **Average monthly invoices in USD equivalent and exchange rate**]*
...				

FORM FIN 1.3.1- FINANCIAL SITUATION: HISTORICAL FINANCIAL PERFORMANCE

To be completed by the Proposer and, if JV, by each member

Proposer's Legal Name: *[insert **Proposer's Legal Name**]*

Date: *[insert **Date**]*

JV Member Legal Name: *[insert **JV Member Legal Name**]*

RFP No.: *[insert **RFP number**]*

Page _____ of _____ pages

Financial information in US$ equivalent	**Historic information for previous** *[insert **number**]* **years** *(US$ equivalent in 000s)*						
	Year 1	**Year 2**	**Year 3**	**Year …**	**Year n**	**Avg.**	**Avg. Ratio**
Information from Balance Sheet							
Total Assets (TA)							
Total Liabilities (TL)							
Net Worth (NW)							
Current Assets (CA)							
Current Liabilities (CL)							
Information from Income Statement							
Total Revenue (TR)							
Profits Before Taxes (PBT)							

Attached are copies of financial statements (balance sheets, including all related notes, and income statements) for the years required above complying with the following conditions:

(a) Must reflect the financial situation of the Proposer or member to a JV, and not sister or parent companies
(b) Historic financial statements must be audited by a certified accountant
(c) Historic financial statements must be complete, including all notes to the financial statements
(d) Historic financial statements must correspond to accounting periods already completed and audited (no statements for partial periods shall be requested or accepted)

FORM FIN 1.3.2- AVERAGE ANNUAL TURNOVER

[To be completed by the Proposer and, if JV, by each member]

Proposer's Legal Name: *[insert **Proposer's Legal Name**]*

Date: *[insert **Date**]*

JV Member Legal Name: *[insert **JV Member Legal Name**]*

RFP No.: *[insert **RFP number**]*

Page _____ of _____ pages

Annual turnover data (applicable activities only)		
Year	Amount and Currency	US$ equivalent
*[insert **year**]*	*[insert **amount and currency**]*	*[insert **amount in USD equivalent and exchange rate**]*
*[insert **year**]*	*[insert **amount and currency**]*	*[insert **amount in USD equivalent and exchange rate**]*
*[insert **year**]*	*[insert **amount and currency**]*	*[insert **amount in USD equivalent and exchange rate**]*
*[insert **year**]*	*[insert **amount and currency**]*	*[insert **amount in USD equivalent and exchange rate**]*
*[insert **year**]*	*[insert **amount and currency**]*	*[insert **amount in USD equivalent and exchange rate**]*
*[insert **year**]*	*[insert **amount and currency**]*	*[insert **amount in USD equivalent and exchange rate**]*
*Average Annual Turnover	*[insert **amount and currency**]*	*[insert **amount in USD equivalent and exchange rate**]*

*Average annual turnover calculated as total certified payments received for work in progress or completed, divided by the number of years specified in Section III, Evaluation and Qualification Criteria, Sub-Factor 1.3.2.

FORM FIN 1.3.3- FINANCIAL RESOURCES

To be completed by the Proposer and, if JV, by each member

Proposer's Legal Name: *[insert **Proposer's Legal Name**]*

Date: *[insert **Date**]*

JV Member Legal Name: *[insert **JV Member Legal Name**]*

RFP No.: *[insert **RFP number**]*

Page _____ of _____ pages

Specify proposed sources of financing, such as liquid assets, unencumbered real assets, lines of credit, and other financial means, net of current commitments, available to meet the total cash flow demands of the subject contract or contracts as indicated in Section III, Evaluation and Qualification Criteria

Source of financing	Amount (US$ equivalent)
1. *[describe **type and source of available financing**]*	*[insert **amount of available financing in USD equivalent and exchange rate**]*
2. *[describe **type and source of available financing**]*	*[insert **amount of available financing in USD equivalent and exchange rate**]*
3. *[describe **type and source of available financing**]*	*[insert **amount of available financing in USD equivalent and exchange rate**]*
4. *[describe **type and source of available financing**]*	*[insert **amount of available financing in USD equivalent and exchange rate**]*

PERSONNEL CAPABILITIES- KEY PERSONNEL

To be completed by the Proposer and, if JV, by each member

Proposer's Legal Name: *[insert **Proposer's Legal Name**]*

Date: *[insert **Date**]*

JV Member Legal Name: *[insert **JV Member Legal Name**]*

RFP No.: *[insert **RFP number**]*

Page _____ of _____ pages

Proposers should provide the names and details of the suitably qualified Personnel to perform the Contract. The data on their experience should be supplied using the Form PER-2 below for each candidate.

The Proposer shall submit one Candidate Summary for each of the six key positions listed below, in this order, using the format of this form. The reference experience and the elements valued in the score for each position are stated in Section III 1.5. 1 Project Manager. 2 ID Solution Architect and Biometrics / ABIS Specialist. 3 Cyber Security and Data Protection Expert. 4 Enrolment Operations Manager. 5 Card Personalisation Manager. 6 Deputy Local Project Manager. A position left without a candidate is scored zero under evaluation criterion F. A candidate proposed for two positions, within the limits of Section III 1.5, is presented once per position, the second Candidate Summary referring to the first.

Key Personnel

1.	Title of position: *[insert **Title of position / role in team**]*	
	Name of candidate: *[insert **Name of Candidate**]*	
	Duration of appointment:	[*insert **the whole period (start and end dates) for which this position will be engaged***]
	Time commitment: for this position:	[*insert **the number of days/week/months/ that has been scheduled for this position***]
	Expected time schedule for this position:	[*insert **the expected time schedule for this position (e.g. attach high level Gantt chart***]
2.	Title of position: *[insert **Title of position / role in team**]*	
	Name of candidate: *[insert **Name of Candidate**]*	
	Duration of appointment:	[*insert **the whole period (start and end dates) for which this position will be engaged***]
	Time commitment: for this position:	[*insert **the number of days/week/months/ that has been scheduled for this position***]

	Expected time schedule for this position:	[*insert* ***the expected time schedule for this position (e.g. attach high level Gantt chart***]
3.	Title of position: **Cyber security Expert/s** ***[Include as required]***	
	Name of candidate: *[insert* ***Name of Candidate****]*	
	Duration of appointment:	[*insert* ***the whole period (start and end dates) for which this position will be engaged***]
	Time commitment: for this position:	[*insert* ***the number of days/week/months/ that has been scheduled for this position***]
	Expected time schedule for this position:	[*insert* ***the expected time schedule for this position (e.g. attach high level Gantt chart***]

Candidate Summary

To be completed by the Proposer and, if JV, by each member

Proposer's Legal Name: *[insert **Proposer's Legal Name**]*

Date: *[insert **Date**]*

JV Member Legal Name: *[insert **JV Member Legal Name**]*

RFP No.: *[insert **RFP number**]*

Page _____ of _____ pages

Position; *[insert **Title of Position**]*		Prime • Alternate
Candidate information	Name of candidate *[insert **Name Candidate**]*	Date of birth *[insert **Date of Birth**]*
	Professional qualifications *[describe **Professional qualifications**]*	
Present employment	Name of Employer *[insert **Name of Present Employer**]*	
	Address of Employer *[insert **Address of Present Employer**]*	
	Telephone *[insert **Telephone** of **Contact**]*	Contact (manager / personnel officer) *[insert **Name**]*
	Fax *[insert **fax of Contact**]*	email *[insert **email** of **Contact**]*
	Job title of candidate *[insert **Job Title Candidate**]*	Years with present Employer *[insert . **Number of years**]*

Summarize professional experience over the last twenty years, in reverse chronological order. Indicate particular technical and managerial experience relevant to the project.

From	To	Company/Project/ Position/Relevant technical and management experienc
*[insert **year**]*	*[insert **year**]*	*[describe **experience relevant to the proposed Contract under the RFP**]*
*[insert **year**]*	*[insert **year**]*	*[describe **experience relevant to the proposed Contract under the RFP**]*
*[insert **year**]*	*[insert **year**]*	*[describe **experience relevant to the proposed Contract under the RFP**]*
*[insert **year**]*	*[insert **year**]*	*[describe **experience relevant to the proposed Contract under the RFP**]*

CODE OF CONDUCT FOR SUPPLIER'S PERSONNEL

We are the Supplier, [*enter name of Supplier*]. We have signed a contract with [*enter name of Purchaser*] for [*enter description of the Information System*]. The Information System will be supplied to and installed at [*enter the Project Site/s]*. Our contract requires us to implement measures to address environmental and social risks.

Note to the Proposer:

The minimum content of the Code of Conduct form as set out by the Purchaser shall not be substantially modified. However, the Proposer may add requirements as appropriate, including to take into account Contract-specific issues/risks.

The Proposer shall initial and submit the Code of Conduct form as part of its proposal.

This Code of Conduct identifies the behavior that we require from Supplier's Personnel employed in the execution of the Contract at the Project Site/s.

Our workplace is an environment where unsafe, offensive, abusive or violent behavior will not be tolerated and where all persons should feel comfortable raising issues or concerns without fear of retaliation.

REQUIRED CONDUCT

Supplier's Personnel employed in the execution of the Contract at the Project Site/s shall:

1. carry out his/her duties competently and diligently;
2. comply with this Code of Conduct and all applicable laws, regulations and other requirements, including requirements to protect the health, safety and well-being of other Supplier's Personnel and any other person;
3. maintain a safe working environment including by:
    a. ensuring that workplaces, machinery, equipment and processes under each person's control are safe and without risk to health;
    b. wearing required personal protective equipment;
    c. using appropriate measures relating to chemical, physical and biological substances and agents; and
    d. following applicable emergency operating procedures.
4. report work situations that he/she believes are not safe or healthy and remove himself/herself from a work situation which he/she reasonably believes presents an imminent and serious danger to his/her life or health;
5. treat other people with respect, and not discriminate against specific groups such as women, people with disabilities, migrant workers or children;

6. not engage in any form of sexual harassment including unwelcome sexual advances, requests for sexual favors, and other verbal or physical conduct of a sexual nature with other Supplier's or Purchaser's Personnel;
7. not engage in Sexual Exploitation, which means any actual or attempted abuse of position of vulnerability, differential power or trust, for sexual purposes, including, but not limited to, profiting monetarily, socially or politically from the sexual exploitation of another;
8. not engage in in Sexual Abuse, which means the actual or threatened physical intrusion of a sexual nature, whether by force or under unequal or coercive conditions;
9. not engage in any form of sexual activity with individuals under the age of 18, except in case of pre-existing marriage;
10. complete relevant training courses that will be provided related to the environmental and social aspects of the Contract, including on health and safety matters, and Sexual Exploitation and Abuse, and Sexual Harassment (SH);
11. report violations of this Code of Conduct; and
12. not retaliate against any person who reports violations of this Code of Conduct, whether to us or the Purchaser, or who makes use of the grievance mechanism for Supplier's Personnel or the project's Grievance Redress Mechanism.

RAISING CONCERNS

If any person observes behavior that he/she believes may represent a violation of this Code of Conduct, or that otherwise concerns him/her, he/she should raise the issue promptly. This can be done in either of the following ways:

1. Contact [*enter name of the Supplier's Social Expert with relevant experience in handling sexual exploitation, sexual abuse and sexual harassment cases, or if such person is not required under the Contract, another individual designated by the Supplier to handle these matters*] in writing at this address [ ] or by telephone at [ ] or in person at [ ]; or
2. Call [ ] to reach the Supplier's hotline *(if any)* and leave a message.

The person's identity will be kept confidential, unless reporting of allegations is mandated by the country law. Anonymous complaints or allegations may also be submitted and will be given all due and appropriate consideration. We take seriously all reports of possible misconduct and will investigate and take appropriate action. We will provide warm referrals to service providers that may help support the person who experienced the alleged incident, as appropriate.

There will be no retaliation against any person who raises a concern in good faith about any behavior prohibited by this Code of Conduct. Such retaliation would be a violation of this Code of Conduct.

CONSEQUENCES OF VIOLATING THE CODE OF CONDUCT

Any violation of this Code of Conduct by the Supplier's Personnel may result in serious consequences, up to and including termination and possible referral to legal authorities.

FOR SUPPLIER's PERSONNEL:

I have received a copy of this Code of Conduct written in a language that I comprehend. I understand that if I have any questions about this Code of Conduct, I can contact [*enter name of Supplier's contact person(s) with relevant experience*] requesting an explanation.

Name of Supplier's Personnel: *[insert **name**]*

Signature: _____

Date: (day month year): *[insert **date**]*

Countersignature of authorized representative of the Supplier:

Signature: _____

Date: (day month year): *[insert **date**]*

ATTACHMENT 1: Behaviors constituting SEA and behaviors constituting SH

ATTACHMENT 1 TO THE CODE OF CONDUCT FORM

BEHAVIORS CONSTITUTING SEXUAL EXPLOITATION AND ABUSE (SEA) AND BEHAVIORS CONSTITUTING SEXUAL HARASSMENT (SH)

The following non-exhaustive list is intended to illustrate types of prohibited behaviors.

(1) **Examples of sexual exploitation and abuse** include, but are not limited to:

- A Supplier's Personnel tells a member of the community that he/she can get them jobs related to the project site in exchange for sex.
- A Supplier's Personnel rapes, or otherwise sexually assaults a member of the community.
- A Supplier's Personnel denies a person access to the Project Site/s unless he/she performs a sexual favor.
- A Supplier's Personnel tells a person applying for employment under the Contract that he/she will only hire him/her if he/she has sex with him/her.

(2) **Examples of sexual harassment in a work context**

- A Supplier's Personnel comment on the appearance of another Supplier's Personnel (either positive or negative) and sexual desirability.
- When a Supplier's Personnel complains about comments made by another Supplier's Personnel on his/her appearance, the other Supplier's Personnel comment that he/she is "asking for it" because of how he/she dresses.
- Unwelcome touching of a Supplier's Personnel or Purchaser's Personnel by another Supplier's Personnel.
- A Supplier's Personnel tells another Supplier's Personnel that he/she will get him/her a salary raise, or promotion if he/she sends him/her naked photographs of himself/herself.

TECHNICAL CAPABILITIES

*[**Note**: To be completed by the Proposer and, if JV, by each member]*

Proposer's Legal Name: *[insert **Proposer's Legal Name**]*

Date: *[insert **Date**]*

JV Member Legal Name: *[insert **JV Member Legal Name**]*

RFP No.: *[insert **RFP number**]*

Page _____ of _____ pages

The Proposer shall provide adequate information to demonstrate clearly that it has the technical capability to meet the requirements for the Information System. The Proposer should summarize important certifications, proprietary methodologies, and/or specialized technologies that the Proposer proposes to utilize in the execution of the Contract or Contracts.

MANUFACTURER'S AUTHORIZATION

***[Note**: This authorization should be written on the letterhead of the Manufacturer and be signed by a person with the proper authority to sign documents that are binding on the Manufacturer.]*

Invitation for Proposals Title and No.: *Supply and Installation of the National Digital Identification System (NDIDS), RFP No. WS-SBS-570867-NC-RFP*

To: *Leota Aliielua Salani, Government Statistician (GS), Samoa Bureau of Statistics*

WHEREAS *[insert: **Name of Manufacturer**]* who are official producers of *[insert: **items of supply by Manufacturer**]* and having production facilities at *[insert: **address of Manufacturer**]* do hereby authorize *[insert: **name of Proposer or Joint Venture**]* located at *[insert: **address of Proposer or Joint Venture**]* (hereinafter, the "Proposer") to submit a proposal and subsequently negotiate and sign a Contract with you for resale of the following Products produced by us:

We hereby confirm that, in case the request for proposals process results in a Contract between you and the Proposer, the above-listed products will come with our full standard warranty.

Name *[insert: **Name of Officer**]* in the capacity of *[insert: **Title of Officer]***

Signed _____

Duly authorized to sign the authorization for and on behalf of: *[insert: **Name of Manufacturer**]*

Dated this *[insert: **ordinal**]* day of *[insert: **month**]*, *[insert: **year**]*.

[add Corporate Seal (where appropriate)]

SUBCONTRACTOR'S AGREEMENT

***Note**: This agreement should be written on the letterhead of the Subcontractor and be signed by a person with the proper authority to sign documents that are binding on the Subcontractor.*

Invitation for Proposals Title and No.: *Supply and Installation of the National Digital Identification System (NDIDS), RFP No. WS-SBS-570867-NC-RFP*

To: *Leota Aliielua Salani, Government Statistician (GS), Samoa Bureau of Statistics*

WHEREAS *[insert: **Name of Subcontractor**]*, having head offices at *[insert: **address of Subcontractor**]*, have been informed by *[insert: **name of Proposer or Joint Venture**]* located at *[insert: **address of Proposer or Joint Venture**]* (hereinafter, the "Proposer") that it will submit a proposal in which *[insert: **Name of Subcontractor**]* will provide *[insert: **items of supply or services provided by the Subcontractor**]*. We hereby commit to provide the above named items, in the instance that the Proposal is awarded the Contract.

Name *[insert: **Name of Officer**]* in the capacity of *[insert: **Title of Officer]***

Signed _____

Duly authorized to sign the authorization for and on behalf of: *[insert: **Name of Subcontractor**]*

Dated this *[insert: **ordinal**]* day of *[insert: **month**]*, *[insert: **year**]*.

[add Corporate Seal (where appropriate)]

List of Proposed Subcontractors

	Item	Proposed Subcontractor	Place of Registration & Qualifications

INTELLECTUAL PROPERTY FORMS

Notes to Proposers on working with the Intellectual Property Forms

In accordance with ITP 11.1(j), Proposers must submit, as part of their proposals, lists of all the Software included in the proposal assigned to one of the following categories: (a) System, General-Purpose, or Application Software; (b) Standard or Custom Software; (c) Proprietary or Open Source. Proposers must also submit a list of all Custom Materials. These categorizations are needed to support the Intellectual Property in the GCC and SCC. The Proposer must also include the text of the software licenses for the software titles proposed.

Software List

	(select one per title)			(select one per title)		(select one per title)	
Title	System	General-Purpose	Application	Standard	Custom	Proprietary	Open Source
[insert Title]							
[insert Title]							
[insert Title]							
[insert Title]							
[insert Title]							
[insert Title]							

Attachments: Proposed Software Licenses

List of Custom Materials

Custom Materials
*[insert **Title and description**]*
*[insert **Title and description**]*
*[insert **Title and description**]*
*[insert **Title and description**]*
*[insert **Title and description**]*

CONFORMANCE OF INFORMATION SYSTEM MATERIALS

Format of the Technical Proposal

In accordance with ITP 16.2, the documentary evidence of conformity of the Information System to the request for proposals documents includes (but is not restricted to):

(a). The Proposer's Preliminary Project Plan, including, but not restricted, to the topics specified in the PDS ITP 16.2. The Preliminary Project Plan should also state the Proposer's assessment of the major responsibilities of the Purchaser and any other involved third parties in System supply and installation, as well as the Proposer's proposed means for coordinating activities by each of the involved parties to avoid delays or interference.

(b). A written confirmation by the Proposer that, if awarded the Contract, it shall accept responsibility for successful integration and interoperability of all the proposed Information Technologies included in the System, as further specified in the Technical Requirements.

(c). Item-by-Item Commentary on the Technical Requirements demonstrating the substantial responsiveness of the overall design of the System and the individual Information Technologies, Goods, and Services offered to those Technical Requirements.

In demonstrating the responsiveness of its proposal, the Proposer must use the Technical Responsiveness Checklist (Format). Failure to do so increases significantly the risk that the Proposer's Technical Proposal will be declared technically non-responsive. Among other things, the checklist should contain explicit cross-references to the relevant pages in supporting materials included the Proposer's Technical Proposal.

Note: The Technical Requirements are voiced as requirements of the *Supplier* and/or the *System*. The Proposer's response must provide clear evidence for the evaluation team to assess the credibility of the response. A response of "yes" or "will do" is unlikely to convey the credibility of the response. The Proposer should indicate *that* – and to the greatest extent practical – *how* the Proposer would comply with the requirements if awarded the contract. Whenever the technical requirements relate to feature(s) of existing products (e.g., hardware or software), the features should be described and the relevant product literature referenced. When the technical requirements relate to professional services (e.g., analysis, configuration, integration, training, etc.) some effort should be expended to describe how they would be rendered – not just a commitment to perform the [cut-and-paste] requirement. Whenever a technical requirement is for the Supplier to provide certifications (e.g., ISO 9001), copies of these certifications must be included in the Technical Proposal.

Note: As required in PDS 11.2 (j), include method statement, management strategies and implementation plans and innovations, to manage cyber security risks.

Note: The Manufacture's Authorizations (and any Subcontractor Agreements) are to be included in Attachment 2 (Proposer Qualifications), in accordance with and ITP 15.

Note: As a matter of practice, the contract cannot be awarded to a Proposer whose Technical Proposal deviates (materially) from the Technical Requirements – *on any Technical Requirement*. Such deviations include omissions (e.g., non-responses) and responses that do not meet or exceed the requirement. Extreme care must be exercised in the preparation and presentation of the responses to all the Technical Requirements.

For this request for proposals, the Technical Requirements whose material deviation leads to rejection are the mandatory requirements listed in Section III, paragraph 2.1. A deviation on any other Technical Requirement is scored under the rated criteria of Section III and is not in itself a ground for a determination of non responsiveness.

(d). Supporting materials to underpin the Item-by-item Commentary on the Technical Requirements (e.g., product literature, white-papers, narrative descriptions of technical approaches to be employed, etc.). In the interest of timely proposal evaluation and contract award, Proposers are encouraged not to overload the supporting materials with documents that do not directly address the Purchaser's requirements.

(e). Any separate and enforceable contract(s) for Recurrent Cost items which the PDS ITP 17.2 required Proposers to propose.

Note: To facilitate proposal evaluation and contract award, Proposers encouraged to provide electronic copies of their Technical Proposal – preferably in a format that the evaluation team can extract text from to facilitate the proposal clarification process and to facilitate the preparation of the Proposal Evaluation Report.

Technical Responsiveness Checklist (Format)

Tech. Require. No. _	Technical Requirement: *[insert:* ***abbreviated description of Requirement*** *]*
Proposer's technical reasons supporting compliance:	
Proposer's cross references to supporting information in Technical Proposal:	

The Purchaser provides the Technical Responsiveness Checklist pre filled as a workbook, one row per Technical Requirement of Section VII, annexed to this Section as a separate file because of its size (SAM-RFP_v1.8_14b_Technical-Responsiveness-Checklist.xlsx). The Proposer completes in that workbook, for every requirement, the compliance statement, the technical justification and the cross reference to the Technical Part, and returns it in its spreadsheet format with the Technical Part.

*[**Note to the Purchaser**: The Technical Responsiveness tables submitted by each Proposer can help structure the Purchaser's technical evaluation. In particular, the Purchaser can append rows to each of the Proposer's submitted responsiveness tables to record the Purchaser's assessment of the compliance, partial compliance, and non-compliance of the Proposer's response to the specific Technical Requirement – including the Purchaser's rationale for its conclusion (including, as appropriate, clear indications of the gaps in the Proposer's response/supporting documentation). These assessments can provide a standardized presentation of the detailed underlying logic of the Purchaser's final assessment of the responsiveness / non-responsiveness of the Proposer's technical proposal. Typically, the detailed response/assessment tables would appear as an attachment to the Proposal Evaluation Report].*

FORM OF PROPOSAL SECURITY (BANK GUARANTEE) – NOT APPLICABLE (A PROPOSAL SECURITY IS NOT REQUIRED UNDER PDS ITP 20; ONLY THE PROPOSAL-SECURING DECLARATION APPLIES)

[The bank shall fill in this Bank Guarantee Form in accordance with the instructions indicated.]

[Guarantor letterhead or SWIFT identifier code]

Beneficiary: *[Purchaser to insert its **name and address**]*

RFP No.: *[Purchaser to insert reference **number for the RFP**]*

Alternative No.*: [Insert identification No if this is a Proposal for an alternative]*

Date: *[Insert **date of issue**]*

PROPOSAL GUARANTEE No.: *[Insert **guarantee reference number**]*

We have been informed that *[insert **name of the Proposer**, which in the case of a joint venture shall be the name of the joint venture (whether legally constituted or prospective) or the names of all members thereof]* (hereinafter called "the Applicant") has submitted or will submit the Beneficiary its proposal (hereinafter called "the Proposal") for the execution of *[insert **Name of Contract**]* under Request for Proposals No. [*insert **number**]* ("the RFP").

Furthermore, we understand that, according to the Beneficiary's, Proposals must be supported by a Proposal guarantee.

At the request of the Applicant, we as Guarantor, hereby irrevocably undertake to pay the Beneficiary any sum or sums not exceeding in total an amount of *[insert **amount in figures** ([insert **amount in words**])]* upon receipt by us of the Beneficiary's complying demand supported by the Beneficiary's statement, whether in the demand itself or a separate signed document accompanying the demand, stating that either the Applicant:

(a) has withdrawn its Proposal prior to the Proposal validity expiry date set forth in the Applicant's Letter of Proposal, or any extended date provided by the Applicant; or

(b) having been notified of the acceptance of its Proposal by the Beneficiary prior to the expiry date of the Proposal validity or any extension thereof provided by the Applicant has failed to: (i) execute the Contract Agreement, if required, or (ii) furnish the performance security, in accordance with the Instructions to Proposers ("ITP") of the Beneficiary's request for proposals document.

This guarantee will expire: (a) if the Applicant is the successful Proposer, upon our receipt of copies of the contract agreement signed by the Applicant and the Performance Security issued to the Beneficiary in relation to such Contract Agreement; or (b) if the Applicant is not the successful Proposer, upon the earlier of (i) our receipt of a copy of the Beneficiary's

notification to the Applicant of the results of the request for proposals process; or (ii) twenty-eight days after the expiry date of the Proposal validity.

Consequently, any demand for payment under this guarantee must be received by us at the office on or before that date.

This guarantee is subject to the Uniform Rules for Demand Guarantees (URDG) 2010 Revision, ICC Publication No. 758.

_____

[signature(s)]

FORM OF PROPOSAL SECURITY (PROPOSAL BOND) – NOT APPLICABLE (A PROPOSAL SECURITY IS NOT REQUIRED UNDER PDS ITP 20; ONLY THE PROPOSAL-SECURING DECLARATION APPLIES)

BOND NO. *[insert **number**]*

BY THIS BOND *[insert **Name**]* as Principal (hereinafter called "the Principal"), and *[insert **Name**]*, **authorized to transact business in** *[insert **Jurisdiction**]*, as Surety (hereinafter called "the Surety"), are held and firmly bound unto *[insert **Purchaser Name**]* as Obligee (hereinafter called "the Purchaser") in the sum of *[insert **amount in figures**]* [5] (*[insert **amount in words**]*), for the payment of which sum, well and truly to be made, we, the said Principal and Surety, bind ourselves, our successors and assigns, jointly and severally, firmly by these presents.

WHEREAS the Principal has submitted or will submit a written Proposal to the Purchaser dated the *[insert **ordinal number** day of [insert **month**] [**insert year**]*, for *[insert **name of Contract**]* (hereinafter called the "Proposal").

NOW, THEREFORE, THE CONDITION OF THIS OBLIGATION is such that if the Principal:

(a) withdraws its Proposal prior to the Proposal validity expiry date set forth in the Principal's Letter of Proposal, or any extended date provided by the Principal; or

(b) having been notified of the acceptance of its Proposal by the Purchaser prior to the expiry date of the Proposal validity or any extension thereto provided by the Applicant has failed to; (i) execute the Contract Agreement, or (ii) furnish the Performance Security in accordance with the Instructions to Proposers ("ITP") of the Purchaser's request for proposals document.

then the Surety undertakes to immediately pay to the Purchaser up to the above amount upon receipt of the Purchaser's first written demand, without the Purchaser having to substantiate its demand, provided that in its demand the Purchaser shall state that the demand arises from the occurrence of any of the above events, specifying which event(s) has occurred.

The Surety hereby agrees that its obligation will remain in full force and effect up to and including the date 28 days after the date of expiry of the Proposal validity set forth in the Principal's Letter of Proposal or extended thereto provided by the Principal.

---

[5] The amount of the Bond shall be denominated in the currency of the *Purchaser*'s Country or the equivalent amount in a freely convertible currency.

IN TESTIMONY WHEREOF, the Principal and the Surety have caused these presents to be executed in their respective names this *[insert **number*** day of *[insert **month**] [insert **year**]*.

Principal: _____	Surety: _____ Corporate Seal (where appropriate)
_____ *(Signature)*	_____ *(Signature)*
(Printed name and title)	*(Printed name and title)*

FORM OF PROPOSAL-SECURING DECLARATION

[The Proposer shall fill in this Form in accordance with the instructions indicated.]

Date: *[insert **date** (as day, month and year)]*
Proposal No.: *[insert **number of request for proposals process**]*
Alternative No.: *[insert **identification No if this is a Proposal for an alternative**]*

To: *[insert **complete name of Purchaser**]*

We, the undersigned, declare that:

We understand that, according to your conditions, Proposals must be supported by a Proposal-Securing Declaration.

We accept that we will automatically be suspended from being eligible for bidding or submitting proposals in any contract with the Purchaser for the period of time specified in Section II – Proposal Data Sheet, if we are in breach of our obligation(s) under the proposal conditions, because we:

(a) have withdrawn our Proposal prior to the expiry date of the Proposal validity specified in the Letter of Proposal or any extended date provided by us; or

(b) having been notified of the acceptance of our Proposal by the Purchaser prior to the expiry date of the Proposal validity in the Letter of Proposal or any extended date provided by us, (i) fail to sign the Contract agreement; or (ii) fail or refuse to furnish the Performance Security, if required, in accordance with the ITP.

We understand this Proposal-Securing Declaration shall expire if we are not the successful Proposer, upon the earlier of (i) our receipt of your notification to us of the name of the successful Proposer; or (ii) twenty-eight days after the expiry date of the Proposal validity.

Name of the Proposer***** *[insert **Name of Proposer**]*

Name of the person duly authorized to sign the Proposal on behalf of the Proposer****** *[insert **Name of authorized person**]*

Title of the person signing the Proposal *[insert **Title of authorized person**]*

Signature of the person named above _____

Date signed *[insert **ordinal number**]* day of *[insert **month**] , [insert **year**]*

*****: In the case of the Proposal submitted by joint venture specify the name of the Joint Venture as Proposer

******: Person signing the Proposal shall have the power of attorney given by the Proposer attached to the Proposal

[Note: In case of a Joint Venture, the Proposal-Securing Declaration must be in the name of all members to the Joint Venture that submits the Proposal.]

Letter of Proposal - Financial Part

INSTRUCTIONS TO PROPOSERS: DELETE THIS BOX ONCE YOU HAVE COMPLETED THE DOCUMENT

The Proposer must prepare this Letter of Proposal on stationery with its letterhead clearly showing the Proposer's complete name and business address.

Note: All italicized text is to help Proposers in preparing this form.

Date of this Proposal submission: [*insert date (as day, month and year) of Proposal submission*]

Request for Proposal No.: [*insert identification*]

Alternative No.: [*insert identification No if this is a Proposal for an alternative*]

To: **[*insert complete name of Purchaser*]**

We, the undersigned, hereby submit the second part of our Proposal, the Proposal Price and Priced Activity Schedule. This accompanies the Letter of Proposal- Technical Part.

In submitting our Proposal, we make the following additional declarations:

(a) **Proposal Validity**: Our Proposal shall be valid until *[insert day, month and year in accordance with ITP 19.1]*, and it shall remain binding upon us and may be accepted at any time on or before this date;

(b) **Total Price**: The total price of our Proposal, excluding any discounts offered in item (c) below is: [Insert one of the options below as appropriate]

[Option 1, in case of one lot:] Total price is: [*insert the total price of the Proposal in words and figures, indicating the various amounts and the respective currencies*];

Or

[Option 2, in case of multiple lots:] (a) Total price of each lot [*insert the total price of each lot in words and figures, indicating the various amounts and the respective currencies*]; and (b) Total price of all lots (sum of all lots) [*insert the total price of*

all lots in words and figures, indicating the various amounts and the respective currencies];

(c) **Discounts:** The discounts offered and the methodology for their application are:

(i) The discounts offered are: [*Specify in detail each discount offered*]

(ii) The exact method of calculations to determine the net price after application of discounts is shown below: [*Specify in detail the method that shall be used to apply the discounts*];

(d) **Commissions,** gratuities **and fees:** We have paid, or will pay the following commissions, gratuities, or fees with respect to the procurement process or execution of the Contract: [*insert complete name of each Recipient, its full address, the reason for which each commission or gratuity was paid and the amount and currency of each such commission or gratuity*].

Name of Recipient	Address	Reason	Amount

(If none has been paid or is to be paid, indicate "none.")

Name of the Proposer:*[*insert complete name of the Proposer*]

Name of the person duly authorized to sign the Proposal on behalf of the Proposer: ** [*insert complete name of person duly authorized to sign the Proposal*]

Title of the person signing the Proposal: [*insert complete title of the person signing the Proposal*]

Signature of the person named above: [*insert signature of person whose name and capacity are shown above*]

Date signed [*insert date of signing*] **day of** [*insert month*], [*insert year*]

*****: In the case of the Proposal submitted by a Joint Venture specify the name of the Joint Venture as Proposer.

**: Person signing the Proposal shall have the power of attorney given by the Proposer. The power of attorney shall be attached with the Proposal Schedules

PRICE SCHEDULE FORMS

Notes to Proposers on working with the Price Schedules

General

1. The Price Schedules are divided into separate Schedules as follows:

   3.1 Grand Summary Cost Table

   3.2 Supply and Installation Cost Summary Table

   3.3 Recurrent Cost Summary Table

   3.4 Supply and Installation Cost Sub-Table(s)

   3.5 Recurrent Cost Sub-Tables(s)

   3.6 Country of Origin Code Table

Unit Rates Schedule and Options Schedule, prescribed by the Purchaser

2. The Schedules do not generally give a full description of the information technologies to be supplied, installed, and operationally accepted, or the Services to be performed under each item. However, it is assumed that Proposers shall have read the Technical Requirements and other sections of these request for proposals documents to ascertain the full scope of the requirements associated with each item prior to filling in the rates and prices. The quoted rates and prices shall be deemed to cover the full scope of these Technical Requirements, as well as overhead and profit.

3. If Proposers are unclear or uncertain as to the scope of any item, they shall seek clarification in accordance with the Instructions to Proposers in the request for proposals documents prior to submitting their proposal.

Pricing

4. Prices shall be filled in indelible ink, and any alterations necessary due to errors, etc., shall be initialed by the Proposer. As specified in the Proposal Data Sheet, prices shall be fixed and firm for the duration of the Contract.

5. Proposal prices shall be quoted in the manner indicated and in the currencies specified in ITP 18.1 and ITP 18.2. Prices must correspond to items of the scope and quality defined in the Technical Requirements or elsewhere in these request for proposals documents.

6. The Proposer must exercise great care in preparing its calculations, since there is no opportunity to correct errors once the deadline for submission of proposals has passed. A single error in specifying a unit price can therefore change a Proposer's overall total proposal price substantially, make the proposal noncompetitive, or subject the Proposer to possible loss. The Purchaser will correct any arithmetic error in accordance with the provisions of ITP 35.

7. Payments will be made to the Supplier in the currency or currencies indicated under each respective item. As specified in ITP 18.2, no more than three foreign currencies may be used.

The line items of the Supply and Installation and Recurrent Cost Schedules are prescribed by the Purchaser in the sub tables below (S1 to S9, R1 to R5, unit rates and options schedules); the comparability rules 8 to 14 above apply.

Prescribed line items and comparability rules (Purchaser):

8. Proposers shall quote every line. No line may be deleted, merged or split.

9. A cost carried by another line is quoted as zero with the carrying line named in a remark; silent zeros are treated as omissions per paragraph 6 above.

10. Where the Quantity column carries a Purchaser fixed value, that value shall be used. Where it reads "by Proposer", the proposer states its quantity and the basis for it.

11. Options are quoted in the Options Schedule below and never included in base totals.

12. Recurrent items are quoted per year, per the 3.5 warranty period layout.

13. The proposer's Technical Responsiveness Checklist (the Technical Responsiveness Checklist workbook annexed to this Section) and these schedules shall be consistent: a Comply on a requirement whose funding line is quoted zero with no carrying line is a contradiction the evaluation will treat as such.

14. The right to use all software shall be irrevocable and shall cover the sizing of this RFP for the life of the System, acquired once with the System and priced in the Supply and Installation schedules. No fee may be charged or withheld to keep the right to use alive, and no royalty per transaction or per registered person applies. The only recurrent software cost is the support, maintenance and update service of line R2. A Proposer whose commercial model is subscription based may satisfy this requirement through a prepaid term covering that period, quoted once in the Supply and Installation schedules.

3.1 Grand Summary Cost Table

		*[insert: **Local Currency**] **Price***	*[insert: **Foreign Currency A**] **Price***	*[insert: **Foreign Currency B**] **Price***	*[insert: **Foreign Currency C**] **Price***
1.	Supply and Installation Costs (from Supply and Installation Cost Summary Table)				
2.	Recurrent Costs (from Recurrent Cost Summary Table)				
4.	Grand Totals (to Proposal Submission Form)				

Name of Proposer:		
Authorized Signature of Proposer:		

3.2 Supply and Installation Cost Summary Table

Costs MUST reflect prices and rates quoted in accordance with ITP 17 and 18.

			Supply & Installation Prices				
			Locally supplied items	**Items supplied from outside the Purchaser's Country**			
Line Item No.	**Subsystem / Item**	**Supply and Installation Cost Sub-Table No.**	*[insert: **Local Currency**]* Price	*[insert: **Local Currency**]* Price	*[insert: **Foreign Currency A]*** Price	*[insert: **Foreign Currency B]*** Price	*[insert: **Foreign Currency C]*** Price
0	Project Plan	- -	- -	- -	- -	- -	- -
1	Enrolment kits, tablets and central enrolment services	S1					
2	IDMS and ABIS platform	S2					
3	IDVS and relying party platform	S3					
4	CRVS platform (DPI components)	S4					
5	Card production chain	S5					
6	ICT infrastructure: data centre, network, power, supervision	S6					
7	PKI and trust services	S7					
8	Implementation services	S8					

			Supply & Installation Prices				
			Locally supplied items	**Items supplied from outside the Purchaser's Country**			
Line Item No.	**Subsystem / Item**	**Supply and Installation Cost Sub-Table No.**	*[insert: **Local Currency**]* Price	*[insert: **Local Currency**]* Price	*[insert: **Foreign Currency A]*** Price	*[insert: **Foreign Currency B]*** Price	*[insert: **Foreign Currency C]*** Price
9	Training, capacity building and transfer	S9					
SUBTOTALS							
TOTAL (To Grand Summary Table)							

Note: - - indicates not applicable. "Indicates repetition of table entry above. Refer to the relevant Supply and Installation Cost Sub-Table for the specific components that constitute each Subsystem or line item in this summary table

Name of Proposer:		
Authorized Signature of Proposer:		

3.3 Recurrent Cost Summary Table

Costs MUST reflect prices and rates quoted in accordance with ITP 17 and ITP 18.

Line Item No.	**Subsystem / Item**	**Recurrent Cost Sub-Table No.**	*[insert:* ***Local Currency] Price***	*[insert:* ***Foreign Currency A] Price***	*[insert:* ***Foreign Currency B] Price***	*[insert:* ***Foreign Currency C] Price***
R1	Hardware maintenance, all goods of S1 to S7 (per year, per sub table)	R				
R2	Software support and updates (IDMS, ABIS, IDVS, CRVS, card chain software, supervision). The right to use is perpetual and paid once in the supply price; this line carries only the support, maintenance and update service, never a licence renewal (per year, per system)	R				
R3	Support and SLA operation, all subsystems (severity regime, response and restore times), including warranty and post acceptance support (per year)	R				

Line Item No.	**Subsystem / Item**	**Recurrent Cost Sub-Table No.**	*[insert:* ***Local Currency]*** ***Price***	*[insert:* ***Foreign Currency A]*** ***Price***	*[insert:* ***Foreign Currency B]*** ***Price***	*[insert:* ***Foreign Currency C]*** ***Price***
R4	Personalisation consumables reorders (films, laminates and similar); the blank card stock is supplied once under line S5.2 and is not reordered	R				
R5	Enrolment consumables reorders (per year, at unit rates)	R				
	Subtotals (to Grand Summary Table)					

Note: Refer to the relevant Recurrent Cost Sub-Tables for the specific components that constitute the Subsystem or line item in this summary table.

Name of Proposer:		
Authorized Signature of Proposer:		

3.4 Supply and Installation Cost Sub-Table *[insert: **identifying number**]*

Line item number: *[specify: **relevant line item number from the Supply and Installation Cost Summary Table** (e.g., 1.1)]*

Prices, rates, and subtotals MUST be quoted in accordance with ITP 17 and ITP 18.

				Unit Prices / Rates					**Total Prices**				
				Supplied Locally	**Supplied from outside the Purchaser's Country**				**Supplied Locally**	**Supplied from outside the Purchaser's Country**			
Component No.	**Component Description**	**Country of Origin Code**	**Quantity**	*[insert: **local currency**]*	*[insert: **local currency**]*	*[insert: **foreign currency A**]*	*[insert **foreign currency B**]*	*[insert: **foreign currency C**]*	*[insert: **local currency**]*	*[insert: **local currency**]*	*[insert: **foreign currency A**]*	*[insert: **foreign currency B**]*	*[insert: **foreign currency C**]*
X.1	____	- -	- -	- -	- -	- -	- -	- -					
Subtotals (to *[insert: **line item**]* of Supply and Installation Cost Summary Table)													

Note: - - indicates not applicable.

Name of Proposer:		
Authorized Signature of Proposer:		

Supply and Installation Cost Sub-Table S1: Enrolment kits, tablets and central enrolment services (line item 1 of the Summary Table)

Component No.	Component Description	Category (Good, Software as perpetual licence, Service)	Country of Origin Code	Quantity	Unit price local	Unit price foreign	Total price local	Total price foreign	Technical coverage (SAM requirement blocks)	Acceptance milestone
S1.1	Portable enrolment kit, case format (laptop, FAP60 minimum, camera, signature pad, document reader, receipt printer, power autonomy)	Good		50 kits (firm)					SAM-ENR-071 to 100 (kit composition and performance)	M2
S1.2	Laboratory and training kit (reference kit for the test environment)	Good		1 kit					SAM-ENR kit blocks, SAM-TST environments	M2
S1.3	Ultra mobile rugged enrolment tablet (FAP60 minimum, rear camera)	Good		10 tablets					SAM-ENR-101 to 120 (tablet blocks)	M2
S1.4	Laboratory and training tablet	Good		1 tablet					Same as S1.3, SAM-TST	M2
S1.5	Spare parts lot (batteries, power banks, sensors, cables), sized per the fleet	Good		1 lot					SAM-ENR maintenance rows, SAM-SLA field repair	M2
S1.6	Central enrolment services (kit fleet management, package	Software (perpetual licence)		1 system					SAM-ENR-121 to 145 (central services, MDM, SDIN pools)	M2

Component No.	Component Description	Category (Good, Software as perpetual licence, Service)	Country of Origin Code	Quantity	Unit price local	Unit price foreign	Total price local	Total price foreign	Technical coverage (SAM requirement blocks)	Acceptance milestone
	reception, MDM, synchronisation)									
S1.7	Enrolment consumables, year 1 (receipt paper, cleaning supplies)	Good		1 lot					SAM-ENR receipt and operations rows	M3
S1.8	Installation, staging and commissioning of the enrolment fleet	Service		1 lump sum					SAM-ENR deployment rows, SAM-SVC installation	M2

Supply and Installation Cost Sub-Table S2: IDMS and ABIS platform (line item 2 of the Summary Table)

Component No.	Component Description	Category (Good, Software as perpetual licence, Service)	Country of Origin Code	Quantity	Unit price local	Unit price foreign	Total price local	Total price foreign	Technical coverage (SAM requirement blocks)	Acceptance milestone
S2.1	IDMS software (population register, identity lifecycle, SDIN generation, adjudication workflow)	Software (perpetual licence)		1 system					SAM-IDM-001 to 065, SAM-ADM, SAM-LEG data rules	M4
S2.2	ABIS software, gallery per the	Software (perpetual licence)		1 licence					SAM-IDM-018 to 020 and 093 (deduplication	M4

Component No.	Component Description	Category (Good, Software as perpetual licence, Service)	Country of Origin Code	Quantity	Unit price local	Unit price foreign	Total price local	Total price foreign	Technical coverage (SAM requirement blocks)	Acceptance milestone
	sizing table of VII.1.5								and accuracy); gallery sized for 250,000 registered persons in the base scope, extensible to 800,000 under option O7	
S2.3	Servers and virtualisation, primary site (SBS)	Good		1 lot					SAM-INF compute rows, SAM-PER throughput	M4
S2.4	Storage, primary site (enrolment packages, biometrics, documents)	Good		1 lot					SAM-INF storage rows; SAM-PER-006 storage of twelve (12) megabytes per registered person, biometric source images and scanned documents included, over a ten year growth horizon	M4
S2.5	Adjudication workstations (dual screen, face comparison grade monitors)	Good		8 workstations					SAM-IDM adjudication rows	M4
S2.6	Investigation workstations	Good		3 workstations					SAM-IDM investigation and fraud referral rows	M4

Component No.	Component Description	Category (Good, Software as perpetual licence, Service)	Country of Origin Code	Quantity	Unit price local	Unit price foreign	Total price local	Total price foreign	Technical coverage (SAM requirement blocks)	Acceptance milestone
S2.7	Test and pre production environment (shared across subsystems)	Software (perpetual licence)		1 environment					SAM-TST-001 to 030 environments	M4
S2.8	IDMS and ABIS installation, configuration and tuning services	Service		1 lump sum					SAM-IDM configuration rows, SAM-TST proof of concept	M4

Supply and Installation Cost Sub-Table S3: IDVS and relying party platform (line item 3 of the Summary Table)

Component No.	Component Description	Category (Good, Software as perpetual licence, Service)	Country of Origin Code	Quantity	Unit price local	Unit price foreign	Total price local	Total price foreign	Technical coverage (SAM requirement blocks)	Acceptance milestone
S3.1	IDVS software (1:1 verification, eKYC with consent, OTP, QR verification, assurance level engine)	Software (perpetual licence)		1 system					SAM-IDV-001 to 107, SAM-ARC-041 consent	M8
S3.2	IDVS redundant nodes, primary site (SBS)	Good		2 nodes					SAM-INF, SAM-PER availability	M8
S3.3	IDVS redundant nodes, secondary site (Vodafone	Good		2 nodes					SAM-INF DR rows, SAM-SLA availability	M8

Component No.	Component Description	Category (Good, Software as perpetual licence, Service)	Country of Origin Code	Quantity	Unit price local	Unit price foreign	Total price local	Total price foreign	Technical coverage (SAM requirement blocks)	Acceptance milestone
	DC), active failover									
S3.4	Relying party portal and sandbox (documentation, onboarding, operational verification channel)	Software (perpetual licence)		1 environment					SAM-IDV portal rows	M8
S3.5	IDVS installation, federation setup and relying party integration tooling	Service		1 lump sum					SAM-IDV integration rows, SAM-ARC standards (OIDC, credential format per SAM-ARC-027)	M8

Supply and Installation Cost Sub-Table S4: CRVS platform (DPI components) (line item 4 of the Summary Table)

Component No.	Component Description	Category (Good, Software as perpetual licence, Service)	Country of Origin Code	Quantity	Unit price local	Unit price foreign	Total price local	Total price foreign	Technical coverage (SAM requirement blocks)	Acceptance milestone
S4.1	Component 1: national civil registration database (single source of truth)	Software (perpetual licence)		1 system					SAM-CRV-001 to 020	M7
S4.2	Component 2: development of the interoperable	Service		1 lump sum					SAM-CRV interoperability rows, SAM-IDM-141	M7

Component No.	Component Description	Category (Good, Software as perpetual licence, Service)	Country of Origin Code	Quantity	Unit price local	Unit price foreign	Total price local	Total price foreign	Technical coverage (SAM requirement blocks)	Acceptance milestone
	back end (standardised, versioned APIs, notification services)								notifications (D7)	
S4.3	CRVS installation, configuration of event types and forms	Service		1 lump sum					SAM-CRV configuration rows (D8 deferral clause)	M7

Supply and Installation Cost Sub-Table S5: Card production chain (line item 5 of the Summary Table)

Component No.	Component Description	Category (Good, Software as perpetual licence, Service)	Country of Origin Code	Quantity	Unit price local	Unit price foreign	Total price local	Total price foreign	Technical coverage (SAM requirement blocks)	Acceptance milestone
S5.1	Card personalisation printers, laser engraving, polycarbonate	Good		4 printers (firm)					SAM-CRD-033 and personalisation rows	M6b
S5.2	Blank polycarbonate cards, whole contract volume in a single delivery (chipless, ID1, monoblock)	Good		250,000 cards					SAM-CRD-025, 044, blank stock rows (volume basis: the card volume is aligned on the provisioned baseline of 250,000 persons of SAM-PER-001, on the instruction of	M6b

Component No.	Component Description	Category (Good, Software as perpetual licence, Service)	Country of Origin Code	Quantity	Unit price local	Unit price foreign	Total price local	Total price foreign	Technical coverage (SAM requirement blocks)	Acceptance milestone
									SBS; it covers the full locally living population, five years of issuance after the mass campaign and the wastage and reject allowance; overseas residents digital first, no card provision; values into the W3 sizing table)	
S5.3	Printing films, laminates and personalisation consumables, year 1	Good		1 lot					SAM-CRD consumables rows	M6b
S5.4	Quality control equipment (verification readers, durability sampling)	Good		1 lot					SAM-CRD QC rows	M6b
S5.5	Card personalisation system software (personalisation data preparation)	Software (perpetual licence)		1 system					SAM-CRD personalisation flow	M6b

Component No.	Component Description	Category (Good, Software as perpetual licence, Service)	Country of Origin Code	Quantity	Unit price local	Unit price foreign	Total price local	Total price foreign	Technical coverage (SAM requirement blocks)	Acceptance milestone
S5.6	Card management software (issuance, delivery, lifecycle)	Software (perpetual licence)		1 system					SAM-CRD lifecycle rows	M6b
S5.7	Quality control software (personalisation QC, reject tracking)	Software (perpetual licence)		1 system					SAM-CRD QC rows	M6b
S5.8	Consumables stock management software	Software (perpetual licence)		1 system					SAM-CRD stock rows	M6b
S5.9	Card design application (design and versioning of the card template)	Software (perpetual licence)		1 system					SAM-CRD design rows	M6b
S5.10	Delivery tracking software (card ready to issuance point)	Software (perpetual licence)		1 system					SAM-CRD delivery rows	M6b
S5.11	Production line installation, Apia site, and production ramp up	Service		1 lump sum					SAM-CRD production rows, SAM-SVC installation	M6b

Supply and Installation Cost Sub-Table S6: ICT infrastructure: data centre, network, power, supervision (line item 6 of the Summary Table)

Component No.	Component Description	Category (Good, Software as perpetual licence, Service)	Country of Origin Code	Quantity	Unit price local	Unit price foreign	Total price local	Total price foreign	Technical coverage (SAM requirement blocks)	Acceptance milestone
S6.1	Rack and in rack fit out, SBS main server room	Good		1 rack					SAM-INF-001 to 010	M4
S6.2	Rack and fit out, Vodafone DR site	Good		1 rack					SAM-INF DR rows	M4
S6.3	Network equipment, hosting sites (firewalls, switches, VPN)	Good		1 lot					SAM-INF network rows, SAM-CYB network controls	M4
S6.4	Backup infrastructure (extension of the existing replication, immutable copies)	Good		1 lot					SAM-INF backup rows, 3-2-1-1-0 strategy (P-022-BKP-01)	M4
S6.5	Central supervision and monitoring platform (single platform, whole System)	Software (perpetual licence)		1 system					SAM-ARC supervision rows, SAM-SLA measurement source	M4
S6.6	Network equipment, card personalisation premises (Apia)	Good		1 lot					SAM-INF, SAM-CRD site rows	M4
S6.7	DR site compute and storage (active	Good		1 lot					SAM-INF DR rows, SAM-ADM	M4

Component No.	Component Description	Category (Good, Software as perpetual licence, Service)	Country of Origin Code	Quantity	Unit price local	Unit price foreign	Total price local	Total price foreign	Technical coverage (SAM requirement blocks)	Acceptance milestone
	passive recovery)								recovery objectives	
S6.8	Infrastructure installation, hardening and commissioning services	Service		1 lump sum					SAM-INF rows, SAM-CYB hardening baselines	M4

Supply and Installation Cost Sub-Table S7: PKI and trust services (line item 7 of the Summary Table)

Component No.	Component Description	Category (Good, Software as perpetual licence, Service)	Country of Origin Code	Quantity	Unit price local	Unit price foreign	Total price local	Total price foreign	Technical coverage (SAM requirement blocks)	Acceptance milestone
S7.1	Root CA HSM (offline root, held by SBS) with backup token set	Good		1 device plus backup set					SAM-INF-040 to 048	M4
S7.2	Operational HSM resilient pair (issuing CA, signing services)	Good		1 pair					SAM-INF-040 to 048, SAM-CRD signing, SAM-ARC-019	M4
S7.3	PKI software, CP and CPS drafting support, key ceremony execution	Service		1 service					SAM-INF PKI rows, SAM-LEG trust obligations	M4

Supply and Installation Cost Sub-Table S8: Implementation services (detailed, no undifferentiated lump sums) (line item 8 of the Summary Table)

Component No.	Component Description	Category (Good, Software as perpetual licence, Service)	Country of Origin Code	Quantity	Unit price local	Unit price foreign	Total price local	Total price foreign	Technical coverage (SAM requirement blocks)	Acceptance milestone
S8.1	Project management and governance (PMO, reporting, milestone management M1 to M12)	Service		1 lump sum					SAM-SVC project management rows, VII.2 schedule	All milestones, pro rata
S8.2	Design workshops and detailed specifications (inception workshops, design decisions per doctrine D6, specification baselines)	Service		1 lump sum					SAM-SVC design rows, deferred parameter workshops named across Section VII	M1
S8.3	Integration and configuration services (interfaces, CRVS bridge, notification services, federation)	Service		1 lump sum					SAM-SVC integration rows, SAM-IDM bridge and write back (D2), SAM-IDM-141 (D7)	M4, M7, M8 per interface
S8.4	Testing campaign services (test plans, early proof of concept, performance and security testing,	Service		1 lump sum					SAM-TST-001 to 030	M4, M6b, M8 per release

Component No.	Component Description	Category (Good, Software as perpetual licence, Service)	Country of Origin Code	Quantity	Unit price local	Unit price foreign	Total price local	Total price foreign	Technical coverage (SAM requirement blocks)	Acceptance milestone
	acceptance support)									
S8.5	CRVS data preloading and stock load services (Version 1 baseline)	Service		1 lump sum					SAM-CRV preload rows, stock versus filter doctrine (W5)	M7
S8.6	Cyber security management services (ISMS operation, risk assessments, hardening verification, crisis exercise participation, security documentation)	Service		1 lump sum					SAM-CYB-001 to 024	M4, then recurrent years
S8.7	Mass registration campaign support (field support during the campaign)	Service		8 months					SAM-ENR operations rows, SAM-SVC field support	M5/M6
S8.8	Card production operation support, first year (train and support the SBS operators)	Service		12 months					SAM-CRD operations rows, SAM-TRF production roles	M6b, then monthly over the 12 month support period
S8.9	Relying party pilot support (3 to 5 relying parties, co	Service		1 programme					SAM-IDV pilot rows, SAM-SVC onboarding	M9

Component No.	Component Description	Category (Good, Software as perpetual licence, Service)	Country of Origin Code	Quantity	Unit price local	Unit price foreign	Total price local	Total price foreign	Technical coverage (SAM requirement blocks)	Acceptance milestone
	developed use cases)									
S8.10	Documentation and knowledge base (living documentation per the capacity building doctrine)	Service		1 lump sum					SAM-TRF knowledge base rows, SAM-ARC reversibility documentation	M12
S8.11	Software engineering and release management services (BPMN and DMN process configuration, Purchaser repository with continuous integration pipelines, shared defect tracking tool, reproducible releases with release notes and SBOM)	Service		1 lump sum					SAM-SVC-003, SAM-SVC-009 to 014, SAM-TRF-021	M4, then per release to M8

Supply and Installation Cost Sub-Table S9: Training, capacity building and transfer (priced per work lot, decision D6 addendum) (line item 9 of the Summary Table)

Component No.	Component Description	Category (Good, Software as perpetual licence, Service)	Country of Origin Code	Quantity	Unit price local	Unit price foreign	Total price local	Total price foreign	Technical coverage (SAM requirement blocks)	Acceptance milestone
S9.1	Capacity building programme management and pairing scheme	Service		1 programme					SAM-TRF-001 to 010	Plan at M1, then per lot, final at M12
S9.2	Work lot: enrolment operations (operators, supervisors, field logistics)	Service		1 lot					SAM-TRF enrolment roles, SAM-ENR operations	Per lot at its release, final at M12
S9.3	Work lot: adjudication and identity management back office	Service		1 lot					SAM-TRF back office roles, SAM-IDM adjudication	Per lot at its release, final at M12
S9.4	Work lot: card production and QC operation	Service		1 lot					SAM-TRF production roles, SAM-CRD	Per lot at its release, final at M12
S9.5	Work lot: platform administration, infrastructure and security operations	Service		1 lot					SAM-TRF technical roles, SAM-ADM, SAM-INF, SAM-CYB operational duties	Per lot at its release, final at M12
S9.6	Work lot: relying party management and verification services operation	Service		1 lot					SAM-TRF service roles, SAM-IDV operations	Per lot at its release, final at M12

Component No.	Component Description	Category (Good, Software as perpetual licence, Service)	Country of Origin Code	Quantity	Unit price local	Unit price foreign	Total price local	Total price foreign	Technical coverage (SAM requirement blocks)	Acceptance milestone
S9.7	Immersion programme and final skills assessment (assessment dated per SCC)	Service		1 programme					SAM-TRF immersion and assessment rows, SCC retention terms	M12 (final skills transfer assessment)
S9.8	Work lot: civil registration operations and CRVS component maintenance and evolution (registrar operations, source code depth)	Service		1 lot					SAM-TRF-030, SAM-TRF-013 and 014 (maintenance and evolution depth), SAM-CRV operations	Per lot at its release (M7), final at M12
S9.9	Work lot: software maintenance and evolution of the custom and open source components (business workflows in BPMN and DMN, reference registries, SDIN generator; build, test and deployment performed by SBS staff)	Service		1 lot					SAM-TRF-013 to 016, SAM-TRF-021, SAM-TRF-023, SAM-SVC-011	Per release from M4, final at M12 (practical deployment criterion)
S9.10	Exit and reversibility	Service		1 lump sum					SAM-SVC-054, SAM-	End of the support period

Component No.	Component Description	Category (Good, Software as perpetual licence, Service)	Country of Origin Code	Quantity	Unit price local	Unit price foreign	Total price local	Total price foreign	Technical coverage (SAM requirement blocks)	Acceptance milestone
	services at the end of the support period (reversibility plan execution per work lot, refresh training for the team taking over, handover of all materials and recordings, contract end evidence and residual dependency list)								TRF-009, SAM-TRF-036, 037, 039, 040	(last recurrent year), after M12

3.5 Recurrent Cost Sub-Table *[insert: **identifying number**] -- **Warranty Period***

Lot number: *[if a multi-lot procurement, insert: **lot number,** otherwise state **"single lot procurement"]***

Line item number**:** *[specify: **relevant line item number from the Recurrent Cost Summary Table** – (e.g., y.1)]*

Currency: *[specify: **the currency of the Recurrent Costs in which the costs expressed in this Sub-Table are expressed**]*

*[As necessary for operation of the System, specify: **the detailed components and quantities in the Sub-Table below for the line item specified above, modifying the sample components and sample table entries as needed.** Repeat the Sub-Table as needed to cover each and every line item in the Recurrent Cost Summary Table that requires elaboration.]*

Costs MUST reflect prices and rates quoted in accordance with ITP 17 and ITP 18.

		Maximum all-inclusive costs (for costs in *[insert: **currency**]*)						
Component No.	Component	Y1	Y2	Y3	Y4	...	Yn	Sub-total for *[insert: **currency**]*
1.	Hardware Maintenance	Incl. in Warranty	Incl. in Warranty	Incl. in Warranty				
2.	Software Licenses & Updates	Incl. in Warranty						
2.1	System and General-Purpose Software	Incl. in Warranty						
2.2	Application, Standard and Custom Software	Incl. in Warranty						

		Maximum all-inclusive costs (for costs in *[insert: **currency**]*)						
Component No.	Component	Y1	Y2	Y3	Y4	...	Yn	Sub-total for *[insert: **currency**]*
3.	Technical Services							
3.1	Sr. Systems Analyst							
3.2	Sr. Programmer							
3.3	Sr. Network Specialist, ….. etc.							
4.	Telecommunications costs [to be detailed]							
5.	[Identify other recurrent costs as may apply]							
	Annual Subtotals:							- -
Cumulative Subtotal (to *[insert: **currency**]* entry for *[insert: **line item**]* in the Recurrent Cost Summary Table)								

Name of Proposer:		
Authorized Signature of Proposer:		

Recurrent Cost Sub-Table R: prescribed recurrent lines R1 to R5, quoted per year for the years Y1 and Y2 after Operational Acceptance

Component No.	Component	Basis	Technical coverage (SAM requirement blocks)	Y1	Y2	Sub-total for [insert: currency]
R1	Hardware maintenance, all goods of S1 to S7	per year, per sub table	SAM-SLA hardware service levels			
R2	Software support and updates (IDMS, ABIS, IDVS, CRVS, card chain software, supervision); support, maintenance and update service only, never a licence renewal	per year, per system	SAM-SLA software currency rows, SAM-ARC upgrade rows			
R3	Support and SLA operation, all subsystems (severity regime, response and restore times), including warranty and post acceptance support (SAM-SVC-049 to 053)	per year	SAM-SLA-001 to 020			
R4	Personalisation consumables reorders (films, laminates and similar); the blank card stock is supplied once under line S5.2 and is not reordered	per year, at the unit rates of the Unit Rates Schedule	SAM-CRD consumables, blank stock rows			
R5	Enrolment consumables reorders	per year, at unit rates	SAM-ENR operations rows			
	Annual subtotals (to lines R1 to R5 of the					

Component No.	Component	Basis	Technical coverage (SAM requirement blocks)	Y1	Y2	Sub-total for [insert: currency]
	Recurrent Cost Summary Table)					

Name of Proposer:		
Authorized Signature of Proposer:		

Unit Rates Schedule (firm rates for reorders and post contract orders)

Line	Item	Unit	Technical coverage	Unit rate local	Unit rate foreign
U1	Blank polycarbonate card	per card	SAM-CRD-025 construction		
U2	Personalisation consumables set (films, laminates)	per 1,000 cards	SAM-CRD consumables		
U3	Additional portable enrolment kit	per kit	SAM-ENR kit blocks		
U4	Additional enrolment tablet	per tablet	SAM-ENR tablet blocks		
U5	Additional adjudication workstation	per workstation	SAM-IDM adjudication		
U6	Expert service day rates by profile (the six key personnel profiles plus integration engineer and field technician)	per day	Change and support work under SAM-SVC		

Options Schedule (quoted separately, never in base totals)

Option	Description	Unit	Quantity	Technical coverage	Price local	Price foreign	Included in the evaluated price
O1	Solar recharge sets for outreach teams	set	12 (indicative 10 to 12)	SAM-ENR outreach power rows			N
O2	Additional card personalisation printers	printer	2	SAM-CRD capacity rows			N
O3	Salelologa production line (printer installation, site fit out, network)	line	1	SAM-CRD two site rows, SAM-INF Salelologa			N
O4	CRVS Component 3: business flow engine (BPMN and DMN configured registration flows)	system	1	SAM-CRV flow rows (V2 scope per decision D2)			N
O5	CRVS office workstations and scanners (Apia and Salelologa)	workstation	6	SAM-CRV office rows			N
O6	Billing integration on a pluggable open source ERP	system	1	SAM-IDV billing rows			N
O7	Population increment: extension from the 250,000 provisioned baseline to 800,000 persons in total including the diaspora (licences, gallery, storage, throughput). Quoted firm at proposal; the prices remain guaranteed for activation by the Purchaser during the contract, in the tranches stated by the proposer	increment	1	SAM-PER sizing rows; baseline 250,000 per the SBS correction (wrap up MOM) and the ruling of 3 Sep			N
O8	CRVS residual stock treatment: rolling migration on demand	lump sum or per record	1	Stock and filter doctrine: the enrolment filter constitutes the new civil registration base, and the residual legacy stock is loaded on demand, priced per record			N

3.6 Country of Origin Code Table

Country of Origin	Country Code		Country of Origin	Country Code		Country of Origin	Country Code

SECTION V - ELIGIBLE COUNTRIES

Eligibility for the Provision of Information System

In reference to ITP 4.8 and ITP 5.1, for the information of the Proposers, at the present time firms and information systems from the following countries are excluded from this procurement process:

Under ITP 4.8(a) and ITP 5.1: *none*

Under ITP 4.8(b) and ITP 5.1: *none*

SECTION VI - FRAUD AND CORRUPTION

(Section VI shall not be modified)

1. Purpose

1.1 The Bank's Anti-Corruption Guidelines and this annex apply with respect to procurement under Bank Investment Project Financing operations.

2. Requirements

2.1 The Bank requires that Borrowers (including beneficiaries of Bank financing); bidders (applicants/proposers), consultants, contractors and suppliers; any sub-contractors, sub-consultants, service providers or suppliers; any agents (whether declared or not); and any of their personnel, observe the highest standard of ethics during the procurement process, selection and contract execution of Bank-financed contracts, and refrain from Fraud and Corruption.

2.2 To this end, the Bank:

a. Defines, for the purposes of this provision, the terms set forth below as follows:

i. "corrupt practice" is the offering, giving, receiving, or soliciting, directly or indirectly, of anything of value to influence improperly the actions of another party;

ii. "fraudulent practice" is any act or omission, including misrepresentation, that knowingly or recklessly misleads, or attempts to mislead, a party to obtain financial or other benefit or to avoid an obligation;

iii. "collusive practice" is an arrangement between two or more parties designed to achieve an improper purpose, including to influence improperly the actions of another party;

iv. "coercive practice" is impairing or harming, or threatening to impair or harm, directly or indirectly, any party or the property of the party to influence improperly the actions of a party;

v. "obstructive practice" is:

(a) deliberately destroying, falsifying, altering, or concealing of evidence material to the investigation or making false statements to investigators in order to materially impede a Bank investigation into allegations of a corrupt, fraudulent, coercive, or collusive practice; and/or threatening, harassing, or intimidating any party to prevent it from disclosing its knowledge of matters relevant to the investigation or from pursuing the investigation; or

(b) acts intended to materially impede the exercise of the Bank's inspection and audit rights provided for under paragraph 2.2 e. below.

b. Rejects a proposal for award if the Bank determines that the firm or individual recommended for award, any of its personnel, or its agents, or its sub-consultants, sub-contractors, service providers, suppliers and/ or their employees, has, directly or

indirectly, engaged in corrupt, fraudulent, collusive, coercive, or obstructive practices in competing for the contract in question;

c. In addition to the legal remedies set out in the relevant Legal Agreement, may take other appropriate actions, including declaring misprocurement, if the Bank determines at any time that representatives of the Borrower or of a recipient of any part of the proceeds of the loan engaged in corrupt, fraudulent, collusive, coercive, or obstructive practices during the procurement process, selection and/or execution of the contract in question, without the Borrower having taken timely and appropriate action satisfactory to the Bank to address such practices when they occur, including by failing to inform the Bank in a timely manner at the time they knew of the practices;

d. Pursuant to the Bank's Anti-Corruption Guidelines, and in accordance with the Bank's prevailing sanctions policies and procedures, may sanction a firm or individual, either indefinitely or for a stated period of time, including by publicly declaring such firm or individual ineligible (i) to be awarded or otherwise benefit from a Bank-financed contract, financially or in any other manner;[6] (ii) to be a nominated[7] sub-contractor, consultant, manufacturer or supplier, or service provider of an otherwise eligible firm being awarded a Bank-financed contract; and (iii) to receive the proceeds of any loan made by the Bank or otherwise to participate further in the preparation or implementation of any Bank-financed project;

e. Requires that a clause be included in bidding/request for proposals documents and in contracts financed by a Bank loan, requiring (i) bidders (applicants/proposers), consultants, contractors, and suppliers, and their sub-contractors, sub-consultants, service providers, suppliers, agents, personnel, permit the Bank to inspect[8] all accounts, records and other documents relating to the procurement process, selection and/or contract execution, and to have them audited by auditors appointed by the Bank.

---

6 For the avoidance of doubt, a sanctioned party's ineligibility to be awarded a contract shall include, without limitation, (i) applying for pre-qualification, expressing interest in a consultancy, and bidding, either directly or as a nominated sub-contractor, nominated consultant, nominated manufacturer or supplier, or nominated service provider, in respect of such contract, and (ii) entering into an addendum or amendment introducing a material modification to any existing contract.

7 A nominated sub-contractor, nominated consultant, nominated manufacturer or supplier, or nominated service provider (different names are used depending on the particular bidding document) is one which has been: (i) included by the bidder in its pre-qualification application or bid because it brings specific and critical experience and know-how that allow the bidder to meet the qualification requirements for the particular bid; or (ii) appointed by the Borrower.

8 Inspections in this context usually are investigative (i.e., forensic) in nature. They involve fact-finding activities undertaken by the Bank or persons appointed by the Bank to address specific matters related to investigations/audits, such as evaluating the veracity of an allegation of possible Fraud and Corruption, through the appropriate mechanisms. Such activity includes but is not limited to: accessing and examining a firm's or individual's financial records and information, and making copies thereof as relevant; accessing and examining any other documents, data and information (whether in hard copy or electronic format) deemed relevant for the investigation/audit, and making copies thereof as relevant; interviewing staff and other relevant individuals; performing physical inspections and site visits; and obtaining third party verification of information.

PART 2 – PURCHASER'S REQUIREMENTS

SECTION VII - REQUIREMENTS OF THE INFORMATION SYSTEM

(INCLUDING TECHNICAL REQUIREMENTS, IMPLEMENTATION SCHEDULE, SYSTEM INVENTORY TABLES, BACKGROUND AND INFORMATIONAL MATERIALS)

VII.1 Technical Requirements

A. Acronyms Used in the Technical Requirements

This annex defines the acronyms and terms used throughout Section VII. Where a term is defined in the National Digital Identification Act 2024 (the NDID Act 2024), the statutory definition prevails over any other usage.

General rules of interpretation for this Section VII: wherever a standard, product family or named technology is cited with an equivalence opening, the burden of demonstrating equivalence rests with the Proposer, with evidence the evaluation committee can verify. Standards are cited in the edition in force at the proposal deadline unless a dated edition is stated; where a specific part of a standard is material, the part applies as cited. Scope and price boundary of the deferred details: outcomes of the design and concertation workshops that remain within the capabilities, behaviours and volumes stated in this Section VII are part of the contract scope and price; only outcomes exceeding those stated capabilities, behaviours or volumes follow the contract change procedure.

A.1 Acronyms

Acronym	Meaning
AAL	Authenticator Assurance Level
ABIS	Automated Biometric Identification System
AML/CFT	Anti Money Laundering / Combating the Financing of Terrorism
API	Application Programming Interface
BDM	Births, Deaths and Marriages (as in the Births, Deaths and Marriages Registration Act 2002)
BPMN	Business Process Model and Notation (OMG standard, version 2.0)
CP/CPS	Certificate Policy / Certification Practice Statement
CRVS	Civil Registration and Vital Statistics
DMN	Decision Model and Notation (OMG standard)
DPI	Digital Public Infrastructure
DPIA	Data Protection Impact Assessment
DR	Disaster Recovery
eKYC	Electronic Know Your Customer
FAP	Fingerprint Acquisition Profile (as in FAP60)
FMR / FNMR	False Match Rate / False Non Match Rate
GRM	Grievance Redress Mechanism
HL7 FHIR	Health Level Seven Fast Healthcare Interoperability Resources
HSM	Hardware Security Module
IAL	Identity Assurance Level
ICAO	International Civil Aviation Organization
IDMS	Identity Management System (registration, deduplication and identity lifecycle platform of the NDIDS)
IDVS	Identity Verification Services (verification, authentication and relying party platform of the NDIDS)
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
JSON	JavaScript Object Notation
JWT	JSON Web Token
KPI	Key Performance Indicator
LoA	Level of Assurance
MCIT	Ministry of Communications and Information Technology
MLI	Multiple Laser Image (card security feature)
MoU	Memorandum of Understanding

MRZ	Machine Readable Zone
NDID	National Digital Identification
NDIDS	National Digital Identification System (established under the NDID Act 2024)
NFIQ	NIST Fingerprint Image Quality
OAG	Office of the Attorney General
OAuth 2.0	Open Authorization framework, version 2.0 (IETF)
OIDC	OpenID Connect
OpenID4VCI	OpenID for Verifiable Credential Issuance
OpenID4VP	OpenID for Verifiable Presentations
OTP	One Time Password
PAD	Presentation Attack Detection (ISO/IEC 30107)
PKCE	Proof Key for Code Exchange
PKI	Public Key Infrastructure
PMU	Project Management Unit
QR code	Quick Response code
RBAC	Role Based Access Control
REST	Representational State Transfer
RP	Relying Party
RPO / RTO	Recovery Point Objective / Recovery Time Objective
SBOM	Software Bill of Materials
SBS	Samoa Bureau of Statistics (the Purchaser)
SCC	Special Conditions of Contract
SDIN	Samoan Digital Identification Number
SLA	Service Level Agreement
SSO	Single Sign On
TOTP	Time based One Time Password
VC	Verifiable Credential: a signed credential that a holder presents and a verifier checks. It is issued in one of the two families of SAM-CRD-002, the IETF SD-JWT VC and the ISO/IEC 18013-5 mobile document (mdoc).
W3C	World Wide Web Consortium
WB	World Bank
WCAG	Web Content Accessibility Guidelines

A.2 Definitions

Definitions marked "as defined in the NDID Act 2024" restate the statutory definitions of section 2 (or the section indicated) of the National Digital Identification Act 2024; in case of doubt the text of the Act prevails.

Term	Definition
Authentication	The process by which the NDIDS confirms the identity of a registered person to a relying party, as defined in the NDID Act 2024, s.2.
Biographical data	Personal data relating to the name, date of birth, address and other aspects of the life of a person, excluding biometric data, as defined in the NDID Act 2024, s.2.
Biometric data	Photographic facial images, fingerprints and specimen signatures, as defined in the NDID Act 2024, s.2. No other biometric modality is within the legal scope of the NDIDS.
Biometric Database	The database established under s.38 of the NDID Act 2024, holding biometric data for the sole purpose of authenticating registered persons, separate from the Identity Database and from authentication records.
Consent	A freely given, specific, informed and unambiguous indication, whether by a written or oral statement or an affirmative action, including consent given on behalf of a person by someone having the authority to do so, as defined in the NDID Act 2024, s.2.
Data processor	Any person who processes personal data on behalf of the Registrar General or of a relying party, as defined in the NDID Act 2024, s.2. The Supplier and its subcontractors act as data processors under the contract.
ID credential	As defined in the NDID Act 2024, s.2, any of: (a) a physical ID card issued by the Bureau; (b) a symbol provided by the Bureau that encodes identity information in a manner

	readable by an electronic scanning device; (c) an application installed on a personal communications device such as a mobile phone.
Identification	The association of a person with their SDIN, associated token or ID credential, as defined in the NDID Act 2024, s.2.
Identity Database	The single electronic register established under s.27 of the NDID Act 2024, containing only the data items listed in s.27(3) and none of the data prohibited by s.27(4).
Identity information	Used in this Section to designate, collectively, the biographical data and the credential status data held about a registered person in the NDIDS. Where the NDID Act 2024 applies, the statutory terms biographical data and biometric data prevail.
Mass registration	The planned nationwide registration campaign conducted under s.20 of the NDID Act 2024, with its period and modalities published in the Savali.
NDIDS	The National Digital Identification System, comprising under s.4 of the NDID Act 2024: (a) the civil registration system, (b) the Identity Database, and (c) the Biometric Database with the authentication processes and records, together with the interoperability among them.
Personal data breach	A breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, as defined in the NDID Act 2024, s.2.
Processing	Any operation performed on personal data, as defined in the NDID Act 2024, s.2.
Purchaser	The Government of Samoa, acting through the Samoa Bureau of Statistics (SBS). Where this document places an obligation or a decision on the Purchaser, it is discharged by SBS unless stated otherwise.
Registrar General	The statutory authority administering the NDIDS under the NDID Act 2024, within SBS.
Registration	The process by which the biographical data of a person are recorded in the Identity Database and an SDIN is issued, as defined in the NDID Act 2024, s.2.
Relying party	Any ministry, agency, legal entity or person that is registered with the Registrar General as such and is entitled to rely on the NDIDS for authentication, as defined in the NDID Act 2024, s.2. Prior registration with the Registrar General is constitutive.
Resident of Samoa	A person who is not a citizen of Samoa but is lawfully permitted to reside in Samoa, as defined in the NDID Act 2024, s.2.
Savali	The official government gazette of Samoa, in which several NDIDS milestones must be published.
SDIN	The Samoan Digital Identification Number: the unique, random, lifelong identification number assigned to a registered person under Part 6 of the NDID Act 2024, comprising a randomly generated number and a checksum, carrying no personal meaning, and never reassigned.
Supplier	The firm or consortium contracted to supply and install the System under this RFP.
System	The information system to be supplied, installed and operated under this contract, implementing the NDIDS components described in this Section VII.
Token	A unique number that is exclusively associated with an SDIN and that is issued by the Bureau to a registered person and may be used in lieu of the SDIN, as defined in the NDID Act 2024, s.2. The law provides for one statutory token per SDIN.
Verifiable Credential (VC)	A tamper evident digital credential, cryptographically signed by its issuer and verifiable offline or online, in one of the families of SAM-CRD-002.

B. Functional, Architectural and Performance Requirements

1.1 Legal and Regulatory Requirements to be met by the Information System (SAM-LEG-001 to 030)

This block translates the legal framework of Samoa into cross cutting system obligations. The two governing instruments are the **National Digital Identification Act 2024 (No. 3)** (the "NDID Act 2024" or "the Act") and the **Samoa National Digital Identification Policy v20.0** (the "Policy"), which operationalises the Act without creating obligations beyond it (Policy §3). The detailed functional requirements implementing these obligations are stated in the blocks referenced in each requirement; this block does not repeat them. In case of conflict between any requirement of this Section and the Act, the Act prevails.

Informational note (no Supplier obligation). Parts 3 (Registration) and 6 (Identification and Authentication) of the Act commence on a date to be nominated by the Minister (s.1(2)). Several operational steps additionally require publication in the Savali: the period and modalities of the mass registration (s.20(2)), the modalities of continuous registration (s.22(2)), the start dates for feeding the Identity Database from civil registration and passports (s.28(2)), the list of relying parties (s.40(6)) and the dates from which civil status certificates display the SDIN or token (s.60(1)(d)). The legal go live is therefore a milestone distinct from the technical go live; both are reflected in the Implementation Schedule (VII.2).

1. General compliance

These requirements bind the System to the NDID Act 2024 as a whole: whatever else is specified, the delivered platform must be lawful under the Act from day one.

ID	Requirement
SAM-LEG-001	The System and all its components, interfaces and operating procedures shall comply with the National Digital Identification Act 2024 (No. 3). The Supplier shall deliver, at the design stage, a compliance matrix mapping every provision of the Act with a system impact to the requirements and design elements that implement it, and shall keep this matrix current at every design review and at operational acceptance. Any conflict identified between the Act and a requirement of this Section shall be raised to the Purchaser without delay; the Act prevails.
SAM-LEG-002	The System shall be consistent with the Samoa National Digital Identification Policy v20.0, which operationalises the Act (Policy §3). Where the Policy sets operational targets or design principles not contradicted by the Act (data minimisation, digital first credentials, offline capability, open standards, KPI targets), the System shall implement them as specified in the relevant blocks of this Section.
SAM-LEG-031	The System and the activities of the Supplier shall comply with the Government of Samoa Information Security Policy and with the applicable information security standards issued under it, as they apply to a public sector information system of this kind. The Supplier shall include the Policy and those Standards in the compliance matrix of SAM-LEG-001 and shall keep the mapping current as the Policy, the Standards and the emerging Critical Information Infrastructure Protection framework evolve during the Contract. The security obligations that follow from this instrument are stated in Section VII.1.6, in particular SAM-CYB-001 and SAM-CYB-006.

2. Data architecture imposed by the law

The Act dictates where data lives: which items the Identity Database may hold, the separation of biometric data and logs, and the uses each store may serve.

ID	Requirement
SAM-LEG-003	The Identity Database shall contain in digital form only the nine data items listed in section 27(3)(a) to (i) of the Act (SDIN and any associated token; name; date of birth; place of birth; sex; home address; names of parents including by adoption; date of death;

	data relating to issued, revoked or cancelled ID credentials), where applicable and available. No additional field shall be added to the Identity Database unless authorised under law or regulation. All other data captured or produced by the NDIDS (contact details, scanned documents, declarant information, operational metadata) shall be stored outside the Identity Database as operational data. Implemented in VII.1.2.1 (SAM-ENR-021, SAM-ENR-024, SAM-ENR-029) and VII.1.2.2.
SAM-LEG-004	The Identity Database shall not contain any biometric data, nor any data that directly identifies the individual's race, religion, ethnicity, language, income or medical history. The System shall provide no field, extension mechanism or configuration option that would allow such data to enter the Identity Database.
SAM-LEG-005	The System shall hold the Identity Database, the Biometric Database and the records of use of the authentication function (s.37(3) records) each in its own database, separate from the others. Access to each of the three data stores shall be limited to specifically authorised personnel, through nominative authorisation and separated access control. The physical and logical separation is specified in the architecture block VII.1.3.
SAM-LEG-006	Biometric data shall be used solely for the deduplication required at registration (s.19(5)) and for the authentication of registered persons (s.38(1) and (2)). The System shall not provide any biometric search or matching capability for any other purpose, including surveillance, profiling or identification services to third parties. Implemented through the ABIS confinement in VII.1.2.2 and the verification dataset regime of VII.1.2.3 (SAM-IDV-002, SAM-IDV-015).

3. SDIN and statutory token

The unique number and its statutory token are creatures of the Act: these requirements fix their properties, uniqueness for life and the rules that keep them safe to print and share.

ID	Requirement
SAM-LEG-007	The SDIN and any associated token shall each be a unique number comprising a randomly generated number, with a number of digits prescribed by regulations, plus one or more checksum digits calculated from the random number according to a formula prescribed by regulations. No digit or combination of digits shall be derived from, intentionally signify or bear any relation to any personal data. Length and checksum formula shall be configurable parameters (see SAM-LEG-030). Implemented in VII.1.2.2 (SAM-IDM-022, SAM-IDM-023).
SAM-LEG-008	An SDIN or associated token assigned to a registered person shall never be assigned to another individual, even after the person's death or the deactivation of the number. The SDIN is unique for life. The numbering space and the uniqueness register shall be dimensioned accordingly. Implemented in VII.1.2.2 (SAM-IDM-024).
SAM-LEG-009	The System shall issue exactly one statutory token per SDIN, exclusively associated with it, generated with the SDIN, usable in lieu of the SDIN, and revocable and replaceable by the Registrar General under s.32(2). Both the SDIN and the token shall be notified to the person or their representative upon registration. The System shall not create sectoral or per relying party aliases of the SDIN. Implemented in VII.1.2.2 (SAM-IDM-025, SAM-IDM-026) and VII.1.2.3 (SAM-IDV-003).
SAM-LEG-010	The System shall deactivate the SDIN of a deceased person within twenty eight (28) days after the death is registered in the civil registration system, and promptly where the integrity of the NDIDS so requires (fraudulent issuance, data breach). Deactivation of an SDIN entails immediate deactivation of its token. Upon deactivation the System shall update the civil registration and passport interfaces and notify the relying parties concerned. Any authentication request presented against a deactivated SDIN or token shall return the specific response "deactivated". Implemented in VII.1.2.2 (SAM-IDM-033) and VII.1.2.3 (SAM-IDV-011).
SAM-LEG-011	The System shall record the SDIN or associated token against every birth, death, marriage and change of name record of a registered person in the Register of Births, Deaths and Marriages, and shall support the display of the SDIN or the token on every certificate issued by the Registrar General from the dates published in the Savali. The choice between SDIN and token on certificates shall be configurable. This duty activates with the CRVS platform of VII.1.2.6; where the corresponding certificate issuance services are not part of the awarded scope, the System shall still provide the display capability so the duty can be activated when those services are commissioned. Implemented in VII.1.2.6 (SAM-CRV-005 and certificate services).

4. Minors, biometric scope and registration conditions

Registration of persons under 18 follows specific legal conditions: biographic only capture, linkage to a parent or guardian, and continuity of the identity at majority.

ID	Requirement
SAM-LEG-012	The System shall not collect, and the NDIDS shall not contain, any biometric data of any person below eighteen (18) years of age. The block shall be enforced both at capture and at central processing. ID credentials (physical or digital) shall be issued only to persons aged 18 years and over; minors hold an SDIN without an ID credential within the meaning of the Act (the birth certificate verifiable credential is not an ID credential). The System shall support the addition of biometric data at age 18 on the existing record, without change of SDIN. Implemented in VII.1.2.1 (SAM-ENR-009, SAM-ENR-010), VII.1.2.2 (SAM-IDM-002) and VII.1.2.4.
SAM-LEG-013	Biometric data processed by the NDIDS shall be limited to photographic facial images, fingerprints and specimen signatures, per the statutory definition. No other modality (including iris) shall be captured, stored or matched. Implemented in VII.1.2.1 (SAM-ENR-032).
SAM-LEG-014	Initial registration and assignment of an SDIN during the mass registration and through registration at birth shall be free of charge for the person. Any fee functionality of the System (duplicates, expedited processing, holder initiated corrections) shall enforce configurable gratuity rules so that no charge can be applied to these free of charge cases, and shall support the fee cases permitted by the framework as set by regulations under s.59(a). Implemented by the citizen fee requirement of VII.1.2.4.
SAM-LEG-015	A registered person's failure to update their biographical or biometric data shall never result in the deactivation or suspension of their SDIN or ID credential. The System shall provide no automatic suspension or expiry mechanism triggered by the holder's inaction; renewal cycles (including the photographic refresh under s.30(3)) shall be managed through reminders and re verification, not through penalty on the identity. Implemented in VII.1.2.4 and VII.1.2.2.

5. Authentication, consent and relying parties

The Act conditions every use of an identity: these requirements carry the consent, purpose and acceptance rules that relying party services must respect.

ID	Requirement
SAM-LEG-016	Acceptance of the SDIN or associated token as proof of identity shall never be conditional on the presentation of an ID credential. The System shall provide authentication factors that operate without any credential (OTP, biometric verification, demographic verification), so that a person can be authenticated with their SDIN or token alone. Implemented in VII.1.2.3 (SAM-IDV-012).
SAM-LEG-017	Relying parties shall not access the authentication function, nor obtain or store personal data about registered persons, without the person's consent. Every authentication, eKYC or data sharing transaction shall carry a valid, traceable consent assertion; transactions without one shall be rejected. In addition, any access by a relying party to data of the Identity Database shall be covered by a memorandum of understanding or other agreement with the Registrar General, managed in the relying party framework. Implemented in VII.1.2.3 (SAM-IDV-016, SAM-IDV-017, SAM-IDV-024 and the relying party management requirements).
SAM-LEG-018	Records of the use of the authentication function (requests, transactions and metadata, including date stamps, search logs and audit trails) shall be stored only to the extent and for so long as required for the effective functioning, monitoring, auditing and security of the NDIDS, and in any event for no longer than two (2) years The retention period shall be configurable below this legal cap, and purge shall be automatic and provable. Implemented in VII.1.2.3 (audit requirements) and VII.1.4.
SAM-LEG-019	Data exchanged for authentication shall be limited to the minimal set that the relying party requires to perform its functions and that the NDIDS requires to authenticate the individual. Minimisation shall be enforced technically through per partner policies (default answer yes or no; attributes released only as authorised per purpose). Implemented in VII.1.2.3 (SAM-IDV-008 and partner policy requirements).
SAM-LEG-020	The System shall support the reasonable alternative procedures that the Registrar General must establish for cases of failure of the NDIDS or of the recording or transmission of

	biometric or biographical data, so that no person is penalised for no fault of their own. This includes degraded and offline modes for enrolment and verification, biometric exception handling at registration, and documented fallback procedures usable by relying parties. Implemented in VII.1.2.1 (offline operation, biometric exceptions), VII.1.2.3 and VII.1.6.

6. ID credential constraints

The law closes the list of what may appear on the credential and conditions machine readable features: these requirements translate those limits for the card and credential designs.

ID	Requirement
SAM-LEG-021	A physical ID credential may display on its face only the following data and no other data: the individual's name; the individual's SDIN or associated token or both; the individual's date of birth; an image of the individual's signature; and a photographic image of the individual's face. The personalisation templates shall technically prevent any additional data on the face of the card. Any element beyond this list (including issuing authority marks) shall be placed on the reverse side only, subject to legal confirmation of the interpretation of "on its face". Implemented in VII.1.2.4 (Part B).
SAM-LEG-022	Machine readability of ID credentials (QR code or another two dimensional barcode, microchip or other technology) is permitted only as prescribed by regulations. Printed machine readable features (QR code, MRZ) are readable as soon as the card is printed and cannot be activated at a later date on a chipless card; consequently, no card bearing such features shall be personalised before the relevant regulation is in force. The s.34(5) regulation is therefore a hard prerequisite to the start of card personalisation (client prerequisite P4 in VII.2), and the dependency shall appear in the Implementation Schedule (see SAM-LEG-030). Implemented in VII.1.2.4 (signed QR code requirements).

7. Rights of the registered person (Part 8) and grievances

Registered persons hold enforceable rights over their data: access, correction and complaint. The System must make those rights practically exercisable.

ID	Requirement
SAM-LEG-023	The System shall enable a registered person to obtain, without constraint or unreasonable delay and at no expense, confirmation of whether their personal data are processed and a copy of such personal data in a paper based or commonly used electronic format, through the citizen portal and through assisted channels at service centres. Implemented in VII.1.2.2 (SAM-IDM-031) and the citizen portal requirements of VII.1.2.3/1.2.5.
SAM-LEG-024	The System shall support the correction of personal data that are inaccurate, out of date, incomplete or misleading and, where correction is not feasible or suitable, their deletion; and the deletion of personal data held without legal right. Correction and deletion shall run as traced workflows with supporting evidence and authorised decision, and shall propagate to affected credentials and subscribed systems. Implemented in VII.1.2.2 (SAM-IDM-029, SAM-IDM-030) and VII.1.2.6 (SAM-CRV-016).
SAM-LEG-025	The System shall display to each registered person, free of charge, the accesses to their personal data: what data were accessed or disclosed, when, by whom and to whom, the purpose, manner and duration of access, how long the data will be stored, whether any profiling or automated decision making is applied, and how to lodge a grievance. The access history shall be structured per person and restitutable through the citizen portal and assisted channels. For authentication events, the visible history is bounded by the retention limit of s.37(3) (two years at most); this limitation shall be stated in the privacy notice given under s.25. Implemented in VII.1.2.3 (SAM-IDV-094, citizen dashboard) and VII.1.2.5.
SAM-LEG-026	The System shall provide a grievance management capability allowing a person to lodge a complaint with the Registrar General (online, by phone or at a service centre), track its handling and record its outcome, with acknowledgement and resolution time indicators. The workflow shall be configurable to match the grievance procedure to be prescribed by regulations (see SAM-LEG-030). Implemented in VII.1.2.2 (SAM-IDM-036) and the GRM requirements.

8. Personal data breaches and processor obligations

These requirements carry the breach handling and processor duties: what must be detected, notified and remedied when personal data is compromised.

ID	Requirement
SAM-LEG-027	The System shall support the statutory breach management chain: detection and qualification of personal data breaches; notification by data processors and relying parties to the Registrar General within seventy two (72) hours after becoming aware of a breach, with the categories and approximate volumes of data concerned; extension cases under s.50(2); notification to affected persons without undue delay in plain and clear language where the breach presents a high risk to their rights; and a permanent record of all personal data breaches. The incident and breach register shall be integrated with the security operations defined in VII.1.4 and VII.1.6.
SAM-LEG-028	The Supplier and its subcontractors act as data processors under the Act. They shall process personal data only on documented instruction of the Registrar General, implement the security measures required by s.46, comply with the breach notification duties of s.47, and enforce the controls that the offence provisions presuppose: individual traceability of all internal accesses, confidentiality undertakings by all staff, control of removable storage media, and protected custody of source code. These obligations shall flow down to every subcontract.

9. Data localisation

Identity data stays under Samoan jurisdiction: these requirements state what must remain in country and under whose control.

ID	Requirement
SAM-LEG-029	The NDID registry (Identity Database, Biometric Database and authentication records) shall be maintained on national servers in Samoa, under the control of SBS, on the two designated sites. Cloud services may be used only as an extension for accessibility, resilience and scalability, within the boundaries set in the architecture block VII.1.3 and subject to the Purchaser's approval. The Act itself is silent on localisation; this requirement implements the Policy (§5.3.1) and the hosting decisions of the Purchaser.

10. Regulatory dependencies

Several parameters of the NDIDS are not fixed by the Act but delegated to regulations made under s.59. The table below lists the regulated parameters relevant to the System. Where NDID Regulations have already been made, the design shall apply them; the table shall be reconciled with the regulations in force at contract signature.

Regulated parameter	Legal basis	Main impacted blocks
Number of digits of the SDIN and of the token	s.31(3)(a)	VII.1.2.2 (SDIN generation)
Checksum formula of the SDIN and of the token	s.31(3)(b)	VII.1.2.2 (SDIN generation)
Machine readability of ID credentials (QR code, bar code, microchip)	s.34(5)	VII.1.2.4 (card and QR), VII.1.2.3 (offline verification)
Protection measures for the digital ID credential	s.35(2)	VII.1.2.4 (wallets)
Procedures, protocols and standards for authentication	s.37(2), s.39(1), s.39(3)	VII.1.2.3 (IDVS)
Cybersecurity measures for the Biometric Database	s.38(3)	VII.1.2.2, VII.1.3, VII.1.6
Eligibility and access procedures for relying parties	s.40(3)(c), s.40(5)	VII.1.2.3 (relying party framework)
General security measures	s.46(3)	VII.1.4, VII.1.6
Grievance procedure	s.53(2), s.59(d)	VII.1.2.2, GRM
Fees and charges (with National Revenue Board approval)	s.59(a)	VII.1.2.3 (billing), fee engine

Additional sources of the Identity Database	s.28(1)(c)	VII.1.2.2, VII.1.2.6
Position of the authorities on the activation of the SDIN ahead of legal status confirmation and, if needed, a Regulation defining a restricted SDIN class; the System is configurable either way	s.19(5)(d), s.59	VII.1.2.1 (SAM-ENR-011), VII.1.2.2 (SAM-IDM-026, SAM-IDM-028), VII.1.2.3 (SAM-IDV-106)

ID	Requirement
SAM-LEG-030	Every parameter listed in the regulatory dependency table above shall be implemented as a configuration item modifiable by SBS without software redevelopment and without Supplier intervention: number lengths and checksum algorithm, activation and content of machine readable features, credential protection measures, authentication protocol profiles, security parameters, retention periods, grievance workflow and fee schedules. Until the relevant regulation is in force, default values shall be agreed with SBS at the design stage. The Supplier shall identify in the Implementation Schedule (VII.2) every milestone that depends on a regulation being made or commenced, and shall structure the plan so that a delay on one regulation does not block workstreams that do not depend on it.

1.2 Business Function Requirements to be met by the Information System

1.2.1 Enrolment (SAM-ENR-001 to 070)

This chapter specifies the field registration of persons: who can be enrolled, how the operator finds and binds the person's civil record, what biographic and biometric data is captured, and how enrolment keeps working where connectivity is poor or absent. Samoa runs a mass registration campaign first, then continuous registration; the requirements cover both, with strong attention to exception cases (no documents, poor biometrics, imprecise dates) so that no eligible person is turned away at capture. The related equipment is specified in part D.

Scope and actors

This section frames who does what at enrolment: the operator roles, their access rights, and the population the operation serves.

ID	Requirement
SAM-ENR-001	The Supplier shall implement, install and deploy a biometric enrolment solution for the National Digital Identification System (NDIDS) of Samoa, comprising fifty (50) portable enrolment kits of the suitcase type, ten (10) tablet based enrolment kits for hospitals and other targeted cases, the enrolment client software, the central enrolment server and its secure data store, and the associated delivery, installation, configuration, commissioning, training and support services.
SAM-ENR-002	Enrolment operations shall be carried out by SBS teams. The Supplier shall train and support the operators, trainers and supervisors, and shall support and supervise the operations for the duration of the contract. The training and skills transfer programme (train the trainer approach, shadowing, assessments) is specified in the capacity building annex 2.4 (cross reference; not developed here).
SAM-ENR-003	The System shall support at least the use case "Enrolment of a person". The Supplier shall describe each use case in a dedicated section of its proposal, with flow diagrams and BPMN diagrams detailing every workflow step and how it will be implemented functionally and technically. The final workflows shall be reviewed and validated during specification workshops at the start of the contract.
SAM-ENR-004	The System shall support the following operator roles with access control based on roles: reception operator, enrolment operator, supervisor, and quality controller. Central adjudication operators are outside the scope of the enrolment kits but the System shall interoperate with the central adjudication workflow.
SAM-ENR-005	The System shall be dimensioned on a planning basis of forty (40) enrolments per kit and per day during the mass enrolment wave, without prejudice to the service levels defined elsewhere in this Section. The applicable service levels are consolidated in the service level chapter (part F); operational targets stated in this Section apply in addition to, never instead of, the service levels defined there.
SAM-ENR-006	The System shall provide national coverage of Samoa across the two main islands (Upolu and Savai'i), the 4 regions, the 51 districts and the 339 villages. Kits shall be transportable by road and by inter island ferry, and shall operate in sites with unreliable electricity supply and limited or no connectivity.
SAM-ENR-007	All data and information used, produced, processed or shared under the contract shall remain the exclusive property of the Government of Samoa. The Supplier shall ensure full confidentiality of the activity and full security of the places of performance and of the data itself.
SAM-ENR-008	Before any data capture, the System shall display, and trace the delivery of, the statutory privacy notice required by section 25 of the NDID Act 2024, covering at least: the purposes of processing, the recipients, the retention periods, the existence of any profiling or automated decision making, the rights under section 51 and the recourse to the Registrar General and the Ombudsman. The notice content shall be configurable by SBS, available in English and Samoan, and the enrolment record shall evidence that the notice was given, including where it was given to a legal representative.

Eligibility

Eligibility determines who may be enrolled and under which conditions; the framework is configurable so that category definitions can be settled with SBS and the Attorney General's Office without redevelopment.

ID	Requirement
SAM-ENR-009	The System shall allow the biometric enrolment of all residents of Samoa aged eighteen (18) years and over. Minors shall be registered without any biometric data, through biographic capture only, in accordance with section 19(2) of the NDID Act 2024: in mass through batch creation of records from the consolidated CRVS stock, and at the enrolment kit for children absent from that stock, with the declaring parent or guardian present and authenticated. Eligibility categories shall be a configurable framework: category definitions, their evidence requirements and their processing routes (automatic deduplication through to card processing, or manual checking) shall be configurable by SBS. The category definitions follow the SBS working model (categories A to J) and shall be confirmed with SBS and the Attorney General's Office before operations.
SAM-ENR-010	The System shall prevent the capture of biometric data for persons under eighteen (18) years of age, in line with the legal limit set by the NDID Act 2024. For persons under 18, identity rests on the birth record and the SDIN; no biometric record is created.
SAM-ENR-011	The System shall support the full enrolment of a person who presents no supporting document and has no established CRVS record: biographic and biometric capture shall be completed in the same manner as for any other applicant, and the application shall be submitted to central biometric deduplication. Where deduplication confirms uniqueness, the SDIN bound to the application shall be activated with the distinct status "active, legal status clarification pending" (SAM-IDM-028), so that the person can be identified through 1:1 verification while the legal status clarification process or the late civil registration procedure runs under the authority of the Registrar General, with reference to sections 19(3) and 19(4) of the NDID Act 2024. The application shall be routed to that clarification process, with the captured elements attached (SAM-CRV-030). While the status lasts, no National ID Card and no national identity credential shall be issued (SAM-CRD-001, SAM-CRD-051), and the services available to the identity are restricted by configuration (SAM-IDM-028, SAM-IDV-106). When the clarification succeeds (late civil registration, or an official document accepted by the Registrar General), the same SDIN moves to full active status; where the clarification definitively fails, the SDIN is deactivated and never reassigned.
SAM-ENR-012	The System shall allow a person to present documents proving the authenticity of their biographic data. Such documents shall be scanned and attached to the enrolment application, and the corresponding data shall be flagged as supported.
SAM-ENR-013	Where a person is not found in the preloaded CRVS data and presents no document, the System shall support the capture of a structured community based attestation (National Digital Identification Policy §3.2.4), as an audited, last resort procedure (attestation form including the biographic data of the person and of the attesting parties, captured as a scanned document). The attestation serves as a supporting element of the legal status clarification file managed by the Registrar General (late civil registration or documentary confirmation, SAM-CRV-030); it does not constitute direct proof of identity for the NDIDS.
SAM-ENR-014	The System shall support family enrolment in a single visit: the applications of parents and of their children shall be capturable in the same session. The children's applications shall be linked to the application reference of the accompanying parent (not to the parent's SDIN), so that the whole family is processed without waiting for the parent's SDIN to be deduplicated and activated. The link shall be resolved automatically when the parent's application succeeds; if the parent's application fails, the children's records shall be routed to a manual processing queue. Where an eligible person declines to proceed with enrolment, the enrolment application shall allow the operator to record the refusal with its reason and to issue a receipt of the interaction; recorded refusals shall feed a configurable follow up workflow (re invitation cadence, escalation) whose parameters are set by SBS. The System does not adjudicate refusals, compel enrolment or apply any sanction; the recorded reasons are examined by SBS, and enforcement of the registration obligation remains an SBS administrative process outside the System.

Enrolment workflow

The capture sequence from the search of the person's civil record through consent, capture and receipt: the steps are fixed, their detailed behaviour is settled at the project inception workshops.

ID	Requirement
SAM-ENR-015	The enrolment workflow shall comprise at least the following steps: search of the person in the preloaded CRVS data; verification and completion of the biographic data; recording of consent; capture of the biometric data; capture of supporting documents where presented; review and validation; generation of the enrolment package; issuance of the enrolment receipt. The detailed functionalities and flows of the enrolment processes will be reviewed in detail and settled at the project inception workshops.
SAM-ENR-016	Biographic data shall be preloaded into the kits from the authoritative CRVS source designated in VII.1.2.6: the existing digital CRVS system until the stock database is commissioned, then the stock database, per SAM-CRV-034. The System shall allow the operator to search the preloaded data by name, date of birth, village or birth record reference, in order to prefill the maximum number of fields, save time and avoid transcription errors. The sequence is search, select and bind: the operator searches, selects the matching record, and the application binds it using the unique CRVS record identifier as the binding key. A no match outcome shall never block capture: enrolment proceeds and the application is flagged for the no match analysis routes.
SAM-ENR-017	The System shall support both real time query of the CRVS data when connectivity is available and the use of preloaded offline extracts when it is not. The interfaces and extract services shall be agreed with SBS during the specification workshops.
SAM-ENR-149	The System shall transmit the SDIN to the CRVS component against the record selected and bound at capture: the write back is triggered by the activation of the SDIN, carries at minimum the SDIN and the unique CRVS record identifier, and completes within the delay defined in the service levels. Failed transmissions shall be retried automatically, unresolved failures shall enter a reconciliation queue, and every write back shall leave audit evidence. The write back targets the new CRVS base of VII.1.2.6.
SAM-ENR-018	The System shall not generate identity numbers in the field. SDINs are pre generated centrally by the standalone unique number generator (SAM-IDM-022) as reserved pools provisioned to the enrolment units (SAM-ENR-140 to 144). At capture, the unit shall bind the next reserved SDIN of its pool to the application; this binding is provisional and does not constitute assignment of the number. The SDIN is activated only after successful biometric deduplication by the central IDMS (SAM-IDM-026). Each enrolment shall also be identified by a unique enrolment application reference generated by the System, used for traceability throughout processing.
SAM-ENR-146	During capture, the enrolment application shall display only a minimal set of digits of the reserved SDIN bound to the application, and shall display the complete number with its checksum only once the enrolment is completed. The number of digits displayed at capture shall be a configuration item.
SAM-ENR-019	Before any data capture, the operator shall inform the person of the purpose of the enrolment, of the data collected and of their rights under the NDID Act 2024. The System shall record the consent of the person, given once at enrolment, as part of the enrolment record, with date, time and the identity of the operator who collected it. Where registration is performed on

	behalf of the person by a parent, a legal guardian, a lawful administrator, a Sui Tamaitai o le Nuu, a Sui o le Nuu or a Minister of religion (section 23 of the NDID Act 2024), the System shall record the identity of the declarant and the nature of their authority, and consent given on behalf of the person shall be recorded against the declarant.
SAM-ENR-020	The System shall apply data minimisation: only the data items defined in this Section, as confirmed in the specification workshops, shall be collected.
SAM-ENR-021	The enrolment client design shall be open and configurable so that SBS can extend the enrolment with the capture of new text fields or document types without the assistance of the Supplier. Additional data shall be stored in a dedicated, named part of the enrolment package so that it can easily be extracted by the receiving system. Extensions shall respect the Identity Database boundary rule per SAM-LEG-003: extended data shall be stored as operational data outside the Identity Database.
SAM-ENR-022	The kits shall give access to the identity lifecycle information services published by the IDMS, allowing an operator to check, from an enrolment application reference, the status of the creation of an identity and of the activation of the SDIN.

Biographic data

What is recorded about the person, and from which source of truth: the CRVS record where one exists, the presented documents otherwise, with every discrepancy flagged rather than silently resolved.

ID	Requirement
SAM-ENR-024	The System shall record at least the following biographic data for each person: family name, given names, date of birth (or approximate year of birth, or "date unknown"), place of birth, sex, names of parents, village and district of residence. The final list shall be validated during the specification workshops. Field lengths, character set and the handling of long or compound names shall be specified at the technical inception workshops, taking as input the field constraints of the legacy civil registration data that seeds the System and the truncation rules of SAM-CRD-036. The attributes stored in the central Identity Database shall be limited to the nine core data items listed in section 27(3) of the NDID Act 2024. Any other data captured at enrolment (contact details, supporting document scans and metadata, declarant information) shall be stored outside the Identity Database, as operational data of the NDIDS. The home address (village and district of residence) shall be captured as declared by the person and shall not be subject to verification; it is recorded as a declared attribute, not as proven identity evidence.
SAM-ENR-025	All mandatory biographic data shall be completed before an enrolment can be finalised.
SAM-ENR-026	Where the person is found in the preloaded CRVS data, the CRVS record shall be the reference for the biographic data. Where the person presents a supporting document, the enrolled biographic data shall be those written on the document, with priority given to the birth certificate over any other document. Any discrepancy between sources shall be flagged in the enrolment record for central review. Flagged discrepancies shall follow their own decision route: the application moves to the Pending Review state with a dedicated review queue, and the resolution decision is recorded with author, date and justification. The operator search in the preloaded CRVS data shall never rely on names alone: it shall combine at least name,

	given name, date of birth and village or district; the operator selects the record, the binding uses the unique CRVS record identifier as key, and the SDIN is written back to the new CRVS base (VII.1.2.6).
SAM-ENR-148	Document examination shall follow a defined evidence hierarchy per eligibility category and per attribute, the birth certificate taking precedence over any other document. The examination of a presented document shall verify at least five conditions: the document type is acceptable for the category and the attribute; the document is authentic on its face; it identifies the applicant; its data are consistent with the captured data; and it is valid, or acceptably expired per policy. The hierarchy and the conditions shall be configurable, and the passport shall never be the sole gate to enrolment.
SAM-ENR-147	As an optional reinforcement, the System may verify a presented passport against the Passport Office system through an interface, where such an interface is available. Passport verification shall never be a dependency of the enrolment flow: enrolment shall complete without connectivity to any external system, and the scanned document kept as evidence remains the reference for later inquiry.
SAM-ENR-027	The System shall allow the scanning of documents up to A4 paper size. Scanned documents shall be kept in the enrolment package and transferred to the IDMS with the data, for later verification.
SAM-ENR-028	For each scanned document the System shall capture the associated metadata: document type selected from a predefined list (at least: birth certificate, certified copy or extract of birth record, existing identity document, attestation form) and document reference number. The final list of document types and metadata shall be validated during the specification workshops.
SAM-ENR-029	The System shall allow the collection of one or two contact details per person, typed (mobile phone, email, physical address, postal address). Each contact detail shall carry an ownership flag (personal by default, or belonging to a named relative or local contact with a free text description of the relationship). The storage and usage regime of contact data (no OTP use of non personal contacts, storage outside the Identity Database, never displayed on any credential) is specified in SAM-IDM-060.
SAM-ENR-030	The System shall support imprecise dates of birth (approximate year, or unknown date) and record the imprecision explicitly rather than forcing a fictitious exact date, using the ISO 8601 truncated date representation. The handling policy for these cases shall be defined with SBS at the design stage.

Biometric data

The capture of fingerprints, portrait and signature, with the quality controls that make deduplication reliable downstream: quality is enforced at the point of capture, not repaired afterwards.

ID	Requirement
SAM-ENR-032	The System shall capture the following biometric data for each enrolled person: facial portrait, fingerprints of the ten fingers, and handwritten signature. Iris capture is excluded from the scope.
SAM-ENR-033	The System shall capture a frontal facial portrait compliant with ICAO Doc 9303 portrait requirements and encoded in accordance with ISO/IEC 19794-5 or ISO/IEC 39794-5.
SAM-ENR-034	The System shall capture flat fingerprints of the ten fingers of both hands in a 4+4+2 slap sequence, with automatic segmentation, finger numbering and sequence control.

	Fingerprint images shall be encoded in accordance with ISO/IEC 19794-4 or ISO/IEC 39794-4, captured on devices of acquisition profile FAP60 at minimum, certified against FBI PIV / EBTS Appendix F image quality specifications (larger acquisition profile classes are welcome), and controlled at capture against quality thresholds based on NFIQ 2 or an equivalent open quality metric. Access to captured fingerprint images, including any decrypted use, shall be restricted to authorised roles under the access control, logging and audit requirements of the cyber security chapter and the biometric data protection requirements of this Section.
SAM-ENR-035	If one or more fingers cannot be captured, they shall be marked as such with the reason recorded (missing, injured, worn). Before a finger is marked as not capturable, at least three capture attempts shall be made and the best capture shall be kept.
SAM-ENR-036	If any biometric modality is absent or not capturable, the System shall record an explicit exception indicator and a comment entered by the operator giving the reason.
SAM-ENR-037	The System shall capture the handwritten signature of the enrolled person. Persons unable to sign shall be recorded as such with the reason.
SAM-ENR-038	The System shall perform automatic quality control of each biometric capture in real time, give immediate feedback to the operator, and prompt recapture when quality thresholds are not met. Quality of captured data shall be a key performance indicator of the operations.
SAM-ENR-039	The certification of the biometric capture devices and the biometric encoding standards are specified in the technology specifications of this Section (SAM-ENR-134, SAM-ENR-135). No proprietary biometric format shall be used for storage or exchange.

Enrolment receipt

Every applicant leaves with a receipt proving the application exists: these requirements fix its content and the reference it gives the person pending their SDIN.

ID	Requirement
SAM-ENR-041	At the end of each enrolment, the System shall issue a receipt to the person, bearing at least the provisional SDIN bound to the application, clearly marked as provisional (pending verification), the enrolment application reference for traceability, the date and place of enrolment, and the identifiers of the kit and of the operator. The receipt shall be handed to the person in printed form, produced on the spot by the receipt printer of each enrolment unit (SAM-ENR-082); an electronic copy may complement, but not replace, the printed receipt.
SAM-ENR-042	The receipt shall carry the provisional SDIN and the enrolment application reference in machine readable form (barcode or QR code) so that the status of the application can later be retrieved at any service point.
SAM-ENR-043	The receipt shall state clearly that the SDIN printed on it is provisional and becomes definitive only upon activation after central biometric deduplication (SAM-IDM-026), and shall explain how the person will be informed of the activation, or of the rejection, of the application through the status channels of the NDIDS (notifications per SAM-IDM-037, status enquiry per SAM-IDM-038) and how the status can be checked from the receipt.
SAM-ENR-044	The System shall provide reporting and audit over the full lifecycle of enrolment application references (generated, assigned to a kit, used for an enrolment, transmitted, processed) and of reserved SDINs (pre generated, provisioned to a unit, bound provisionally to an application, activated, or voided and permanently retired where a duplicate is found or the application is rejected, a voided number being never assigned to any person, in accordance with sections 31(7) and 31(8) of the NDID Act 2024).

Offline operation and synchronisation

Field enrolment cannot depend on connectivity: kits work fully offline and synchronise when a connection returns, with no data loss and no duplicate submissions.

ID	Requirement
SAM-ENR-046	The kits shall be able to perform complete enrolments fully offline, with no loss of functionality for data capture, and to store locally all enrolments pending transmission.
SAM-ENR-047	By default, transmission of enrolment data shall be automatic: each enrolment is sent as soon as it is completed if connectivity is available; if not, it is queued and sent automatically when connectivity is restored.

SAM-ENR-048	The System shall also support manual transmission triggered by the operator (for example at the end of the day), sending all data not yet transmitted. This mode shall be reserved for enrolment in areas without coverage from which a regular return to a covered area is possible.
SAM-ENR-049	Where connectivity is unavailable, unstable or insufficient, the System shall allow the export of all pending enrolments to an encrypted physical medium (USB drive or disk) for physical transport to a connected site or directly to the central system. Such exports shall be traceable, verifiable and secured to prevent fraud or injection of false enrolments.
SAM-ENR-050	After successful transmission and acknowledgement, enrolment data shall remain stored on the kit as long as available storage permits. A purge mechanism shall allow the operator to free space by deleting already transmitted data, with selection by enrolment date range and display of the storage space to be freed before deletion; purged data shall be erased irreversibly.
SAM-ENR-051	The System shall keep the preloaded CRVS extracts on the kits up to date through a controlled synchronisation mechanism, so that offline search operates on reasonably fresh data.

Data transmission and field data security

Captured data is protected from the moment of capture: encryption, signing and authenticated devices guarantee that what reaches the centre is what was captured, by whom, on which kit.

ID	Requirement
SAM-ENR-053	Each kit shall transmit the data of enrolled persons to the central enrolment server. The connection shall be asynchronous and resilient to interruptions, with resumption without data loss or duplication.
SAM-ENR-054	Each enrolment shall be packaged as a single compressed enrolment package, internally segmented into named sections so that the central system can quickly isolate the data intended for each receiving system (IDMS, CRVS follow up, additional data).
SAM-ENR-055	The file name of the enrolment package shall identify the enrolment application, the kit, the enrolment site and the date of enrolment. Limited metadata may appear in clear in a dedicated part of the package to facilitate logistics, but shall under no circumstances contain personal data (biographic, biometric or document information).
SAM-ENR-056	Each enrolment package shall be encrypted so that it cannot be read by any intermediary, and shall be timestamped, signed and authenticated so as to guarantee that it was generated by a known and authorised kit and operator and has not been altered by a third party.
SAM-ENR-057	Biometric data shall be protected by encryption at the moment of capture, before any storage or transfer, so as to guarantee that the data originates from an authorised capture device and to prevent any substitution of the captured face or fingerprint images.
SAM-ENR-058	The System shall protect personal data in accordance with the NDID Act 2024 and any data protection rules issued by SBS or the competent Samoan authority.
SAM-ENR-059	Enrolment packages received centrally shall be kept in a secure digital vault: a secure, resilient file store whose purpose is to hold the packages, encrypted in their original form to guarantee integrity and prevent unauthorised access, pending their transfer to the IDMS for deduplication and creation of the unique biometric identity. Operational enrolment data held outside the Identity Database (the enrolment database) shall carry a defined retention and purge policy, applied after the operations end; contact data needed for notifications may be retained per the retention schedule agreed with SBS.
SAM-ENR-060	The System shall provide or send the enrolment data to the IDMS. Data formats, protocols and APIs shall be based on open standards or open source specifications, and shall be finalised during the technical workshops in accordance with the IDMS solution selected.

Exceptions and adjudication routing

Real operations produce hard cases: these requirements make every exception explicit, recorded and routed to the right review queue instead of blocking the person at the counter.

ID	Requirement

SAM-ENR-062	The System shall handle at least the following exception cases without blocking the capture: poor biometric quality (worn or damaged fingerprints), absence of supporting documents, imprecise or unknown date of birth, person not found in the preloaded CRVS data, foreign resident, and suspected duplicate enrolment. Applications captured without any supporting document and without an established CRVS record follow the pathway of SAM-ENR-011. Eligibility as a citizen or resident of Samoa shall be verified in accordance with section 19(5)(d) of the NDID Act 2024. The eligibility evidence shall be recorded as operational data outside the Identity Database; no nationality, residency class or immigration status attribute shall be stored in the Identity Database or displayed on any credential.
SAM-ENR-063	Where a person has no CRVS record, the System shall capture the elements needed to initiate the birth registration follow up with the civil registration authority. These elements shall be stored in a separate section of the enrolment package so that they can be transmitted to the CRVS system.
SAM-ENR-064	Every exception shall be flagged explicitly in the enrolment record and in the enrolment package, with the reason and any operator comment, so that it can be routed to central review or adjudication. Suspected biometric duplicates are resolved centrally by adjudication operators; the resolution workflow itself is outside the scope of the kits.
SAM-ENR-065	The kits shall be able to display, from the enrolment application reference, the outcome of central processing (identity created, pending adjudication, rejected) as published by the IDMS.

Continuous registration

After the mass campaign, enrolment becomes a permanent service: these requirements keep the same capture standards in a steady state operating model.

ID	Requirement
SAM-ENR-067	The System shall support two modes of operation with the same software and data flows: a mass enrolment wave with mobile deployment of the kits across the country, followed by continuous registration from permanent sites to which SBS will redeploy the kits.
SAM-ENR-068	During continuous registration, the Supplier shall support operations remotely and intervene on site only when necessary, in accordance with the service levels defined elsewhere in this Section.
SAM-ENR-069	The ten (10) tablet based kits shall provide the same functional enrolment capability as the suitcase kits, in a lighter form suitable for hospitals and other targeted cases (persons with reduced mobility, remote villages), within the device constraints defined in the technical requirements.

1.2.2 IDMS: functional requirements (SAM-IDM-001 to 067, 142 and 143)

The Identity Management System is the heart of the platform: it receives enrolment packets, establishes that each person is unique through biometric deduplication, generates and activates the SDIN, and manages the identity through its life (updates, corrections, suspension, death). This chapter states the functional behaviour: the processing pipeline, the lifecycle state model, the manual adjudication of doubtful cases, and the audit trail that makes every decision accountable. Bidders should note that lifecycle behaviour is driven by configurable rules, not hard coded flows.

1. Scope and actors

This section frames the central processing roles and the boundary of the IDMS within the platform.

ID	Requirement
SAM-IDM-001	The IDMS shall be the single authoritative biometric identity register for Samoa. It shall guarantee the existence and the uniqueness of every registered person and serve as the trust anchor for the SDIN and for downstream digital identity services.
SAM-IDM-002	The System shall manage the full resident population. Adults aged 18 and over shall hold biometric records (face, fingerprints, signature). Persons under 18 shall exist in the register with an SDIN and without any biometric template, their records being created either from CRVS records or from biographic field capture at the enrolment kits. No iris data shall be collected or stored.
SAM-IDM-003	The System shall be dimensioned for the gallery volumes defined in VII.1.5 (SAM-PER-001) and shall scale to the full lifetime volume without architectural change or additional licence procurement by the Purchaser.
SAM-IDM-004	The System shall support at least the following use cases: processing of an enrolment application, application status enquiry, identity data update, data correction, identity deactivation (death, confirmed duplicate), manual biometric adjudication, anomaly management, fraud case management, complaint management, right of access to own data, update of contact data, and card issuance triggering. This list is preliminary and shall be completed during the specification workshops.
SAM-IDM-005	The Supplier shall document every use case in its proposal with a dedicated section, flow diagrams and BPMN diagrams, and shall describe how each step of each flow will be implemented functionally and technically.
SAM-IDM-006	All business processes shall be implemented as configurable workflows on a workflow engine following a business process, event driven or business rules approach, using BPMN 2.0 and DMN notation or an equivalent open modelling standard, delivered as executable, versioned configurations with their source. SBS shall be able to modify decision rules, statuses, thresholds and notification triggers through DMN configuration, without software redevelopment; this configuration autonomy is required from go live. The Supplier may deliver a simpler configurable workflow implementation at go live, provided the processes are re implemented as executable models on the workflow engine (through API integration to the engine where relevant) before the end of the contract, with the corresponding capacity building. Modification and creation of the process models themselves shall be performed by trained SBS staff with the assisted workflow update service of SAM-IDM-127.
SAM-IDM-007	The System shall provide distinct roles with access based on least privilege, including at minimum: adjudication operator, investigation officer, administrative agent, call centre agent, quality controller, system supervisor and auditor. Role definitions shall be configurable by SBS. The System shall enforce segregation of duties on user identity: the same user shall not be able to act as enrolment operator and as adjudication operator or final authoriser on the same application.

2. Packet reception and processing

How enrolment packets enter central processing: integrity checks, quality gates and the pipeline that feeds deduplication.

ID	Requirement

SAM-IDM-008	The System shall receive enrolment packets from the enrolment platform through a documented interface based on open standards. Reception shall be asynchronous and every packet shall be individually acknowledged.
SAM-IDM-009	Before processing, the System shall verify each packet: digital signature valid, originating device and operator known and authorised, timestamp coherent, content integrity intact. Packets failing any verification shall be rejected with a traceable, machine readable reason.
SAM-IDM-010	Packets shall remain encrypted at rest and in transit. Decryption shall occur only inside the secure processing environment of the IDMS. Biometric data shall stay protected end to end from capture to storage.
SAM-IDM-011	The System shall exploit the sectioned structure of the enrolment packet to extract and route each data section to its destination (identity register, CRVS interface, other authorised systems) without exposing sections to components that do not need them.
SAM-IDM-012	Received packets shall be stored in a secure digital vault until processing is complete. The original packet shall be retained in its encrypted form for later verification or investigation, according to the retention policy defined with SBS.
SAM-IDM-013	Scanned supporting documents and their metadata (document type, document number) received in the packet shall be stored linked to the identity record, and shall be retrievable for adjudication, investigation and audit purposes.
SAM-IDM-014	Packet processing shall be idempotent: a packet submitted more than once shall be detected and shall not create a second application or a second identity record.
SAM-IDM-015	On reception the System shall run automated quality and completeness checks (mandatory fields present, formats valid, biometric exception flags coherent). Applications failing these checks shall be routed to an anomaly queue with an explicit reason, for resolution by authorised staff.
SAM-IDM-016	The System shall handle the documented exception cases without blocking the overall flow, including: degraded or missing biometrics with justification, declared data without supporting evidence (where the application has no documentary or CRVS basis at all, it follows the legal status clarification pathway of SAM-ENR-011 and SAM-IDM-028, not a blocking exception), imprecise or unknown date of birth, repeated enrolment of the same person, and foreign nationals. Each exception path shall be described by the Supplier.
SAM-IDM-067	The System shall resolve the family enrolment links carried in the enrolment packets per SAM-ENR-014: applications of children linked to the application reference of the accompanying parent shall be resolved automatically when the parent's application succeeds, the link being then re anchored on the parent's SDIN or identity record per SAM-IDM-053. When the parent's application fails, the children's applications shall be routed to a manual processing queue for resolution by authorised staff.

3. Deduplication and SDIN generation

The core guarantee of the system, one person one SDIN: biometric deduplication establishes uniqueness, and the standalone generator turns reserved numbers into activated identities.

ID	Requirement
SAM-IDM-017	Every accepted adult application shall be deduplicated 1:N against the full gallery using face and fingerprint data before any SDIN is activated. The outcome shall be one of: unique, potential duplicate (sent to manual adjudication), or confirmed duplicate.
SAM-IDM-018	Deduplication accuracy shall be expressed and contracted as measurable outcomes at search level: a false positive identification rate (FPIR) not exceeding 0.01 percent and a false negative identification rate (FNIR) not exceeding 1 percent, measured on operational data, against the provisioned gallery of SAM-PER-001, at the decision thresholds configured for Samoa. The Supplier shall describe its measurement protocol, and may report comparison level rates (FMR and FNMR) in addition, as supporting information. The decision thresholds shall remain configuration parameters owned by SBS, validated at the early

	proof of concept (SAM-TST-029); the contracted outcomes above apply at the thresholds so configured.
SAM-IDM-019	Deduplication throughput shall absorb the daily intake of the mass enrolment wave, as sized in VII.1.5 (SAM-PER-002, SAM-PER-015), without the processing backlog exceeding five (5) working days, and shall maintain equivalent service at the full lifetime gallery volume (SAM-PER-001).
SAM-IDM-020	The proportion of applications sent to manual adjudication that prove to be false duplicates shall be measured and reported monthly, and shall not exceed two (2) percent of processed applications, so that the adjudication workload stays within the capacity defined in section 5.
SAM-IDM-021	The System shall provide the high level of certainty required by the NDID Act that one person holds exactly one SDIN. Any residual duplicate discovered after activation shall be resolved through the deactivation workflow with full traceability.
SAM-IDM-022	The SDIN shall be generated by the **unique number generator: a standalone, government controlled component developed by the Supplier and delivered with its full source code, build and deployment documentation to the Purchaser**, operable by the Purchaser independently of any other component, including through any partnering or phased build up of in house capability chosen by the Purchaser. For adult enrolment, the generator shall pre generate SDINs as reserved pools allocated to the enrolment units through the central enrolment service (SAM-ENR-140 to 144); the binding of a reserved SDIN to an application at capture is provisional, and the legal assignment of the SDIN is its activation, which occurs only after deduplication has confirmed uniqueness. For minors, the generator serves the birth registration path through the CRVS (see SAM-CRV-043). Numbers voided before activation (duplicate found, application rejected) shall be permanently retired in the generator register and shall never be assigned to any person, in accordance with sections 31(7) and 31(8) of the NDID Act 2024. SDIN generation shall never depend on any external or proprietary service.
SAM-IDM-023	The SDIN shall be random and shall carry no semantic meaning: no date of birth, sex, place, sequence or any other personal information shall be derivable from it. It shall include a checksum allowing detection of typing errors. The SDIN shall be ten digits: eight randomly generated digits followed by two checksum digits. The number of digits and the checksum formula shall remain configurable, and their values shall be confirmed with the Supplier at the design stage in accordance with SAM-LEG-030. The checksum algorithm shall detect single digit errors and transpositions (for example Verhoeff or Damm).
SAM-IDM-024	An SDIN shall never be reassigned to another person, including after death, deactivation or record merge. Retired SDINs shall remain reserved permanently.
SAM-IDM-025	The System shall generate, for each SDIN, the single statutory token provided for by section 31 of the NDID Act 2024: one token per SDIN, generated together with the SDIN, notified to the person, revocable and replaceable in accordance with section 32(2), and printable on civil status certificates. The System shall not create multiple aliases of the SDIN. For minors registered at birth, the System shall expose an identity creation service callable by the CRVS component (SAM-CRV-043) that returns the SDIN and its statutory token together in the same transaction.
SAM-IDM-026	The SDIN shall be activated once uniqueness is confirmed. Activation shall confirm as the definitive SDIN the same provisional number bound to the application at capture (SAM-ENR-018); no different number shall be substituted. Sub requirements SAM-IDM-026.01 to SAM-IDM-026.03 detail the consequences of activation.
SAM-IDM-026.01	For applications without a documentary or CRVS basis, activation shall occur upon deduplication success with the status "active, legal status clarification pending" per SAM-IDM-028 and SAM-ENR-011.
SAM-IDM-026.02	Upon activation the System shall notify the individual through the configured channels, shall issue the associated token of the SDIN and shall notify both the SDIN and the token to the individual or their representative, in accordance with sections 19(7) and 31(6) of the NDID Act 2024; the identity shall become available for verification services through the IDVS interface, within the per status service restrictions of SAM-IDM-028 and SAM-IDV-106 where applicable.
SAM-IDM-026.03	Upon activation of the identity of a person aged 18 or over, the System shall also trigger, through an event driven interface, the issuance of the digital national identity credential specified in VII.1.2.4 (SAM-CRD-001), except for identities in "active, legal status

	clarification pending" status, for which this trigger fires when the status is lifted to full active status; the trigger does not wait for, nor depend on, the card personalisation queue of SAM-IDM-057.
SAM-IDM-027	Applications with missing or degraded biometric modalities (flagged at capture with a reason) shall follow a documented alternative deduplication path, with reinforced controls or systematic adjudication, so that no population group is excluded from obtaining an SDIN.

4. Identity lifecycle (updates, corrections, death, deactivation)

An identity lives for decades: these requirements govern every state change through the six state model, with traceability of who decided what and why.

ID	Requirement
SAM-IDM-028	The System shall manage the full identity lifecycle through an explicit, documented state model of six states: Reserved, Captured, Pending Review, Active, Suspended and Revoked. The model shall distinguish four layers: State, Status or Sub status, Flag, and Reason Code, so that conditions such as "active, legal status clarification pending" are carried as a Sub status of the Active state, temporary conditions are carried by the Suspended state with their Reason Codes, and permanent terminations (death, confirmed duplicate, confirmed fraud) are carried by the Revoked state with their Reason Codes, revoked records being retained. Sub requirements SAM-IDM-028.01 to SAM-IDM-028.03 detail the activation rule, the legal status clarification path and the per status configurability.
SAM-IDM-028.01	Reservation of a number is not legal SDIN activation; activation is automated by decision rules, with no manual desk activation.
SAM-IDM-028.02	The status "active, legal status clarification pending" applies to identities activated after successful deduplication without a documentary or CRVS basis (SAM-ENR-011): the identity moves to full active status when the legal status clarification succeeds (late civil registration, or an official document accepted by the Registrar General, per SAM-CRV-030), and to deactivated where the clarification definitively fails, the SDIN being never reassigned.
SAM-IDM-028.03	The services available to identities in each status, including for the "legal status clarification pending" status the availability of 1:1 identification and demographic verification and the disclosure of the status flag to relying parties (SAM-IDV-106), shall be configurable by SBS per status, without software redevelopment. Every state transition shall be traced with author, timestamp and reason.
SAM-IDM-029	The System shall process identity data updates (change of name, change of attribute) as workflow cases, with supporting evidence attached, validation by an authorised agent, and propagation of the change to subscribed systems.
SAM-IDM-030	An administrative agent shall be able to record a data correction request on behalf of an individual. The correction procedure, the evidence required and the approval chain shall be described by the Supplier and finalised in the project workshops.
SAM-IDM-031	The System shall support the right of access: an individual shall be able to obtain, through an administrative agent, the biographic data and document metadata held about them, together with the list of updates applied to their record.
SAM-IDM-032	The System shall allow individuals to update their contact data through a light procedure distinct from identity data correction.
SAM-IDM-033	Upon a death notification received from the CRVS, the System shall mark the person as deceased and deactivate the SDIN for all verification services, while preserving the full record and its history. Deactivation shall be completed within twenty eight (28) days after the death is registered in the civil registration system, as required by section 32(1) of the NDID Act 2024. Upon deactivation the System shall update the civil registration interface, notify the passport system interface where implemented, and notify the relying parties concerned, in accordance with section 32(3). Where an unconfirmed death notice is received ahead of civil registration (for example a health system notice), the System shall support suspension of the SDIN pending confirmation, with revocation only upon the registered death, per the state model of SAM-IDM-028.

SAM-IDM-034	When an investigation confirms a duplicate, the System shall allow deactivation of the redundant record. The surviving record shall keep its SDIN. The decision, its author, its date and its justification shall be recorded and shall be reversible only through an authorised reactivation procedure.
SAM-IDM-035	The System shall support reactivation of a deactivated identity when the deactivation is proven erroneous, subject to a documented authorisation workflow, with full traceability.
SAM-IDM-036	The System shall register and manage complaints lodged by individuals by phone, in an office or online, track their resolution and record the outcome. The complaint procedure shall be described by the Supplier. Complaint handling shall run on the single shared open source service desk of the NDIDS, or an equivalent service desk giving the Purchaser the same rights of use, adaptation and export of its data without licence dependence, in a dedicated citizen grievance queue separate from the partner support queue (SAM-IDV-086), integrated with the other components by API.
SAM-IDM-037	The System shall send notifications to individuals at key lifecycle steps (action required on the application, SDIN activated, card available for collection) through SMS and email gateways, with templates configurable by SBS and the capacity to add further channels without redevelopment.
SAM-IDM-038	Individuals shall be able to check the status of their application through a public web portal using their application reference, without authentication revealing any personal data beyond the status itself.

5. Manual adjudication workflow

Where the machine is unsure, trained operators decide: queues, side by side comparison, controlled decisions and second validation, sized for the mass campaign and the legacy caseload.

ID	Requirement
SAM-IDM-039	The System shall include a manual adjudication module organising potential duplicate cases into work queues, with case assignment, priority management and workload monitoring.
SAM-IDM-040	For each case, the adjudication workstation shall present the candidate records side by side with their biographic data, portraits, fingerprint images, signatures and scanned supporting documents, so that the operator can decide on documented evidence.
SAM-IDM-041	Adjudication decisions shall be limited to a controlled set: unique, confirmed duplicate, or escalation to investigation. Every decision shall be recorded with operator identity, timestamp, decision and reason code. Free text justification shall be possible.
SAM-IDM-042	The System shall support configurable double validation: for decision classes defined by SBS, a second operator shall confirm the decision before it takes effect. This control shall be activatable per decision type without redevelopment.
SAM-IDM-043	The adjudication capacity shall be sized for the mass enrolment adjudication volumes defined in VII.1.5 (SAM-PER-003), with a sustained throughput of several hundred cases per day, supported by an investigation cell of 2 to 4 persons.
SAM-IDM-044	The System shall support an investigation workflow for escalated cases: request for additional evidence, recording of field verification results, and a final documented decision feeding back into the adjudication queue.
SAM-IDM-045	Queue ageing shall be measurable: the System shall report the age of pending cases and alert when cases exceed the resolution time defined in the service levels.
SAM-IDM-046	Cases showing indications of deliberate identity fraud (multiple enrolment attempts, falsified documents) shall be flagged and routed as cases of type "fraud" in the single case management queue of SAM-IDM-109, with a case file usable by the competent authorities.
SAM-IDM-047	The training, supervision and guidance of the adjudication operators provided by the Government are specified in SAM-IDM-108 (selection support, initial training, adjudication procedures, quality supervision and reporting).

6. Interfaces (enrolment platform, CRVS, IDVS, card personalisation)

The IDMS talks to every other subsystem: these requirements fix the exchanges, their direction and their resilience, including the notification services.

ID	Requirement

SAM-IDM-048	The exchange protocol with the enrolment platform (packet format envelope, acknowledgement, status callback, error handling) shall be fully documented and based on open standards, and shall be agreed in the technical workshops at project start.
SAM-IDM-049	The System shall return a processing status to the enrolment platform for every application. The status list is owned by this block and shall include at minimum: received, processing, deduplication in progress, potential duplicate under adjudication, accepted with SDIN, rejected with reason. Rejections shall always carry a machine readable reason code.
SAM-IDM-050	Statuses shall be available to enrolment operators through the enrolment platform in near real time, so that field teams can inform applicants and correct rejected applications.
SAM-IDM-051	The System shall confirm the secure erasure of preloaded CRVS extracts that were distributed to enrolment devices and not used (erasure performed on the units per SAM-ENR-108). Erasure confirmations shall be collected per device, logged and auditable.
SAM-IDM-052	The System shall receive life event notifications (births, deaths and civil status changes) from the CRVS component specified in VII.1.2.6, which fronts the existing digital CRVS system during V1 (SAM-CRV-033, SAM-CRV-035). The register shall be updated accordingly. The synchronisation frequency between the legacy system and the CRVS component shall be compatible with the twenty eight (28) day death deactivation deadline of SAM-IDM-033. The CRVS remains the authoritative source for civil status; its replacement is out of scope of this block. The in scope notification services shall include the death notice suspension channel and the antenatal notification channel from the health system, serving the civil registration flow and the identity lifecycle.
SAM-IDM-053	The System shall create the identity record of a minor and assign an SDIN without any biometric template, through three creation paths: (i) upon a birth notification from the CRVS; (ii) upon biographic field capture at an enrolment kit with an authenticated declarant present; and (iii) in bulk, by batch creation of records from the certified CRVS stock of VII.1.2.6 (per SAM-ENR-009), with biographic deduplication before creation and SDIN allocation through the unique number generator of SAM-IDM-022. Deduplication of minors shall rely on biographic data only. The minor's record shall be securely linked to the SDIN or identity record of a parent or legal guardian for verification and relationship validation purposes, this link being stored as operational data outside the Identity Database. When the person reaches eighteen (18) years, the System shall support the addition of biometric data to the existing record, its full biometric deduplication against the gallery and the issuance of credentials, without change of SDIN, including automated invitation campaigns to the persons concerned.
SAM-IDM-054	When deduplication confirms a unique person who has no civil registration record, the System shall notify the CRVS so that the retroactive civil registration procedure can be initiated, and shall track the case until the civil status link is established.
SAM-IDM-055	The System shall provision the IDVS exclusively through tokenisation mechanisms based on the SDIN and its statutory token. The IDVS shall never access the master identity data directly; only the derived data strictly needed for verification services shall be provisioned.
SAM-IDM-056	Provisioning of the IDVS shall be event driven: activation, update, deactivation and death events shall propagate to the IDVS within the delay defined in the service levels.
SAM-IDM-057	When an identity meets the card issuance conditions (unique, aged 18 or over, and legal identity confirmed), the System shall place a personalisation request in the card issuance queue and expose the required data to the card personalisation chain through a documented API. Legal identity is confirmed when the civil registration link is attached to the record, or when the Registrar General has formally confirmed the documentary evidence of sections 19(3) and 19(4) of the NDID Act 2024 where no civil record is retrievable. The National ID Card shall never be personalised before this confirmation (see SAM-CRD-051); the digital credential of SAM-IDM-026 is not subject to this gate. Card production itself is covered by a separate block.
SAM-IDM-058	Card lifecycle feedback (produced, delivered to collection point, collected by the individual) received from the card chain shall be reflected in the application status visible to operators and to the individual.

7. Data model and data quality

The identity data model and the quality rules that keep it trustworthy, extensible by SBS without Supplier intervention.

ID	Requirement

SAM-IDM-059	The identity data model shall cover at minimum: biographic attributes, typed contact data, document metadata and scans, biometric exception flags, lifecycle status and SDIN. SBS shall be able to extend the model with new attributes through configuration, without Supplier redevelopment. Extensions shall respect the Identity Database boundary rule per SAM-LEG-003: extended data shall be stored as operational data outside the Identity Database.
SAM-IDM-060	Contact data shall be typed (mobile phone, email, physical address, postal address) and carry an ownership flag. Only contact data marked as personal shall be usable for authentication purposes such as one time passwords. Contact details are operational service data: they shall be held outside the Identity Database defined by section 27(3) of the NDID Act 2024 and shall never be displayed on any credential.
SAM-IDM-061	Every biographic attribute shall carry an evidence marker distinguishing declared data from data supported by a scanned document, and the System shall allow later upgrade of an attribute from declared to evidenced.
SAM-IDM-062	The System shall handle imprecise dates of birth (approximate year, unknown date) as explicit values, usable in search, deduplication support and card issuance without manual workarounds.
SAM-IDM-063	Data quality shall be measured continuously (completeness, evidence coverage, biometric exception rates, correction rates) and reported as key performance indicators to SBS.
SAM-IDM-142	Bulk extraction of the Identity Database, of the biometric gallery and of the civil registry records shall be impractical by design, stated as an outcome: no single authorised session, account, role or interface shall be able to read, copy or export the whole or a substantial part of the identity records, of the biometric records or of the civil registry records. The threshold that defines a substantial part is a configuration parameter set by SBS during detailed design, consistent with SAM-IDM-006; the outcome is demonstrated against it at the security acceptance tests of SAM-CYB-051. The Supplier shall describe its mechanism in its technical proposal and shall demonstrate the outcome at the security acceptance tests of SAM-CYB-051. Partitioning of the stores, per record or per partition encryption with key material held in the cryptographic modules of SAM-INF-040, volume thresholds per account and per interface with alerting to the security monitoring of SAM-CYB-010, and the technical blocking of any read outside the declared application paths, are all explicitly acceptable implementations. The requirement applies separately to the Identity Database, to the Biometric Database, to the consolidated stock database and the certified records of VII.1.2.6, and to the authentication and transaction log store, consistent with the separation imposed by SAM-IDM-066, and mirrors for the central registers the outcome already required of the verification dataset by SAM-IDV-031. Operations that legitimately require volume, being backup and restoration under SAM-ADM-017 to SAM-ADM-020, the reversibility export of SAM-IDM-130, the preloading extracts of SAM-ENR-108 and the migration runs of SAM-SVC-023, are exempt from this requirement and are governed by SAM-IDM-143.

8. Audit and traceability

Every operation on an identity leaves a tamper evident trace: these requirements make the audit trail complete enough to reconstruct any decision, including the biometric ones.

ID	Requirement
SAM-IDM-064	The System shall keep a complete, tamper evident audit trail of every operation on identity records and on SDINs: who, when, what, from where and why. This includes the SDIN lifecycle (generated, assigned, activated, deactivated), adjudication decisions, corrections, deactivations, data accesses and secure erasure events. Audit records shall be protected against modification, retained per the agreed policy and searchable by authorised auditors. Audit records relating to authentication transactions are governed by the two (2) year maximum retention of section 37(3) of the NDID Act 2024 and shall be purged or irreversibly anonymised accordingly. Administrative audit records on identity records and SDIN lifecycle events are not subject to that cap and follow the retention policy agreed with SBS.
SAM-IDM-065	The System shall produce operational statistics and dashboards for SBS: applications received and processed, deduplications completed, SDINs activated, adjudication throughput and backlog, average packet processing time, with daily, weekly and monthly views. These views shall be served by the single BI and reporting layer shared across all components of the NDIDS, not by a separate reporting build. All data and statistics remain the exclusive property of the Government of Samoa. Statistics shall be

	disaggregated at least by sex, age group, disability status, region and district, in support of the annual reporting obligation of section 16 of the NDID Act 2024 (level of registration nationally and by region, level of use of the NDIDS) and of the monitoring framework of the National Digital Identification Policy.
SAM-IDM-143	Any extraction, export or outbound disclosure of personal data drawn from the Identity Database, from the Biometric Database or from the civil registry stock, other than the responses of the verification services governed by VII.1.2.3, shall pass through an approval workflow requiring the agreement of two authorised persons, one of whom shall be designated by the Registrar General, and shall be recorded in a disclosure register. The register shall hold, for each entry: the requester, both approvers, the purpose, the legal basis relied on, the recipient, the data classes and the volume concerned, the channel used, the date of the extraction, and the date of return or destruction where one applies. The register shall be tamper evident on the same terms as the audit trail of SAM-IDM-064, shall be exportable in full for audit, and shall be reported to SBS monthly through the supervision layer of SAM-IDM-117. No extraction within the scope of this requirement shall be technically possible outside this workflow, consistent with SAM-IDM-142. This requirement does not create any right of disclosure: it governs how a disclosure otherwise permitted by the National Digital Identification Act 2024 is authorised and traced.
SAM-IDM-066	The System shall implement the data separation mandated by sections 27(4) and 38(4) of the NDID Act 2024: the Identity Database, the Biometric Database (facial images, fingerprint images and specimen signatures) and the authentication and transaction log store shall each reside in its own database, physically or logically separated from the others, with access to each store limited to specifically authorised personnel. The Identity Database shall contain no biometric data and no data directly identifying race, religion, ethnicity, language, income or medical history. Each biometric datastore shall implement biometric information protection consistent with ISO/IEC 24745, with access, encryption and monitoring controls aligned to a recognised NIST or ISO control framework, stated by the Supplier in its proposal.

1.2.2 (continued) IDMS: components and platform (SAM-IDM-071 to 140)

This chapter describes the software components delivering the IDMS functions: the platform and its workflow engine, the ABIS specified through measurable outcomes rather than internals, the adjudication and investigation applications with their workstations, case management for fraud and anomalies, supervision, and the exit arrangements that keep SBS sovereign over the platform. A recurring theme for bidders: components must be replaceable and the Purchaser must be able to operate, configure and eventually re procure each part without dependency on the original Supplier.

IDMS software platform

The platform components delivering the IDMS functions: modular, workflow driven, configurable by SBS, with the unique number generator delivered in full sovereignty.

ID	Requirement
SAM-IDM-071	The IDMS platform shall be a modular software platform comprising at least: the enrolment package manager, the workflow orchestration engine, the unique identification module (which invokes, for SDIN generation and activation, the standalone unique number generator specified in SAM-IDM-022: a standalone, government controlled component developed by the Supplier and delivered with its full source code, build and deployment documentation to the Purchaser, operable by the Purchaser independently of any other component), the person registry, the manual adjudication application, the case management function for anomaly, fraud and investigation cases, and the supervision application. It shall be deployable, without modification, on the two hosting sites defined in the architecture block (see SAM-ARC-020 and SAM-ARC-021), on virtualised infrastructure. Infrastructure sizing, replication and disaster recovery are specified in the architecture and administration block and are outside the scope of this subsection.
SAM-IDM-072	The IDMS shall ingest enrolment packages through the secure exchange protocol defined in VII.1.2.1 and in requirements SAM-IDM-001 to 066 (signed enrolment packages deposited in a secure file store and consumed asynchronously by the IDMS, then archived by the IDMS in its own file store). No other channel shall be used for the creation of identities from mass or continuous enrolment.
SAM-IDM-073	The enrolment package manager shall be an autonomous, scalable and highly available software module in charge of consuming the enrolment packages deposited by the enrolment system and of starting the verification workflows leading to the creation of unique identities. Its file based interface shall provide inherent flow control, since packages can be deposited at one rate and consumed at another.
SAM-IDM-074	The enrolment package manager shall apply a lifecycle to each enrolment package, materialised by its status. The following statuses are envisaged at least: RECEIVED, IN PROCESSING, NOT INTEGRATED, NOT AUTHENTIC, NOT ELIGIBLE, DUPLICATE, FRAUD, REJECTED, VALID. The final list shall be reviewed during the specification workshops.
SAM-IDM-075	Before any processing, the enrolment package manager shall verify: (i) the integrity of each package through the data signature; (ii) the authenticity of the enrolment source through the data signature; and (iii) that the enrolment station and its operator were both declared to the central system, active and authorised to enrol at the date, time and place of the enrolment. Packages failing these checks shall be routed to the anomaly or fraud workflows as relevant. Once all verifications are

	passed, the package shall be structured to feed the identity creation workflow.
SAM-IDM-076	All transactions of the IDMS, and in particular all transactions modifying data, shall be recorded in an audit log identifying at least: the transaction identifier, the nature of the operation, the data changed, the date and time, the place and the authenticated person responsible for the change.
SAM-IDM-077	The Supplier shall deliver the source code of the enrolment package parsing libraries (analysis and extraction of package data) so that SBS can freely evolve the interfaces towards new data structures or new forms of enrolment. Delivery of the source code of the whole enrolment package manager will be assessed favourably. Source code delivery and the associated skills transfer shall follow the capacity building annex of this Section.
SAM-IDM-078	The orchestration engine shall execute the preconfigured business workflows of the IDMS following a business process, event driven or business rules approach. The business workflows shall be delivered as executable, versioned configurations in BPMN 2.0 and DMN or an equivalent open modelling standard, with their source. The Supplier may deliver a simpler configurable implementation at go live, provided the workflows are re implemented as executable models on the engine (through API integration where relevant) before the end of the contract, with the corresponding capacity building; the DMN configuration autonomy below is required from go live. SBS autonomy applies to decision rules, statuses, thresholds and notification triggers, which shall be modifiable through DMN configuration without software redevelopment; modification of the process models themselves is performed by trained SBS staff with the assisted workflow update service of SAM-IDM-127.
SAM-IDM-079	The orchestration engine shall be delivered with: (i) a graphical design tool allowing trained SBS business analysts, supported by the workflow update service of SAM-IDM-127, to describe workflows and events graphically and to export them for execution; and (ii) a graphical supervision interface giving an overall view of running workflows (volumes and load) and allowing an operator to inspect a specific workflow instance, analyse its state and unblock it where needed.
SAM-IDM-080	The orchestration engine shall be based on an open source workflow engine distribution, or an equivalent engine giving SBS the same rights, so that SBS can move to new versions in the future and benefit from the plugins and evolutions of the community. The corresponding source code shall be delivered.
SAM-IDM-081	The nominal identity creation workflow shall at least: verify that the person is eighteen (18) years of age or over; verify that the person is biometrically unique; and verify the link with the civil registration record in the CRVS system. When all checks pass, the workflow shall end with the activation of the SDIN and the notification of the card personalisation process. If the person is not biometrically unique, an investigation shall be launched through the adjudication and fraud workflows. If the CRVS link cannot be confirmed at the time of processing, the activation of the SDIN shall not be blocked: the record shall be activated, subject to successful deduplication, and placed in a deferred CRVS attachment queue, with automatic follow up upon notification from the CRVS system and a dashboard showing the stock of records not yet attached. Where the application has a documentary basis compliant with sections 19(3) and 19(4) of the NDID Act 2024, or an established CRVS record, activation shall carry the full active status; where it has neither, activation shall carry the status "active, legal status clarification pending" of SAM-IDM-028, and the record shall be routed to the legal status clarification process

	(SAM-ENR-011, SAM-CRV-030). The final workflow shall be validated during the specification workshops.
SAM-IDM-082	The implementation of the business workflows shall guarantee scalability and the insertion of new tasks without recoding the application; a microservice decomposition is an acceptable means, but no one microservice per process step is mandated. The source code of the services specific to the Samoa business processes and of the interfaces to external systems shall be delivered, as they are part of the customisation of the System and are necessary to guarantee continuity of service over time.
SAM-IDM-083	The Supplier shall deliver the unique identification module, which establishes the uniqueness of a person following biometric enrolment. This module drives the ABIS for deduplication and the manual adjudication application. Once biometric uniqueness is established, it shall obtain the SDIN by invoking the standalone unique number generator of SAM-IDM-022 (delivered with its full source code and documentation, operable by the Purchaser independently) and shall activate the SDIN for downstream services.
SAM-IDM-084	When a duplicate is detected, the unique identification module shall notify all systems subscribed to the "duplicate detected" event through the publish and subscribe mechanism defined in this Section. Where the duplicate is detected before activation, the provisional SDIN bound to the affected application shall be voided and permanently retired per SAM-IDM-022 and SAM-ENR-144, without ever being activated or assigned to any person. Where the duplicate concerns an already activated identity, the SDIN concerned shall be suspended (not deactivated) pending resolution, consistently with the state model of SAM-IDM-028 and the "deactivated" response rule of SAM-IDV-011.
SAM-IDM-141	The System shall provide a subscription based notification service through which authorised systems are informed of identity events and civil registration events as they occur, without having to poll the registries. The Population Registry and the Civil Registry shall each expose the service in both directions, publishing and subscribing. Sub requirements SAM-IDM-141.01 to SAM-IDM-141.04 state the subscription, the event set, the collection of details and the delivery and resilience obligations.
SAM-IDM-141.01	The System shall expose an interface through which an authorised system registers as a subscriber to identity change events. A subscription shall be authorised per relying party, per use case and per event type, on the legal basis established for that use case. The System shall allow a subscription to be listed, suspended and revoked, and every subscription and every change to a subscription shall be traced with its author, its timestamp and its reason.
SAM-IDM-141.02	The event set shall cover at minimum the creation of an identity, the update of its attributes, its suspension or deactivation and the registration of a death, together with the civil registration events of birth, death and change of civil status. Each notification shall carry the event type, the date and time of the event and a reference allowing the details to be

	collected. A notification shall carry no personal data beyond what the subscriber is authorised to receive, the reference being the normal payload.
SAM-IDM-141.03	The System shall expose an interface through which a notified subscriber collects the details of the event. The response shall be limited to the data items covered by the authorisation attached to the subscription, in application of the minimisation rule of the NDID Act 2024, and every collection shall be logged in the records of use of the authentication and verification functions.
SAM-IDM-141.04	Delivery shall use callbacks over HTTPS with verification of the intent of the subscriber endpoint, signature of the delivered payload and renewal of the subscription at a stated interval, following the W3C WebSub pattern or an equivalent published mechanism proposed by the Supplier. The System shall retry a failed delivery with a progressive delay, shall allow a subscriber to reconcile the events it has missed over a configurable window, and shall lose no event when a subscriber or a source system is unavailable. The notification layer shall keep operating when any single source system is unavailable, with retry, reconciliation and audit.
SAM-IDM-085	The unique identification module being the foundation of trusted identification in Samoa, SBS intends to remain sovereign and resilient, independently of the Supplier. The SDIN generation function shall be provided by the standalone unique number generator of SAM-IDM-022, a component developed by the Supplier and delivered with its full source code, build and deployment documentation to the Purchaser, operable by the Purchaser independently of any other component; this delivery obligation is firm. The Supplier shall in addition describe in its proposal the technical arrangements that make SBS independent in the maintenance and future evolution of the unique identification module itself.
SAM-IDM-086	The person registry shall store the core identity information of individuals linked to their SDIN. It shall be built on a resilient, highly available database associated with a service API to interact with the data. The registry APIs shall be based on recognised open standards in worldwide production use, so as to guarantee interoperability and fast integration with external systems without modification. The person registry implements the Identity Database of section 27 of the NDID Act 2024: it shall contain no biometric data. Facial images, fingerprint images and signature images reside in the Biometric Database and shall be served to authorised consumers (card personalisation, adjudication, and the IDVS eKYC provisioning of the portrait image per SAM-IDV-002) through dedicated, logged services. Biometric references stored in the registry shall be opaque internal identifiers only.

SAM-IDM-087	The person registry API shall allow: (i) the injection of a new identity including its SDIN and all its biographic attributes, biometric references, contact information and, optionally, typed alias identifiers issued by other systems; and (ii) the update of one or more attributes of an existing identity identified by one of its identifiers. In both cases the System shall implement a security mechanism guaranteeing the authentic origin of the injected data, to protect against the injection of false identities or false data.
SAM-IDM-088	The SDIN shall remain unchanged for the life of the person. In case of confirmed identity theft, the response shall be the revocation and reissuance of the statutory token and of the credentials of the person, in accordance with section 32(2) of the NDID Act 2024, typically upon a court decision or a decision of the Registrar General; the SDIN itself shall never be replaced. In case of suspected identity theft, the SDIN can be suspended temporarily during the investigation and reactivated once the investigation concludes; verification services for that SDIN are unavailable during the suspension period. All these operations shall be fully traceable.
SAM-IDM-089	Consultation APIs shall be available for all non biometric data of an individual, excluding the portrait. The use of these APIs shall be strictly reserved to the subcomponents of the IDMS and shall not be exposed publicly. In addition, the IDMS shall provide APIs allowing the implementation of a self service web portal, a mobile application or a customer care function, in the conditions defined in the architecture block.

ABIS (outcome based)

The biometric matching engine is specified through measurable outcomes, accuracy, throughput and reporting, not through internal design: bidders propose the engine, the contract holds the results.

ID	Requirement
SAM-IDM-090	The ABIS is the component performing the biometric deduplication (1:N search) of individuals. On completion of its processing it shall determine whether an identity is unique or not on the basis of the available biometric and biographic information, and shall route undecided cases to the manual adjudication application.
SAM-IDM-091	The ABIS shall perform deduplication using the two biometric modalities enrolled in Samoa: facial portrait and ten flat fingerprints. The handwritten signature is captured and stored as the digitised representation of the captured signature image, kept as identity data, and shall not be used as a matching modality. Iris is not captured and shall not be required. The ABIS may use any combination or fusion of the two modalities to achieve the accuracy targets.
SAM-IDM-092	The ABIS shall be sized for the gallery volumes defined in VII.1.5 (SAM-PER-001), and shall be scalable to the full lifetime gallery without redesign and without blocking or prohibitive cost for SBS. For the avoidance of doubt, the maximum gallery the ABIS shall support without redesign is 250,000 identities (multi modal records per SAM-PER-001), with licensing and pricing stated up to that volume in the proposal.
SAM-IDM-093	The ABIS shall achieve a false negative identification rate (FNIR) of no more than 0.5% at a false positive identification rate (FPIR) of no more than 0.1% on the Samoa gallery, measured under the conditions defined in the acceptance test plan. The System shall be capable of reporting the measured FPIR and FNIR.
SAM-IDM-094	The deduplication throughput of the ABIS and of the identity creation chain shall be compatible with the peak daily intake defined in VII.1.5 (SAM-PER-002, SAM-PER-015), with a 1:N search completing in no more than ten (10) seconds on the full gallery, so that no persistent backlog builds up during the mass enrolment wave. The ABIS shall be available in line with the service levels defined elsewhere in this Section and shall have no single point of failure.
SAM-IDM-095	Accuracy claims shall be supported by evidence from recent independent public benchmarks relevant to civil identity use: for fingerprint technology, the NIST PFT III

	evaluation (one to one) and MINEX III (template interoperability) where applicable; for face technology, the NIST FRTE one to one and one to many tracks. An equivalent recent independent public benchmark is accepted. Published results shall be consistent with the accuracy targets of this Section. In all cases, the accuracy targets shall be verified on Samoa data during acceptance.
SAM-IDM-096	The 1:N search result shall not be affected by the inversion of thumb placement in slap images, and the ABIS shall tolerate the fingerprint exceptions recorded at enrolment (missing or unreadable fingers) without manual intervention.
SAM-IDM-097	The ABIS shall be robust to gallery growth. It shall be structured to allow the replacement, upgrade or insertion of a new matching algorithm at SBS request, without loss of data and without dependence on a single supplier.
SAM-IDM-098	The System shall preserve the source biometric data (face images and fingerprint images) in standard formats allowing their external reuse: fingerprints in WSQ with a compression factor not exceeding 1:5 (or an equivalent open standard), portraits in accordance with ISO/IEC 19794-5 or ISO/IEC 39794-5. Access to these data shall be strictly limited and logged, and their storage shall be secured.
SAM-IDM-099	To protect SBS against proprietary lock in, the System shall maintain protected and accessible copies of the source images of the captured biometrics, duplicated continuously into a secure storage system under SBS control, so that in case of a change of ABIS supplier the biometric gallery can be rebuilt in full. The ABIS shall interface with the unique identification module through an open interoperability standard supported by several suppliers and already deployed on production platforms.
SAM-IDM-100	The ABIS shall use an internal biometric identifier which is not the SDIN. It shall be possible to suspend or deactivate an SDIN while keeping the same internal biometric identifier in the ABIS, in support of the identity lifecycle and of the revocation and reissuance of the statutory token and credentials (the SDIN itself is never replaced, see SAM-IDM-088).

Adjudication workstations and application

The tooling of human decision making: workstations suited to facial comparison, an application that presents the evidence, and controlled decision paths.

ID	Requirement
SAM-IDM-101	The adjudication application shall allow a human operator to manually compare a full enrolment record with the list of duplicate candidates identified by the ABIS, two records at a time. It shall be a web application, so that additional operators can be given access on non specific workstations when needed.
SAM-IDM-102	The adjudication application shall manage a queue of adjudication requests assigned automatically to adjudication operators. A supervisor shall be able to modify an assignment, and an operator shall be able to reassign a case to a more senior operator, for example when unable to reach a decision. The queue catalogue shall follow the adjudication case catalogue consolidated with SBS, including the eligibility ineligibility and biometric refusal queues, whose routing (desk versus central refusal) is confirmed at the design stage. Adjudication capacity shall be sized to absorb the legacy discrepancy caseload in addition to the enrolment flow.
SAM-IDM-103	The adjudication application shall allow the operator to compare side by side the enrolled modalities (fingerprints and facial portraits), the stored signature images and the biographic data of the candidates proposed by the ABIS, with mechanisms facilitating the pairwise comparison of portraits and of text data.
SAM-IDM-104	The adjudication application shall allow the operator to take a decision on the uniqueness of the examined person, or to declare a candidate as identical or suspect and reject the identity creation. Each decision shall be preserved for later audit with the unambiguous identification of the operator, the workstation, the date and time, the verification points checked and, for any rejection, a systematic, clear and detailed comment. The audit trail shall use a structured text format easy to process programmatically (JSON, YAML, XML or equivalent), referencing internal identifiers and the SDIN where relevant.
SAM-IDM-105	The adjudication application shall support a configurable adjudication workflow, including parallel adjudication of the same case. The configurable second validation of adjudication decisions (second review by another operator or a supervisor) is specified in SAM-IDM-042.
SAM-IDM-106	The Supplier shall provide the workstations needed for manual adjudication: fixed stations with a wide screen of 27 to 32 inches and 4K or QHD resolution suited to facial

	image comparison, keyboard and mouse, running Windows 11 or later, or an equivalent desktop operating system under the same conditions as SAM-ENR-074, protected by antivirus software at no additional charge. The number of stations shall be sized for the expected manual adjudication workload, with eight (8) stations as the working assumption (acceptable range five to ten), and stated in the proposal with unit prices.
SAM-IDM-107	Adjudication operators shall authenticate on the workstations with two factor authentication providing a high level of assurance, so that their identity is certain and accountable in case of fraud. Operator access on the workstations shall be restricted to the adjudication application, enforced either by workstation lockdown or by role based identity and access management using operator certificates and roles, unless expressly requested by SBS.
SAM-IDM-108	Adjudication operators will be provided by SBS. The Supplier shall support SBS in their selection (job descriptions, participation in candidate evaluation), provide their initial training, supply the adjudication procedures, and supervise the adjudication operations with regular reporting on volumes, decisions and incidents. The corresponding staff profiles are defined in Section III.

Case management (fraud cases)

Suspected fraud follows its own workflow with chain of evidence controls, so findings hold up in legal or disciplinary proceedings.

ID	Requirement
SAM-IDM-109	The System shall provide a single case management queue inside the supervision and adjudication application, handling cases of the types anomaly, fraud and investigation, with assignment, priority, status tracking and reporting per case type. Fraud cases shall give access to the applications identified as fraudulent and to the associated reasons, from the web administration interface of the IDMS. The case handling processes shall be BPMN workflows executing in the IDMS orchestration engine, which SBS shall be able to enrich later with its own processes under the doctrine of SAM-IDM-078 and SAM-IDM-127; the implementation of such future workflows is not in the scope of the contract, but giving SBS the capacity to implement them is. No separate fraud or anomaly application shall be delivered.
SAM-IDM-110	The System shall maintain fraud control lists used during processing, including at least: records flagged as suspect, and enrolment stations or operators that have been deactivated or are under investigation. Matches against these lists shall route the affected applications to the fraud workflow. Fraud cases shall carry chain of evidence controls: integrity protection of the case record, custody of the supporting evidence, and an exportable audit trail suitable for legal or disciplinary proceedings.
SAM-IDM-111	The Supplier shall provide access to fraud specialists as a bank of on demand expert days, priced in the proposal, mobilised at the request of SBS when frauds are identified, to support SBS and to help it follow the identified cases through to closure. No standing fraud specialist team is required on site.
SAM-IDM-112	The Supplier shall perform root cause analysis of the exceptions and frauds identified during the project, implement processes to resolve them, support SBS in their technical implementation, and report regularly on fraud cases, trends and resolution status.

Case management (anomaly cases)

Anomalies that are not fraud, data faults and processing incidents, get their own managed queue so they are fixed, not lost.

ID	Requirement
SAM-IDM-113	Rejected applications shall be handled as cases of type "anomaly" in the single case management queue of SAM-IDM-109. Anomaly cases shall give access to the applications and to the reasons for rejection, from the web administration interface of the IDMS, and shall follow BPMN workflows executing in the IDMS orchestration engine, which SBS shall be able to enrich later following its own processes, in the same conditions as for fraud cases.
SAM-IDM-114	The case management function shall provide statistics and reports on anomalies by type, origin (station, operator, region) and period, in support of quality management of the enrolment operations, served through the shared BI and reporting layer of SAM-IDM-117.

Supervision and monitoring

Operational visibility over the identity pipeline: queues, backlogs, throughput and alerts for the teams running the system.

ID	Requirement
SAM-IDM-115	The System shall provide a web administration and supervision application to manage requests, identities and the documents held by individuals. Access shall be restricted to authorised personnel, with roles giving access either to requests only (operations staff) or to the full information (investigation staff).
SAM-IDM-116	The supervision application shall allow SBS to follow the status of a person's registration file end to end across the services of the NDIDS programme, including at least: biometric enrolment, IDMS processing, CRVS verification, card personalisation, card distribution and delivery, and the lifecycle of the documents held.
SAM-IDM-117	The supervision application shall include dashboards for SBS giving a synthetic view of: production volumes (enrolments received, identities created, SDIN activated), processing queues and backlogs, rejection rates by cause, adjudication workload and decisions, and the statuses of individuals in the registry. These dashboards shall be views of the single BI and reporting layer shared across all components of the NDIDS, not a separate reporting build. The exact content shall be defined during the project.
SAM-IDM-118	The supervision application shall raise alerts related to the service levels and performance targets, in particular on queue build up, abnormal rejection rates and processing delays, on the same shared supervision and reporting layer.
SAM-IDM-119	The supervision application shall allow searching for a registration file or an individual by SDIN, by name, given names and date of birth, or by a document number. Results shall be displayed as a list showing the search attributes and the latest status on each line; a click on a line shall open the supervision page of the file or the data page of the individual.
SAM-IDM-120	The supervision page of a file shall give access to the latest global status, the full status history with timestamps, the metadata reported, and the related alerts. The identity section shall allow viewing an identity, the known attached identity documents and the creation file of the identity, excluding fingerprint biometric data.
SAM-IDM-121	The public online status enquiry is specified in SAM-IDM-038 (status check by application reference, exposing no personal data beyond the status itself). In support of it, a web service shall be provided and installed on a public portal provided by SBS, so that the status can also be accessed from a web portal or another channel retained by SBS.
SAM-IDM-122	The source code of the supervision application shall be delivered, and the SBS teams shall be trained on it after go live, so that SBS can make it evolve with the NDIDS ecosystem without time limitation.

Test environment

A permanently available environment where SBS and its partners can test, integrate and experiment without touching production.

ID	Requirement
SAM-IDM-123	In addition to the production environment, the Supplier shall deliver and maintain at least the following environments: test, staging (pre production) and training. These environments may be sized smaller than production and mutualised where justified, and shall be usable by SBS for experimentation, integration testing with other systems and training without impact on production.
SAM-IDM-124	The Supplier shall provide an operational IDMS instance for the test environment, allowing SBS and its partners to test the delivered components, integrate them with other systems, and experiment with new use cases. The corresponding IDVS test environment instance is specified in the IDVS and relying parties block.

Operations support

The support obligations around the running IDMS: assistance, incident handling and the operating documentation kept current.

ID	Requirement

SAM-IDM-125	The Supplier shall implement all the services necessary for the operation, support and maintenance of the delivered modules, in order to guarantee the availability of the unique identity creation service in accordance with the service levels defined elsewhere in this Section.
SAM-IDM-126	The Supplier shall state in its proposal the exhaustive list of the operation and support services it proposes in this respect, including the tooling used.
SAM-IDM-127	The Supplier shall provide a workflow update support service: a series of services to accompany SBS in learning and then practising the modification of existing business workflows and the creation of new ones, using the open workflow standards (BPMN) implemented in the System. These services shall be described in the proposal, shall appear in the execution schedule, and shall be aligned with the capacity building annex of this Section.

Exit transition and reversibility

The platform must survive its Supplier: reversibility, data and configuration handover, and an assisted transition period protect Samoa's continuity at contract end.

ID	Requirement
SAM-IDM-128	The last phase of the contract shall be an exit transition phase with three objectives: (i) ensure that all assets and their ownership rights have been transferred to SBS (equipment, licences, secrets, subscriptions); (ii) make SBS autonomous in continuing to operate the System; and (iii) support SBS in redeploying the hardware and software for the continuous enrolment service following the mass enrolment wave.
SAM-IDM-129	The Supplier shall prepare an exit transition plan, based on the transition terms of reference provided by SBS, to be approved by SBS. The plan shall include an assisted transition period of six (6) months after handover, during which the Supplier remains available to support SBS operations teams.
SAM-IDM-130	The System shall be fully reversible, as specified in SAM-ARC-038 (complete export of all data, configurations, workflow definitions and parameter sets, executable by the Purchaser, in open, documented formats, tested during acceptance). In addition, the export procedures shall be retested during the exit transition.
SAM-IDM-131	The exit services shall include: delivery of the final updated versions of all documentation, training sessions, and theoretical and practical skills transfer sessions covering all the services managed by the Supplier until then, together with the transfers of ownership. These services shall be aligned with, and not duplicate, the capacity building annex of this Section, which defines the skills transfer mechanism, its evaluation and the associated retention.
SAM-IDM-132	As a transverse requirement applicable to all blocks of this Section, all licensed software and systems shall be delivered with a perpetual licence, without time limitation and without further payment after the end of the contract. The only permitted exception concerns the infrastructure software licences of the enrolment central services identified in SAM-ENR-111, which shall cover at least three (3) years; any such exception shall be identified as such in the proposal, with its renewal cost and exit strategy.

Technology standards and interoperability

The open standards the IDMS must implement so that data and interfaces outlive any product choice.

ID	Requirement
SAM-IDM-133	The System shall pass mandatory security tests covering at least the OWASP Top 10 vulnerabilities, and shall provide full audit trails for security and operational events, with the intended mechanism described in the proposal. The complete cybersecurity requirements applicable to the NDIDS as national critical infrastructure are defined in VII.1.6 and prevail over this requirement where more demanding.
SAM-IDM-134	The System shall follow a layered, service oriented architecture based on microservices, isolating the front end (user interfaces subject to fast business and technology evolution) from the back end services, the database, the file store and the messaging services, so as to open the System to multiple channels (web, mobile) and to interoperability.
SAM-IDM-135	All external interfaces of the IDMS shall be exposed as open APIs using REST and JSON, documented with OpenAPI specifications, versioned and testable by SBS and by third parties authorised by SBS. The authentication and attribute sharing standards

	applicable to the verification services (OpenID Connect, OpenID4VC, and the credential format selected under SAM-ARC-027) apply to the IDVS block and are specified in the architecture block; this subsection does not restate them.
SAM-IDM-136	The IDMS shall provide a publish and subscribe mechanism allowing authorised systems to subscribe to categories of data or events, to receive notifications when new data arrive, and then to collect the data through API. Data may be of any type: text, images, documents. The first integration shall be with the CRVS component of VII.1.2.6, which fronts the existing digital CRVS system of Samoa during V1 (civil registration events towards the IDMS, identity creation and status events towards the CRVS), with a synchronisation frequency compatible with the 28 day deadline of SAM-IDM-033; further functional systems designated by SBS shall be able to subscribe later through the same mechanism without redevelopment.
SAM-IDM-137	As a transverse requirement applicable to all blocks of this Section, the Purchaser shall be able to operate, modify and replace each component of the System without dependence on the Supplier. That outcome is satisfied either by delivery of the full source code under the conditions of SAM-IDM-138, or, for packaged software specific to the System whose publisher does not release its source, by the escrow arrangement of the Special Conditions of Contract covering the source code, the build scripts and the design and deployment documentation. For the biometric identification system, the exit guarantees named in SCC GCC 15.5 may replace escrow. Standard Software widely available on the market, such as operating systems and database management systems, is outside both routes: its replacement is ensured by open formats, documented interfaces and the data export of SAM-ARC-038. The route chosen shall be stated and justified for each component, with its exit strategy. The database shall be an established relational database whose data and schema the Purchaser can export and reuse without licence dependence.
SAM-IDM-138	For all software subject to a source code delivery requirement and for all open source software, the source code shall be delivered at the same time as the software at the relevant project milestones, archived by the Supplier in a repository made available by SBS, and covered by a skills transfer from the Supplier teams to the teams designated by SBS, in accordance with the capacity building annex.
SAM-IDM-139	The System shall implement personal data protection by design, in accordance with the NDID Act 2024 and, where the Act is silent, with internationally recognised good practice of the GDPR type: purpose limitation, data minimisation, access control and logging of access to personal data, and support for the rights of the person as defined by the Act.
SAM-IDM-140	All user facing interfaces of the IDMS (administration, supervision, adjudication, online status service) shall support English, and the public facing online status service shall also support Samoan. The System shall allow the later addition of languages by configuration.

1.2.3 IDVS and Relying Party Services (SAM-IDV-001 to 110)

Introductory note. The Identity Verification Services platform (IDVS) is the component through which authorised public and private relying parties verify identities against the national identity register. It is deliberately specified here in terms of capabilities and open standards, not products. A compliant solution may be built on established open source identity platforms or on equivalent market solutions, provided every requirement below is met through standard, documented interfaces. The credentials and wallet functions are specified in block VII.1.2.4; the CRVS reuse of the relying party framework is specified in SAM-CRV-055 to 062; cybersecurity requirements are in VII.1.6; the overall architecture is in VII.1.3. This block does not repeat them.

1. IDVS platform principles (SAM-IDV-001 to 010, 031)

The ground rules of the verification platform: minimised data, no master data storage, relying party agnosticism and the performance envelope.

ID	Requirement
SAM-IDV-001	The IDVS shall be a distinct platform, logically decoupled from the IDMS registration infrastructure, with its own databases. Registration and verification shall never share the same runtime data store.
SAM-IDV-002	The IDVS shall not store master identity data. It shall operate on a replicated, minimised verification dataset holding, for each individual, only the information needed to serve 1:1 verification and eKYC (verification biometric templates, the portrait image where authorised for eKYC release per SAM-IDV-016, and the minimal attribute set), keyed to the SDIN or to its statutory token. The replicated verification dataset, insofar as it holds biometric verification templates or the portrait image, shall be governed as part of the Biometric Database regime of section 38 of the NDID Act 2024: used solely for authentication of registered persons, held separately from any identity attribute store, and accessible only to specifically authorised personnel.
SAM-IDV-003	The identifiers exposed to relying parties shall be the SDIN or the single statutory token of section 31 of the NDID Act 2024: one token per SDIN, stable, notified to the person, and revocable and replaceable in accordance with section 32(2). The IDVS shall not create or manage relying party specific aliases of the SDIN.
SAM-IDV-004	The IDVS shall be highly available. It shall be deployed redundantly with no single point of failure and shall expose multiple service endpoints so that verification remains continuously available even during maintenance of individual nodes.
SAM-IDV-005	The IDVS shall be deployable, upgradable and scalable independently of the IDMS. Planned IDMS maintenance or an IDMS incident shall not interrupt verification services, which shall continue to operate on the replicated verification dataset.
SAM-IDV-006	The IDVS shall be dimensioned for the Samoan context: a target volume of 5,000 verification and eKYC transactions per day at steady state, and 20,000 per day at event peaks, with an order of magnitude in the tens of thousands per day at maturity, and shall scale to at least 50 percent above the target peak hourly load without architectural change.
SAM-IDV-007	The end to end response time for an online verification shall not exceed 2 seconds under nominal load, measured at the IDVS service boundary.
SAM-IDV-008	The IDVS and all its interfaces shall apply privacy by design and data minimisation: no service shall return more personal data than the minimum required by the requesting service and permitted by the partner policy.
SAM-IDV-009	The IDVS shall be built on open standards recognised by international bodies (ISO, W3C, IETF, OpenID Foundation). The design shall be technology and vendor neutral and shall avoid dependence on any single vendor, including for future upgrades.
SAM-IDV-010	All IDVS functions shall be exposed as fully documented RESTful APIs secured in transit, published as a complete API specification enabling third parties to build compliant applications.
SAM-IDV-031	The IDVS shall apply **privacy by design compartmentalisation of personal data**, stated as an outcome: the compromise of one verification record or of one key shall not expose any other individual's record, and bulk extraction of the verification dataset shall be impractical. Per record encryption with individual keys, and envelope encryption with HSM held master keys combined with partitioning of the verification store, are both

	explicitly acceptable implementations. The Supplier shall describe its mechanism and demonstrate that it achieves this outcome.

2. Verification and authentication services (SAM-IDV-011 to 030, 106)

The service catalogue itself: verification, authentication and eKYC in all modalities, with consent enforced on every attribute release and configurable response levels.

ID	Requirement
SAM-IDV-011	Any verification, authentication or eKYC request presented against a deactivated SDIN or a deactivated token shall return the specific response "deactivated", as required by section 32(4) of the NDID Act 2024, without disclosing any further personal data.
SAM-IDV-012	The IDVS shall provide a 1:1 verification service returning a yes or no answer only: the submitted identifier and input data either match the reference record or they do not. No personal data shall be returned in a plain verification response. The IDVS shall support the authentication of a person who presents no ID credential, using the SDIN or its token together with OTP, demographic or biometric factors, so that acceptance of the SDIN or token is never conditional on the presentation of an ID credential, as required by section 33(2) of the NDID Act 2024. Beyond the plain verification response, the IDVS shall support configurable response levels per use case and per partner policy: confirmation only; attribute bundle, served through the eKYC service under its consent rules; and rich receipt including verification type, timestamp, achieved assurance level and validity semantics. The response level served to each relying party service is configuration under the assurance framework (SAM-IDV-044 to 048), not redevelopment. Verification outcomes shall distinguish at minimum: Confirmed, Not confirmed, and Unable to confirm (further action required), each with a traceable transaction reference. Service unavailability shall never be returned as a negative identity result, and shall never cause a silent downgrade to a weaker check.
SAM-IDV-013	The IDVS shall support demographic verification: a relying party submits the SDIN or the statutory token together with one or more demographic attributes (name, date of birth, sex, address) and receives a match or no match result per attribute, with configurable exact and approximate matching rules.
SAM-IDV-014	The IDVS shall support one time password (OTP) authentication delivered to the registered mobile number or email address of the individual, with time based OTP (TOTP) as a supported option. The OTP shall always be delivered to the holder, never to the relying party. The platform shall support authenticator style TOTP generation embedded in the national Digital ID mobile application, as an alternative to SMS and email delivery, reducing dependence on message delivery at authentication time; SMS and email OTP remain available. Activation of the embedded generator is confirmed with SBS at the design stage.
SAM-IDV-015	The IDVS shall perform biometric 1:1 verification **itself**: it receives the SDIN (or its statutory token) and the captured biometric sample, matches it 1:1 against the individual's verification template held in the IDVS verification dataset, and returns a yes or no answer. The ABIS remains inside the secured IDMS environment and shall never be exposed to, or invoked by, verification traffic. Biometric verification shall be offered where the applicable service policy and the law permit.
SAM-IDV-016	The IDVS shall provide an eKYC service releasing a defined attribute set (with photograph where authorised) only after successful authentication of the individual and capture of their

	explicit consent, and only within the attribute scope authorised by the partner policy.
SAM-IDV-017	Each consent given by an individual shall be valid for a single eKYC transaction. Consent shall not be reused across transactions: it shall be requested each time a relying party needs an electronic version of the person's data.
SAM-IDV-018	The IDVS shall support combined, multi factor requests (for example demographic plus OTP, OTP plus biometric, credential plus OTP) in a single transaction, each factor being verified independently against the reference data.
SAM-IDV-019	The IDVS ecosystem shall support offline verification of digitally signed QR code content carried on physical or digital credentials, without any network connection, using published verification keys. The QR content and signature scheme are specified in block VII.1.2.4.
SAM-IDV-020	The IDVS shall publish and maintain the public key material and trust lists needed by third party verifier applications to validate signed credentials and QR codes, including a documented key rotation and distribution mechanism.
SAM-IDV-021	The IDVS shall provide a credential status service allowing an authorised verifier to check whether a credential is active, suspended, revoked or expired, without disclosing any personal data of the holder. The IDVS shall not authenticate an individual relying on a cancelled ID credential (section 36(2)(b) of the NDID Act 2024): credential status shall be checked at every transaction involving a credential, and revocation data shall be published for caching so that offline verifiers can apply the same rule.
SAM-IDV-022	Every IDVS response (verification, eKYC, status) shall be digitally signed by the platform so that relying parties can verify its authenticity, integrity and origin.
SAM-IDV-023	Every request shall carry a timestamp and shall be accepted only within a configurable time window between the request timestamp and its reception by the verification server. Requests outside the window shall be rejected.
SAM-IDV-024	Before processing, the IDVS shall validate each request against at least: partner registered and active, partner API key valid, request signature valid, request within the configured time window, domain and environment details valid, request content consistent with the selected authentication mode, requested operation permitted by the partner policy linked to the API key, identifier (SDIN or statutory token) valid, and evidence of the individual's consent to the transaction (consent assertion) present and valid, as required by section 39(4) of the NDID Act 2024; requests without a valid consent assertion shall be rejected.
SAM-IDV-025	For requests containing biometric data, the IDVS shall additionally verify that the biometric block is signed by a registered capture device key and that the device attestation block is valid and within its own time window.
SAM-IDV-026	Every rejection or error shall be recorded and returned with a specific, documented, machine readable error code, without leaking personal data or the existence of a record.
SAM-IDV-027	For every processed transaction the IDVS shall generate a transaction token based on the policy defined for the partner, enabling the partner to reference the transaction without receiving or storing the SDIN.
SAM-IDV-028	After each authentication or eKYC transaction, a notification shall be sent to the registered email address or mobile number of the individual, based on rules configurable per service and per channel, in English, Samoan or both according to the individual's preference. Notification at each transaction shall be the default behaviour, in line with the National Digital

	Identification Policy (§12.5); any exception shall be configured by SBS within the limits of the law.
SAM-IDV-029	All authentication and eKYC requests and responses shall be logged for audit with a unique transaction identifier, and these logs shall feed the fraud analysis capability defined in SAM-IDV-076. The audit record of every transaction shall include the consent evidence.
SAM-IDV-030	Verification services shall be consumable from web and mobile channels, system to system integrations, and assisted channels (counter operator acting for the individual), through the same secured APIs.
SAM-IDV-106	For identities in the status "active, legal status clarification pending" (SAM-IDM-028), the IDVS shall serve 1:1 verification (biometric, OTP and demographic factors) and demographic verification in the same conditions as for any active identity, so that the person can be identified while the clarification process runs. Disclosure of the status flag to relying parties shall be configurable per partner policy by SBS. No eKYC attribute release shall occur for such identities beyond the attribute scope configured for this status in the partner policy. All service restrictions attached to this status shall be enforced through SBS configuration, without software redevelopment.
SAM-IDV-110	The IDVS shall provide a controlled service for linking existing relying party records to SDINs: identity matching against the reference data, automatic linkage for unambiguous matches, routing of uncertain matches to a review queue with an exception process, and a full audit trail of every linkage decision. The first served use case is the linkage of passport records (sized in the order of 60 to 120 requests per day at steady state); the service shall be usable by other authorised relying parties by configuration, per use case authorisation.
SAM-IDV-109	The IDVS is a relying party agnostic platform: the full modality catalogue is mandatory in scope, at minimum visual verification support, QR verification online and offline, OTP, 1:1 facial verification, 1:1 fingerprint verification, wallet credential presentation, digital seal verification and eKYC attribute services, with the assurance levels defined as predefined combinations of modalities (SAM-IDV-044 to 048) and an attribute sharing policy engine. Every capability shall be available to every authorised relying party by configuration per use case. Relying party preferences collected during preparation are expected usage profiles, documented in annex; they shall never restrict the capability set. Per relying party modality and attribute sharing configurations are settled at the post procurement concertation workshops.
SAM-IDV-108	The Supplier shall deliver, and manage end to end, the multi modal authentication and eKYC user experience serving the modality catalogue and assurance levels of this block: a consistent, usable interface covering all usage contexts, at minimum online and offline operation, use at the person's home and at a public office or service counter, and use on the person's own device and on an agent's device in attended or assisted mode (including for elderly persons, persons with disabilities and persons without a phone). The practical experience in each context is part of the procured scope. Detailed interaction elements will be provided to the Supplier at the project inception workshops, on the basis of the interaction document under elaboration with the relying parties.
SAM-IDV-107	The IDVS shall provide outbound notification services to relying parties, on the same subscription model as SAM-IDM-141: relying parties authorised per use case may subscribe to the event types relevant to their services (at minimum status changes affecting verifiability of an identity, such as

	suspension, revocation or death), and collect event details through a dedicated API after notification. No personal data beyond the event envelope shall be pushed in the notification itself.

3. Federation and standards (SAM-IDV-032 to 042)

The open standards rails of the verification services, so relying parties integrate once, against interfaces that outlive product versions.

ID	Requirement
SAM-IDV-032	The IDVS shall provide a federated authentication service compliant with OpenID Connect (OIDC), supporting at minimum the authorization code flow with PKCE, so that relying parties can integrate national identity sign in using standard OIDC client libraries.
SAM-IDV-033	API access shall be authorised through OAuth 2.0, with scoped access tokens reflecting the partner policy, and standard token lifecycle management (issuance, refresh, revocation).
SAM-IDV-034	Relying parties shall be able to use the federated service either as their primary authentication mechanism or as a secondary factor within their own applications.
SAM-IDV-035	The IDVS shall support issuance of verifiable credentials through the OpenID for Verifiable Credential Issuance (OpenID4VCI) protocol, in coordination with the credential and wallet functions of block VII.1.2.4.
SAM-IDV-036	The IDVS shall support presentation and verification of verifiable credentials through the OpenID for Verifiable Presentations (OpenID4VP) protocol, including selective disclosure of individual attributes. In Version 1 this capability shall be demonstrated through conformance evidence (results of conformance testing against the published protocol suites, or equivalent); integrated relying party use cases based on OpenID4VP are not a Version 1 delivery.
SAM-IDV-037	Credentials issued and verified through the IDVS shall conform to the credential format selected under SAM-ARC-027.
SAM-IDV-038	The IDVS shall expose standard discovery and metadata endpoints (OIDC provider metadata, JSON Web Key Sets) so that relying parties can configure their integrations automatically and follow key rotations without manual intervention.
SAM-IDV-040	Data exchange shall use open formats, JSON and JWT as primary formats, with XML supported where required for integration with existing government systems.
SAM-IDV-041	The complete API specifications for authentication and eKYC shall be published, versioned and maintained, with release notes, so that an ecosystem of applications can be developed against them.
SAM-IDV-042	No proprietary extension, SDK or licensed client component shall be required for a relying party to integrate with the IDVS. Conformance of a relying party integration shall be verifiable against the published specifications alone.

4. Assurance levels framework (SAM-IDV-044 to 052)

Note: the exact identity and authentication assurance levels for Samoa are. The requirements below specify the mechanism the platform must provide; the levels themselves will be set by SBS policy.

ID	Requirement
SAM-IDV-044	The IDVS shall implement an assurance framework distinguishing identity assurance levels (confidence in who the person is) and authentication assurance levels (confidence in the current transaction). Two or three levels shall be fixed at design stage from Annex A of the National ID Policy; a fully configurable redefinition of the levels themselves is not required and shall be offered only where native to the proposed platform.
SAM-IDV-045	Assurance policies shall be definable per service and per partner: for each relying party service, SBS shall be able to configure the minimum assurance level required and the authentication factors accepted to reach it.
SAM-IDV-046	The framework shall support combining factors (demographic, OTP, biometric, signed credential) within one transaction to reach a higher authentication assurance level, and shall evaluate the achieved level from the factors actually verified.

SAM-IDV-047	Factor mappings and per partner policies, including the minimum assurance level required per partner, shall be configurable by trained SBS administrators through the administration interface, without software redevelopment. Redefinition of the assurance levels themselves is fixed at design stage per SAM-IDV-044 and shall be offered only where native to the proposed platform.
SAM-IDV-048	The assurance level achieved shall be recorded in the transaction log of every verification, authentication and eKYC transaction, and shall be included in the signed response returned to the relying party.
SAM-IDV-049	Where native to the proposed platform, the framework should support step up authentication: when a session or transaction requires a higher level than currently achieved, the IDVS requests the additional factor rather than restarting the transaction. Step up authentication shall not be custom developed for Version 1.
SAM-IDV-050	Requests that do not satisfy the minimum assurance level configured in the partner policy shall be rejected with a specific error code indicating the level required, without disclosing personal data.
SAM-IDV-051	The assurance framework shall be documented with reference to recognised international frameworks (such as ISO/IEC 29115 and NIST SP 800-63) so that levels defined for Samoa can be mapped to international practice. Its default configuration shall implement the levels of assurance defined by the National ID Policy (section 13 and Annex A), as refined through the identity proofing and online access deliverables.
SAM-IDV-052	The Supplier shall deliver the assurance framework documentation, the default policy configuration agreed with SBS, and evidence of conformance testing of the level evaluation logic.

5. Relying party management (SAM-IDV-053 to 079)

Note: the relying party management application is the property of SBS and the operational core of this block. It implements a four stage framework: (1) registration and contract, (2) service plans, (3) monitoring, (4) audit trail.

ID	Requirement
SAM-IDV-053	The relying party framework shall include, as onboarding obligations enforced through the relying party agreement: (a) informing the individual, before each authentication request, of the data shared, the purposes and any available alternative means of authentication (section 43 of the NDID Act 2024); (b) offering reasonable alternative identification means to persons who are not registered or cannot be authenticated (section 39(5)); and (c) not refusing or significantly delaying a service due to non provision of an SDIN, token or ID credential (sections 14(5) and 39(6)). The relying party documentation shall include the reasonable alternative procedures established under section 44 for cases of failure of the NDIDS or of biometric or biographical capture or transmission. The relying party agreement shall also prohibit the caching, storage or reuse of verification outcomes: a verification result attests the status at the instant of the query only, and shall not be relied upon at any later time.
SAM-IDV-054	The Supplier shall deliver a relying party management application, owned and operated by SBS, covering the full lifecycle of relying parties, trusted service providers (TSPs) and authentication devices, and delivered with full administration documentation and training.
SAM-IDV-055	Stage 1, registration and contract: the application shall support onboarding, registration, suspension (blacklisting), reactivation and discharge of partners, with the underlying service agreement or contract recorded against the partner profile. For relying parties accessing attributes of the Identity Database, the recorded agreement shall constitute or reference the memorandum of understanding or other agreement required by section 29(3) of the NDID Act 2024; no attribute sharing shall be enabled before that instrument is recorded against the partner profile.
SAM-IDV-056	The application shall manage the partner categories of the ecosystem, at minimum relying parties, trusted service providers and device providers, and shall register and manage the authentication devices used by them.
SAM-IDV-057	The application shall generate unique partner codes and identifiers, and shall allow retrieval of the current status of any partner or registered device.
SAM-IDV-058	Stage 2, service plans: each partner shall be assigned a service plan defining the services authorised, the data attributes that may be returned for each declared purpose, the applicable assurance policy, and the transaction quotas. Plans shall be configurable by SBS.

SAM-IDV-059	The attribute scope of each service plan shall be enforced technically at transaction time: the IDVS shall never return an attribute outside the plan of the requesting partner, whatever the content of the request.
SAM-IDV-060	The platform shall enforce per partner quotas and rate limits, with configurable throttling and alerting when a partner approaches or exceeds its plan.
SAM-IDV-061	Stage 3, monitoring: the application shall provide per partner statistics and dashboards covering transaction volumes, success and failure rates, response times and quota consumption, refreshed at configurable intervals, served as views of the single BI and reporting layer shared across the NDIDS.
SAM-IDV-062	The application shall generate activity reports per partner, per service and per period, exportable in standard formats, for SBS management and for the partners themselves, produced from the same shared BI and reporting layer.
SAM-IDV-063	Stage 4, audit trail: every transaction shall leave a firm, tamper evident audit record identifying which partner verified which person (by SDIN or statutory token), when, through which service, with which result and which assurance level. Audit records shall not be modifiable or deletable by any operational role.
SAM-IDV-064	The audit trail shall be visible to the individual concerned: each person shall be able to consult the history of verifications performed on their identity (partner, date, service), through the citizen channels of section 7.
SAM-IDV-065	Authentication and eKYC transaction logs containing personal data shall be retained for a period **configurable by SBS**, up to the legal maximum of two years set by section 37(3) of the NDID Act, and shall then be deleted or irreversibly anonymised automatically. Aggregated, anonymised statistics may be kept beyond that term.
SAM-IDV-066	Onboarding shall follow a digital workflow: application by the candidate partner, review of eligibility and purpose, approval by SBS, contract registration, then technical enablement. Every step shall be traced.
SAM-IDV-067	No partner shall receive production credentials before completing integration testing in the sandbox environment (section 6) and passing the technical certification tests defined by SBS.
SAM-IDV-068	Technical certification shall be repeatable: a partner shall be recertified after any major change to its integration, and SBS shall be able to update the certification test suite as the platform evolves.
SAM-IDV-069	The application shall manage the full lifecycle of partner keys, API keys, licences and certificates: generation, secure distribution, renewal, rotation and revocation, with expiry alerts to the partner and to SBS.
SAM-IDV-070	Suspension or revocation of a partner, an API key or a device shall take effect immediately across all IDVS services: subsequent transactions shall be rejected with the appropriate error code.
SAM-IDV-071	Biometric authentication devices shall be registered before use, with their attestation keys, and shall be manageable through the same lifecycle (register, suspend, discharge, status query).
SAM-IDV-072	The platform shall support configurable charging models per partner and per service: free of charge, subscription based, or per transaction, following the fee policy approved by SBS or the Government. Changing a partner's model shall be a configuration action.
SAM-IDV-073	Transactions shall be metered per partner and per service as the basis for reporting and, where applicable, billing.
SAM-IDV-074	OPTION, exercisable when the fee policy is adopted: the billing function shall generate invoices on a configurable cycle (monthly, quarterly, yearly), notify partners, track payments and receivables, and record settlements against the partner account, with online payment integration. This invoicing chain shall be priced as a separate option; metering and quotas (SAM-IDV-060, SAM-IDV-073) remain in the base scope.
SAM-IDV-075	OPTION, exercised together with SAM-IDV-074: the application shall support suspension of service for partners with dues unpaid beyond a configurable threshold, with prior notification and automatic reinstatement once settled.
SAM-IDV-076	The platform shall analyse authentication transactions for potentially fraudulent patterns (replay attempts, bursts of similar operations from one partner or device, activity outside normal hours), with configurable rules, flagging for investigation, and alerts to SBS. Flagged transactions shall open cases of type "investigation" in the single case management queue of SAM-IDM-109; no separate fraud analysis application shall be delivered.
SAM-IDV-077	An individual shall be able to lock and unlock authentication on their own identity, globally or per authentication mode. SBS shall additionally be able to lock authentication

	for a given person in proven fraud contexts. Transactions against a locked identity shall be rejected with a generic code that does not disclose the lock to the relying party beyond what the law requires.
SAM-IDV-078	The onboarding of the 3 to 5 pilot relying parties and the five co developed use cases are specified in the capacity building annex (cross reference). The relying party framework of this section shall be used for the pilot without deviation.
SAM-IDV-079	The stated default route for the optional invoicing chain of SAM-IDV-074 and 075 is the configuration and integration of an **established ERP or billing platform, open source or commercial,** rather than custom development. The partner management application shall expose metering and account data through documented APIs enabling such an integration, and any ERP so integrated shall comply with the licensing, reversibility and skills transfer requirements of the Contract.

6. Relying party portal (SAM-IDV-080 to 090)

The single entry point for partners: onboarding, documentation, sandbox, and the operational verification channel for authorised staff of approved relying parties.

ID	Requirement
SAM-IDV-080	The Supplier shall deliver a relying party portal, the single entry point for partners and candidate partners, integrated with the relying party management application of section 5. The mandatory core of the portal is: the published API documentation (SAM-IDV-081), the sandbox with test keys (SAM-IDV-082, 083) and the SBS administered key lifecycle (SAM-IDV-069). The self service functions (SAM-IDV-084 to 086) are desirable ("should") or priced options, as stated per requirement. The relying party portal shall also operate as a real verification channel for authorised staff of approved relying parties: for an approved use case, an authorised user selects the purpose, enters or scans the identity reference, runs the permitted verification method, receives the result and any approved attributes, and obtains a traceable transaction reference. The portal and the API are two doors into the same verification service: for the same approved use case they shall apply the same verification method, permitted data, result format, consent basis and audit rules. The portal shall never allow open searching or browsing of the population (SAM-ARC-044).
SAM-IDV-081	The portal shall publish the full API documentation: specifications, release notes, versioning policy and deprecation notices.
SAM-IDV-082	The portal shall give access to an internet accessible sandbox that emulates the production environment, in which developers can make API calls and observe results using test identities, without any production data.
SAM-IDV-083	The portal shall provide sample code, public keys for the test environment, tutorials, a FAQ section and information on technical support, as a single stop for developers building applications on the IDVS.
SAM-IDV-084	In the base scope, partner keys, API keys and certificates are administered by SBS through the lifecycle of SAM-IDV-069. Self service key management for partners through the portal (request, renewal, rotation and revocation of their own keys, subject to SBS approval workflows) is desirable ("should") and may be offered as a priced option.
SAM-IDV-085	Partner facing dashboards in the portal (transaction volumes, error rates, quota consumption, service plan, invoices and account status) are desirable ("should") and may be offered as a priced option; where delivered, they shall be views of the shared BI and reporting layer, and a partner shall never see data of another partner. In the base scope, the equivalent information is available to partners through the reports of SAM-IDV-062.
SAM-IDV-086	Partner support tickets shall be handled on the single shared open source service desk of the NDIDS (or its equivalent under SAM-IDM-036), in a dedicated partner support queue separate from the citizen grievance queue (SAM-IDM-036), integrated by API. A ticket function embedded in the portal itself is desirable ("should") and may be offered as a priced option; where delivered, it shall front the shared service desk, not a second ticketing system.
SAM-IDV-087	Partner accounts shall support several named users per organisation with roles and permissions (administrator, developer, billing contact), managed by the partner's own administrator.
SAM-IDV-088	The portal shall notify partners of planned maintenance, API changes and deprecations, and expiry of their keys and certificates, through the portal and by email.
SAM-IDV-089	The portal shall comply with current WCAG accessibility guidelines and shall be usable on desktop and mobile browsers with a consistent experience.

SAM-IDV-090	Portal access shall be protected by HTTPS with current TLS versions, and partner administrator accounts shall require multi factor authentication.

7. Citizen portal and channels (SAM-IDV-092 to 105)

The person's own window on their identity: history, consents, locking, reporting and rights of access, on web and mobile channels.

ID	Requirement
SAM-IDV-092	The Supplier shall deliver a citizen portal giving each registered person an authenticated personal space for identity related services, accessible through standard web browsers. Authentication to the portal shall support multi factor authentication, and may use verification of the holder by face or fingerprint through the same verification services offered to relying parties.
SAM-IDV-093	Through the portal, an individual shall be able to track the status of their applications and requests (enrolment, update, credential issuance) and download the related acknowledgements and receipts.
SAM-IDV-094	The portal shall display the individual's authentication history: which relying party verified their identity, when and through which service, drawn from the audit trail of SAM-IDV-063 and 064. For each access, the history shall show what personal data were accessed, when, by whom, to whom the data were disclosed, and the purpose, manner and duration of the access, in line with section 51(1)(f) of the NDID Act 2024, at no expense to the individual. The portal shall state that authentication events older than the statutory retention limit of section 37(3) (two years) are no longer available.
SAM-IDV-095	The portal shall provide consent management: the individual shall be able to view the consents they have given, the data shared under each, and manage their data sharing preferences within the limits of the law.
SAM-IDV-096	The individual shall be able to lock and unlock authentication on their identity from the portal and from the mobile channel, with immediate effect (see SAM-IDV-077).
SAM-IDV-097	The individual shall be able to report a lost or stolen credential and trigger its suspension, from the portal and through assisted channels. Credential lifecycle itself is specified in block VII.1.2.4.
SAM-IDV-098	The portal shall support the right of access: the individual shall be able to view the biographic data held about them in the identity register, without exposing data of any other person. The individual shall also be able to obtain, without constraint, unreasonable delay or expense, a copy of their personal data in a commonly used electronic format, and to submit correction and deletion requests from the portal, feeding the IDMS correction workflow, in accordance with sections 30(1) and 51(1) of the NDID Act 2024.
SAM-IDV-099	The individual shall be able to set notification preferences: channel (SMS, email), and language (English, Samoan or both). Notifications shall follow these preferences for all IDVS events concerning them.
SAM-IDV-100	A public information portal (no authentication) shall present the NDIDS services: how to enrol, fees and office hours, how institutions can connect to the verification services, application forms, FAQ and news. The public portal shall publish and keep current the list of all registered relying parties, including suspensions and terminations, as required by section 40(6) of the NDID Act 2024, fed automatically from the relying party management application.
SAM-IDV-101	The public and citizen portals shall be managed through a content management system so that trained SBS staff can create, edit and publish all content in both languages without Supplier intervention.
SAM-IDV-102	All citizen facing interfaces shall be available in English and Samoan with UNICODE support, shall comply with current WCAG accessibility guidelines, and shall use responsive design usable on low cost smartphones.
SAM-IDV-103	The portal shall allow individuals to submit and track complaints and feedback concerning identity services, feeding the grievance workflow of the IDMS (SAM-IDM-036) without duplicating it.
SAM-IDV-104	For information: the Government intends to establish a whole of government single sign on in a separate initiative. The IDVS federation services (section 3) shall be designed so that the citizen account can later federate with that mechanism through OIDC, without redevelopment. No delivery obligation arises from this paragraph.

SAM-IDV-105	The mobile wallet application and the digital credentials it carries are specified in block VII.1.2.4. The citizen portal, the mobile channel and the wallet shall consume the same IDVS APIs of this block, with no parallel or private interfaces.

1.2.4 Credentials and National ID Card (SAM-CRD-001 to 092)

Samoa follows a digital first approach: a signed digital credential is issued on activation, and the physical polycarbonate card is its companion. Verification security rests on the digital elements: everything printed on the card is also stored and signed in the QR code, and the portrait is protected both in the signed QR and as a ghost picture in the MLI zone. This chapter specifies the credential infrastructure and catalogue, the card construction and security features, the personalisation chain and its logistics. Bidders should weigh physical security features against this digital anchor when proposing the card design.

Part A. Digital first credentials

The digital credential is the primary credential: issued on activation, signed in the national trust chain, carried in the wallet and verifiable online and offline.

Principles and standards

The credential model and the standards it implements, so that Samoan credentials verify anywhere the standards are understood.

ID	Requirement
SAM-CRD-001	The NDIDS shall follow a digital first approach: as soon as the identity of a person aged eighteen (18) years or over is activated by the IDMS (SAM-IDM-026), a digital national identity credential shall be issued to the person. Issuance of the digital credential shall not depend on, and shall precede, the production of the physical card. Minors shall not receive the national identity credential: the birth certificate credential is the only credential linked to persons under 18 (SAM-CRD-005, section 19(2) of the NDID Act 2024). Identities in the status "active, legal status clarification pending" (SAM-IDM-028) shall not receive the national identity credential while that status lasts: the issuance trigger fires when the status is lifted to full active status (SAM-IDM-026); the physical card is gated separately by SAM-CRD-051. The mapping of identity states and assurance levels to credential issuance (which states receive which credential type, at which assurance level) shall be a configurable matrix; its values shall be confirmed with SBS at the design stage.
SAM-CRD-002	Digital credentials shall be issued through an issuance module able to produce and sign credentials in at least two open families: the IETF SD-JWT VC (media type application/dc+sd-jwt) and the ISO/IEC 18013-5 mobile document (mdoc). A W3C Verifiable Credentials Data Model credential secured with SD-JWT (vc+sd-jwt) is not the SD-JWT family meant here. The Purchaser selects the family placed in production under SAM-ARC-027, and may later activate the other without redevelopment and without additional charge. Each credential shall be digitally signed by the national issuing authority operated on behalf of SBS, within the national trust chain of the NDIDS.
SAM-CRD-003	Credential issuance to wallets shall use the OpenID for Verifiable Credential Issuance (OpenID4VCI) protocol.
SAM-CRD-004	Credential presentation to relying parties shall use the OpenID for Verifiable Presentations (OpenID4VP) protocol, and shall support selective disclosure so that the holder presents only the attributes required for the transaction. In Version 1 this capability shall be demonstrated through conformance evidence (SAM-IDV-036); integrated OpenID4VP use cases with relying parties are not a Version 1 delivery. Credential issuance through OpenID4VCI (SAM-CRD-003) and the signed QR code of Part B are unaffected and remain full Version 1 deliveries.
SAM-CRD-005	The initial credential catalogue shall be limited to two credential types: the national identity credential and the birth certificate credential. The birth certificate credential is issued by the CRVS component of VII.1.2.6 (SAM-CRV-057) through the shared trust infrastructure of this block (same trust chain, HSM held keys and status services); its availability in Version 1 follows the release of the certified CRVS stock (certified records), and issuance from the registration flow follows the CRVS flow option. The credential infrastructure shall nevertheless be designed so that SBS can add further credential types later without redesign of the platform. The later credential catalogue may include a citizenship record credential, subject to agreement with the Immigration authorities.

SAM-CRD-006	The digital credential and the physical card shall carry the same certified data, drawn from the same IDMS record. The System shall guarantee that no divergence can arise between the data certified in the digital credential, the data personalised on the card and the data in the signed QR code. When the underlying identity data change, affected credentials shall be revoked and reissued. The revocation shall propagate to the associated document signer credential, and relying parties shall check the issuer revocation status (certificate revocation list or status list) at each verification.

Mobile wallet application

The wallet holds and presents the person's credentials: these requirements fix its scope, its security and its behaviour offline.

ID	Requirement
SAM-CRD-007	The Supplier shall provide a companion mobile wallet application for the NDIDS, available for Android and iOS, allowing a person to receive, hold, view and present their digital credentials. Access to the wallet and to credential presentation shall be protected by a local activation factor (PIN, passcode or device biometric), so that the holder can meet the obligation of section 35(2) of the NDID Act 2024 to prevent another person accessing and using the ID credential.
SAM-CRD-008	The initial functional scope of the mobile application shall be strictly limited to the national identity credential and the birth certificate credential (receipt, storage, display, presentation and status). The birth certificate credential becomes available in the wallet as the CRVS component issues it (SAM-CRD-005, SAM-CRV-057): from the release of the certified CRVS stock in Version 1, then from the registration flow under the CRVS flow option. Any extension of scope shall require prior validation by SBS. Credential status shall be verifiable both offline (signed credential validity) and through the online status query service, per SAM-CRV-062.
SAM-CRD-009	Wallet activation shall bind the wallet to the person through a secure onboarding process agreed with SBS during the specification workshops, combining the SDIN, a verified contact channel and a biometric or documentary check. The onboarding process shall be usable at SBS service points for assisted activation.
SAM-CRD-010	Credentials held in the mobile wallet shall be presentable both online and in proximity or offline settings, so that a relying party can verify a presented credential without a connection to central systems, based on the issuer signature and cached status information. The proximity presentation of the mobile document shall implement the full ISO/IEC 18013-5 proximity flow as defined by the standard (device engagement, session establishment and encryption, data retrieval, reader authentication), and shall be interoperable with independent readers as tested under SAM-TST-030.

Cloud wallet for persons without a smartphone

Note: the cloud wallet service of SAM-CRD-011 to 013 is deferred to Version 2 as a designed for capability. In Version 1, persons without a smartphone are served by the physical National ID Card and its signed QR code, verifiable offline (Part B).

ID	Requirement
SAM-CRD-011	DEFERRED TO VERSION 2 (designed for capability): the Supplier shall provide a cloud wallet service so that persons without a smartphone hold the same digital credentials as mobile wallet holders. The cloud wallet shall be operated within the NDIDS infrastructure under the control of SBS. The Version 1 credential architecture shall permit the addition of the cloud wallet without redesign, and the Supplier shall evidence this in its design deliverables.
SAM-CRD-012	DEFERRED TO VERSION 2, with SAM-CRD-011: access to the cloud wallet shall be possible in assisted mode at SBS service points and through simple channels available in Samoa (at minimum an OTP on a verified personal contact channel). Contact details flagged as not personal at enrolment shall not be usable for this purpose.
SAM-CRD-013	DEFERRED TO VERSION 2, with SAM-CRD-011: a person shall be able to hold a mobile wallet, a cloud wallet, or both, and to migrate credentials from the cloud wallet to a mobile wallet (and back) when their equipment changes, without loss of identity or history.

Part B. Physical card

The card is the companion credential: a chipless polycarbonate carrier whose trust rests on the signed digital elements it carries.

Card body and security features

The physical construction of the card: monoblock polycarbonate, security print in the transparent layers over the personalised zones, and features stated with their intellectual property position.

ID	Requirement
SAM-CRD-025	The national ID card shall be a polycarbonate card without a chip, in ID-1 format, no thicker than 0.76 mm, forming a monoblock structure at end of manufacture with no separable layers. The transparent outer layers of the laminated body shall carry printed security graphics (for example guilloche, optically variable or ultraviolet elements) overlapping the personalised zones, in particular the portrait photograph and the QR code, so that any attempt at alteration or overlay visibly damages the printed security. A die cut transparent window is not required. The Supplier shall propose the combination of features offering the best balance of security effectiveness and cost, per international best practice for polycarbonate identity cards. A security feature is non proprietary where the Proposer evidences, feature by feature, that the Purchaser can source it from at least two suppliers at the end of the Contract.
SAM-CRD-026	The card shall have a guaranteed durability of at least ten (10) years once personalised.
SAM-CRD-027	Personalisation shall be by black and white laser engraving on both faces of the card, at a print resolution of at least 600 dpi, sufficient to print a good quality portrait and a dense, reliably readable QR code.
SAM-CRD-028	No expiry date shall be printed on the card body, in accordance with the legal framework of Samoa. Card validity shall be managed digitally through the card lifecycle system and the credential status services.
SAM-CRD-029	The card body shall carry a pre printed background unique to Samoa, designed for optimal legibility of the personalised elements. The Supplier shall propose background designs in its proposal (or examples produced for other contracts) and shall work with SBS to define and validate the final design, which may use iconic elements of Samoa.
SAM-CRD-030	The Supplier shall propose security features that are effective against alteration and difficult to reproduce, and that are available from more than one supplier on the market. The Supplier shall demonstrate this availability feature by feature in its proposal, and shall state, feature by feature, the intellectual property position of each proposed feature. A feature that only the Supplier can provide shall not be proposed in the baseline set. This rule protects the sourcing of Samoa over the life of the card: SBS must be able to procure equivalent blank cards, consumables and personalisation from several suppliers. The card design, the artwork files and all design assets are in any case the exclusive property of SBS (SAM-CRD-041). The security of the card rests on the combination of features, on the controlled production chain and on the signed QR code content, not on the exclusivity of any single technique. Vendor lock in is further managed at card series level: the card design and its security features shall be refreshable at a new card series.
SAM-CRD-031	The Supplier shall prioritise the lowest card cost without sacrificing material quality, selecting the security features with the best security to price ratio. The target unit cost of the personalised card is below two (2) US dollars.
SAM-CRD-032	The card shall include a zone printable with MLI (Multiple Laser Image) technology of at least one square centimetre, for a ghost picture of the holder interlaced with the SDIN. A CLI (Changeable Laser Image) implementation is acceptable as an equivalent. The interlaced content may include the date of birth in addition to the SDIN. The Supplier shall state the intellectual property position of the proposed implementation and its personalisation equipment implications, including any tilt capable engraving hardware required.
SAM-CRD-033	The printing method and materials shall withstand heat, water, humidity and the variable tropical conditions of Samoa. The Supplier shall justify its choice of materials and engraving method with concrete, verifiable arguments in its proposal. Card body compliance shall be demonstrated against ISO/IEC 7810 and the ISO/IEC 10373 test methods. The Supplier shall describe the laser engraving approach, including the level of carbonisation and any intentional tactile raised engraving features proposed.

SAM-CRD-034	The Supplier shall provide in its proposal an exhaustive list of the physical security functions of the proposed card, describing each precisely, stating its benefits and limitations, and the international standards it relies on.

Card data content and layout

What appears on the card and where: the closed legal list of data items and the layout constraints that follow from it.

ID	Requirement
SAM-CRD-036	The front of the card shall carry only the five data items permitted by section 34(4) of the NDID Act 2024: the name of the holder; the SDIN or the statutory token (or both); the date of birth; the image of the signature of the holder; and the portrait photograph. Where a name exceeds the printable field, the Supplier shall apply documented truncation rules, stated in the design file and applied consistently to the printed card and to the content of the QR code, the full name always being retained in the Identity Database. In addition, the front shall include the MLI zone with a ghost picture of the holder interlaced with the SDIN, subject to legal confirmation that this combination of two permitted elements (photograph and SDIN) complies with section 34(4). The final position of the MLI zone is deferred to the design workshops. No other data shall appear on the front of the card. The card layout shall reference the ICAO Doc 9303 or the EU ID 1 card layout zoning, and the bidder shall return its proposed layout together with the technical considerations on construction, personalisation and durability that constrain it.
SAM-CRD-037	The back of the card shall carry the signed QR code described below, plus any complementary printed data agreed in the design workshops.
SAM-CRD-038	The Supplier shall first propose the card design, then rework it during the design workshops at the start of the project until print ready artwork is approved. The card design process is politically sensitive: the Supplier shall carry out all design concept work and specimen production needed until the authorities of Samoa approve the design.
SAM-CRD-039	The Supplier shall attach to its proposal physical sample cards (actual printed cards, not only design artwork), realistic and representative of the proposed design, allowing evaluation of the background, the portrait engraving, the QR code on the back and the printed texts, accompanied by high definition photographs of both faces reproduced full page in the technical proposal.
SAM-CRD-040	The Supplier shall provide a card design application allowing SBS to create and modify card designs (front and back), with named designs, version management, fixed and variable text and image fields, on screen preview with default data, and printing of test cards bearing a visible and indelible SPECIMEN marking. The files produced shall be directly usable by the card personalisation system. The Supplier shall install the application on SBS workstations and train SBS teams to create and modify designs autonomously. Design creation and modification remain bounded by the manufacturing and security integrity constraints of the card body, such as background print compatibility and minimum distances between security features; the application or its accompanying documentation shall make these constraints visible to the designer.
SAM-CRD-041	The final card design, the artwork files and all design assets shall be the exclusive property of SBS.

Signed QR code

The QR code makes the card self verifiable: every printed element is also stored and signed in it, and the portrait template supports strengthened offline verification.

ID	Requirement
SAM-CRD-044	The back of the card shall carry, first, the printed data moved from the front for compliance with section 34(4) of the NDID Act 2024: the document number, the date of issue and the issuing authority. The back shall also carry a digitally signed, compressed QR code that can be verified offline, without any connection to central systems, whose content and encoding are specified in the following requirements. The card QR is a static signed credential verified offline, chosen for verification in places without connectivity and for inclusion of persons without a smartphone. The verifier does not contact the issuer at the time of verification. The QR carries only the data of SAM-CRD-045, so selective disclosure is not offered on the card: it is offered by the mobile credential (SAM-CRD-004, SAM-CRD-010), and online checks go through the IDVS (SAM-CRD-049).

	No more than one QR code shall appear on any face of the card. Blank card stock shall carry no personalised or document specific data: the document number, the date of issue and the QR code content are applied at personalisation only, and blank stock control shall rely on the blank document number of SAM-CRD-091 and on batch level identifiers managed by the consumables stock management function.
SAM-CRD-045	The QR code shall contain at least: the document number; the SDIN or its statutory token; the biographic data of the holder; and the biometric template of the portrait in an interoperable format. The portrait template is retained by design as a means of strengthened, secure offline visual verification. No fingerprint data shall be included in the QR code. The QR payload capacity shall be assessed at the design stage (the portrait template is retained subject to that assessment and to a suitable error correction level), and the profile of SAM-CRD-046 shall be selected and its encoding parameters fixed at the design stage. Should the payload capacity assessment show that the portrait template does not fit in a symbol readable under SAM-CRD-048 in any of the profiles trialled, the reduction of the template (resolution, format) or its removal shall be decided with SBS at the design stage, with the re scoping of the offline verification functions described below. Should the legal reading conclude that the MLI zone cannot appear on the front of the card, concessions on the QR content (in particular the portrait template) shall be decided with SBS during the design phase in order to preserve strengthened offline visual verification. Any concession on the portrait template shall entail a re scoping of the offline verification functions that rely on it, in particular SAM-CRD-049 (offline portrait check) and SAM-CRD-086 (offline face verification at delivery). The payload capacity assessment shall be confirmed by an engraving trial on the design stage specimens of SAM-CRD-038, before the profile, the geometry of the symbol and the retention of the portrait template are frozen. The trial covers the IETF SD-JWT VC, the fallback profile proposed and, where the Purchaser designates one, the profile designated under SAM-CRD-046. The specimens shall be engraved on the pre printed background submitted for approval at the resolution of SAM-CRD-027, on the personalisation equipment proposed for the Contract or equipment of the same model, and their QR code content shall be read and verified with the verification application on reference devices and with at least one verifier built only from the published specifications and verification keys, under representative lighting and wear. Where the artwork of the QR zone changes after the trial and before the approval of the card design, the trial is repeated on the changed background for the profile selected. The trial record shall state, for each profile, the QR version, the error correction level, the module size, the resolution and format of the portrait template used, the read rate obtained and whether the portrait template fits. The trial protocol is shared with the World Bank task team before the trial, and the trial record after it. On the trial record, the Purchaser selects the IETF SD-JWT VC if it keeps the portrait template readable, otherwise the fallback profile trialled that does, and if more than one fallback profile does, the one with the higher read rate. The specimen production of SAM-CRD-038 serves both design approval by the authorities of Samoa and this trial, and neither purpose replaces the other.
SAM-CRD-046	The QR code content shall be a compact credential, digitally signed and verifiable offline. The envisaged profile is the IETF SD-JWT VC (media type application/dc+sd-jwt), subject to its capacity to carry the data of SAM-CRD-045, the portrait template included, in a symbol readable under SAM-CRD-048. Failing that, another equivalent profile that is standard and mature applies. Standard means an open specification published by a recognised standards body, such as the IETF, ISO/IEC, ICAO or W3C, that any party may implement on royalty free terms and without restriction on use, the purchase price of the published document aside; a proprietary or vendor specific profile is not a standard profile under this requirement. Mature is assessed by the Purchaser at the date of selection, in particular on the evidence provided by the Supplier on the status of the specification, its independent implementations and its deployments at scale, and the assessment is recorded in writing with the trial record of SAM-CRD-045. An example is a CBOR Web Token (IETF RFC 8392) signed with CBOR Object Signing and Encryption (IETF RFC 9052), provided it is a self contained credential, read from the symbol alone and verified with the published verification keys and status information only. Whichever profile is selected, its claim set and data model as used for Samoa shall be published, or shall be delivered to the Purchaser and published by it as the national card profile, so that any relying party can build a verifier from published material alone. The Proposer shall propose a fallback profile, demonstrate that an offline verifier for it is publicly available or is delivered under the Contract, and state for each profile the expected QR version, error correction level and physical dimensions of the symbol at the engraving resolution of SAM-CRD-027. The Purchaser selects the profile at the technical inception workshops, before the approval of the card design at milestone M1, on the results of the engraving trial of SAM-CRD-045, and may designate for the trial one

	equivalent standard and mature profile other than the one proposed, that meets the conditions of this requirement and has a publicly available offline verifier. The Purchaser designates it no later than the start of the technical inception workshops, so that it is trialled together with the others. The trial and the delivery of the profile selected, its offline verifier included, are within the contract price and carry no additional charge. The QR code content shall use only open and published encodings, with no proprietary encoding, compression or data structure, and shall contain no URL and no reference to a service controlled by the Supplier or by any third party: verification relies only on the QR content, the published verification keys and the published status information (SAM-IDV-019 to SAM-IDV-021). The encoding parameters (QR version and error correction level) are fixed at the design stage with the profile selected. The QR code content shall be signed within the same national trust chain as the digital credentials of Part A, with signing keys generated and held in the HSMs of SAM-INF-040, so that one verification infrastructure covers both the digital credential and the card. The card QR signing key is dedicated to that use and is not shared with the signing of the credentials of Part A; the usage period of its private key is limited under the Key Management Plan of SAM-CYB-110, and its certificate remains valid for that usage period plus the validity period of the cards it signed, as for ICAO document signer certificates, under the CP/CPS of SAM-INF-045. For the IETF SD-JWT VC the applicable version is the RFC if published by the proposal deadline, failing which the latest Internet Draft published at that date. For any other profile it is the edition in force at the date of selection. A later version is adopted at the design stage with the agreement of the Purchaser.
SAM-CRD-047	The full source code of the QR code generation module shall be delivered to SBS, with a build, test and deployment training, in order to guarantee the sovereignty of Samoa over its card.
SAM-CRD-048	The QR code shall be engraved with a module size that is a multiple of the printer pitch, with sufficient margin, so that readability is guaranteed at the 600 dpi engraving resolution. QR readability shall be a systematic quality control criterion.
SAM-CRD-049	Cards shall be verifiable through the IDVS defined in section VII.1.2.3, both online (status included) and offline (signature and portrait check from the QR code). The Supplier shall provide the verification libraries and sample programs, with source code, needed by SBS and relying parties to read and verify the QR code without any per verification fee.

Personalisation systems and equipment

The production chain that turns blank cards into personalised ones: laser engraving pools, sites and throughput, sized on the stated production rates.

ID	Requirement
SAM-CRD-051	The National ID Card shall never be personalised for a person whose legal identity is not confirmed: the personalisation of a card shall be triggered only once the person's civil registration link is attached to their identity record, or once the Registrar General has formally confirmed the documentary evidence of sections 19(3) and 19(4) of the NDID Act 2024 where no civil record is retrievable, per the issuance gate of SAM-IDM-057. The digital credential of SAM-CRD-001 may precede the card and is not subject to this gate.
SAM-CRD-052	The Supplier shall provide a card personalisation system. Personalisation requests shall be triggered by the IDMS (or another authorised system) through a secured API operating in publish and subscribe mode: the requesting system publishes a print request with a token, and the personalisation system then retrieves the card data and launches production.
SAM-CRD-053	Before production, the system shall allow an SBS operator to verify the request file and validate the issuance of the card from one or more workstations. The validation workflow, which may include more than one validation step, shall be settled in the specification workshops.
SAM-CRD-054	The personalisation system shall connect to a pool of desktop laser engraving units, providing redundancy through more than one device and scalability, shall be able to direct card engraving to any production site, and shall operate per card or per batch of cards.
SAM-CRD-055	The print station software shall operate in pooling mode with publish and subscribe: whenever a station has printing capacity, it requests the next card for its centre and takes exclusive ownership of that request. Each station shall be able to drive several printers. Licences for the station software shall be perpetual, one per physical station delivered.

SAM-CRD-056	The card printers shall be desktop laser engraving printers for polycarbonate ID-1 cards up to 0.76 mm thick, engraving both faces in black and white, with a throughput of at least 150 cards per hour per printer in double sided black and white printing (taking into account the card design: one portrait, one dense QR code and text on both faces), an input hopper of at least 200 cards, a security lock on consumables, and USB, Ethernet or WiFi connectivity. Printers shall be delivered, deployed, installed, configured, tested and commissioned by the Supplier at the production sites, with a warranty covering the contract duration and a spare parts stock. The printers shall include a specimen engraving function for the production of test and specimen cards.
SAM-CRD-057	The Supplier shall provide locked down print stations and quality control stations (desktop computers with screens, QR scanner on the quality control stations, endpoint protection), configured to prevent any use other than their intended purpose. As a baseline for pricing, each personalisation site shall be equipped with at least two print stations and one quality control station.
SAM-CRD-058	The Supplier shall provide quality control software covering all personalised elements, in particular QR code readability, correct engraving of texts and portrait, and overall document quality. It shall be interconnected with the personalisation system to report accepted and rejected cards, and rejected cards shall be re personalised. The Supplier shall deliver a defect library at delivery, updated during the first months of production and regularly thereafter.
SAM-CRD-059	The Supplier shall provide a personalised card management system handling the full card lifecycle: printing, quality control, packaging, storage, transport, reception, storage pending delivery, delivery to the holder, and loss or theft, then the post delivery lifecycle to end of life (cancellation, loss, theft, renewal).
SAM-CRD-091	Every movement of blank card bodies and of personalised cards shall be recorded as a custody transfer between two named, individually identified holders. The Supplier shall have a unique blank document number printed on each blank card body by the card manufacturer at production. This number is distinct from the document number applied at personalisation and carries no personal data; every custody transfer, destruction and reconciliation is recorded against it. The chain shall cover at minimum: withdrawal from the main warehouse, receipt at a production site, issue to a print station, passage through quality control, packaging into a box, transport between sites, receipt at a delivery point, issuance to the holder, and the return of unused card bodies and of personalised cards not yet issued to the main warehouse or to the production site. The card management system of SAM-CRD-059 and the consumables stock management system of SAM-CRD-070 shall hold these transfers as a single continuous record per card body and per batch, reconcilable at any moment through the location and status service of SAM-CRD-089. Each transfer shall be attributable to an individual account under SAM-CYB-032, and no person shall be able to record a transfer on behalf of another, except under the forced return below. Where the holder of record is not available, a custodian designated by the Registrar General, acting together with a second authorised person, shall be able to record a forced return of the stock held under that holder's name; the forced return shall record the reason and the identity of both persons, shall be followed by a physical count reconciled against the record, and shall be reported to SBS. A card body or a batch whose custody chain is broken shall be flagged automatically to SBS and shall not be issued until the break is resolved and recorded.
SAM-CRD-060	The card management system shall keep the IDMS and authorised third party systems informed of every card status change, and shall notify the holder when their card is available, stating where, when and how to collect it.
SAM-CRD-061	The personalisation system shall keep the history of prints performed, and shall purge personal data once the card is printed, keeping only audit and history data.
SAM-CRD-062	The Apia production site shall include a signature HSM server for the signing of the QR code content and credentials, delivered with perpetual software licences. Under the Salelologa production line option (SAM-CRD-076), the second site shall include the same signature HSM capability. This signing service is provided by the operational HSM resilient pair of the trust infrastructure (SAM-INF-040 to 048), hosted in the secured hosting sites and not in the card production premises: personalisation events submit the data to be signed to the central signing service and receive the signed objects for engraving, so no HSM is hosted in the production centre.
SAM-CRD-063	The connection between the personalisation system and the print stations shall be secured against interception and fraud. In case of a physical print quality problem, the operator shall be able to trigger the reprint of a card.
SAM-CRD-064	The personalisation capacity shall be dimensioned for the volumes of Samoa: an initial issuance wave covering the enrolled adult population and a steady state renewal flow,

	within a total contract volume in the order of 250,000 cards. The Supplier shall state in its proposal the daily production capacity per site and the assumptions used (shifts, working days, printer availability).
SAM-CRD-065	For each main use case (card print request, duplicate request, print processing, quality control, delivery) the proposal shall include a dedicated section with flow diagrams and BPMN diagrams describing each workflow step and how it will be implemented functionally and technically. The list of use cases shall be completed during the specification workshops.
SAM-CRD-066	The System shall support the collection of citizen fees where provided by the fee regulation, implementing SAM-LEG-014: configurable fees for duplicate cards, expedited processing and holder initiated corrections, with receipts and reconciliation reporting, and configurable gratuity rules (the first card, standard corrections initiated by SBS, and any category defined by regulation shall be configurable as free of charge). Fee schedules and gratuity rules shall be configurable by SBS without redevelopment.

Consumables

Blank cards and production consumables, sized on the contract volume with a justified wastage allowance and non proprietary supply.

ID	Requirement
SAM-CRD-068	The Supplier shall supply blank polycarbonate cards without a chip, in ID-1 format, up to 0.76 mm thick, conforming to the security construction of SAM-CRD-025, pre printed with the validated Samoa background, for the personalisation of the cards. Blank cards shall remain fit for personalisation after at least six (6) years of storage under the storage conditions specified by the Supplier, so that the whole stock, delivered once, stays usable over the entire issuance period of the contract.
SAM-CRD-069	The Supplier shall supply the whole blank card stock of the contract in a single delivery, before the operational acceptance of the card production chain, in the quantity stated in SAM-CRD-064 (in the order of 250,000 cards), including a justified wastage and reject allowance that covers calibration and test runs, acceptance testing, specimen cards, spoils and SBS staff training runs. The quantity of SAM-CRD-064 is the quantity delivered, and the Proposer shall state, within it, the allowance assumed for the non issued uses. The stock shall be delivered in sealed, batch numbered packaging suitable for long term storage, and the Supplier shall state the storage conditions required; the storage area is part of the Apia personalisation centre (site S3 of VII.2). Personalisation consumables are supplied as a first year lot and reordered per year at the unit rates of the Price Schedules.
SAM-CRD-070	The Supplier shall provide a consumables stock management system covering the main warehouse and the stock of the Apia production site (and of the Salelologa site where the production line option of SAM-CRD-076 is exercised), managing receipts and issues by box, inventories, a catalogue of consumable types and packagings, expiry dates with alerts, and configurable low stock alerts including predictive alerts.
SAM-CRD-071	The stock management system shall include anti theft and anti fraud functions, in particular the ability to track and revoke batches of consumables.
SAM-CRD-072	The Supplier shall supply the secondary consumables needed for card logistics: boxes holding up to 200 personalised cards for movements within the production centre and transport to delivery points, envelopes for the circulation of production listings and signed delivery lists, and A4 paper.
SAM-CRD-073	The Supplier shall prepare a consumables handling manual, with the control and handling procedures applicable in the production centres, to prevent rejects caused by poor handling.
SAM-CRD-092	Card bodies that are spoiled during personalisation, rejected at quality control under SAM-CRD-058, damaged in handling, or withdrawn from stock for any other reason, shall be physically destroyed so that no element of the card body, of its security features or of any data borne on it can be reused. Destruction shall follow a documented procedure executed by two authorised persons acting together, and shall be recorded against the serial number or the batch of each card body destroyed, with the date, the reason and the identity of both persons. The Supplier shall provide, within the stock management system of SAM-CRD-070, a destruction register and a periodic reconciliation between blank card bodies received, blank card bodies consumed, cards personalised, cards delivered and card bodies destroyed. Any unexplained difference shall raise an alert to SBS. The procedure and the register shall be covered by the consumables handling manual of SAM-

	CRD-073 and shall be transferred to SBS under the autonomy transition of SAM-CRD-080.

Local production sites and autonomy transition

Production runs in Samoa, and the capability transfers: these requirements organise the sites and the path to autonomous SBS operation.

ID	Requirement
SAM-CRD-076	Card production shall be installed at Apia (Upolu), the production site of the base scope. Salelologa (Savai'i) is a delivery and collection point in the base scope (see SAM-CRD-085 to 087). A second production line at Salelologa shall be priced as a separately exercisable option; under that option, the whole of this clause applies to both sites, and each site shall be able to operate autonomously. All equipment shall be delivered on site, installed, configured, tested and commissioned by the Supplier, with an inventory and acceptance at reception and an operational acceptance before go live, based on an acceptance workbook validated by SBS.
SAM-CRD-077	The Apia site shall be equipped with a pool of desktop laser engraving units (at least 150 cards per hour each), print stations, a quality control station and access to the signature HSM. The bidder shall size the engraver pool per site against the expected daily personalisation rates of the mass registration phase and of steady state operations, as stated in the schedule and volumes of VII.2. Under the Salelologa production line option (SAM-CRD-076), the second site shall be equipped in the same way, each site remaining able to produce autonomously, and the distribution of capacity between the two sites shall be proposed by the Supplier and validated by SBS.
SAM-CRD-078	Production shall start with a proof of concept and pilot phase allowing hypotheses to be tested and approaches corrected in real conditions, followed by a gradual ramp up to full scale, with the Supplier responsible for reconfiguring the systems and deploying the full equipment for the scale up. The start of the pilot phase shall be anchored to the Implementation Schedule milestones (a stated number of weeks after the platform operational acceptance of M4, feeding the card milestones M6b and M6c), not to a calendar date.
SAM-CRD-079	During the initial operating period, the Supplier shall provide the production site supervisors and shall supervise operations; SBS shall provide the operators. The Supplier shall operate, support and maintain the delivered systems in line with the service levels defined elsewhere in this Section.
SAM-CRD-080	Before the end of the contract, the Supplier shall execute an exit transition so that SBS produces, supervises and maintains the cards in full autonomy: delivery of updated documentation, training and practical skills transfer sessions on all delivered elements, transfer of supervision to SBS supervisors, and transfers of ownership. The detailed programme is defined in the capacity building annex of this Section.
SAM-CRD-081	The Supplier shall train SBS technical teams on all delivered systems and equipment, and shall train the card production operators, before the start of pilot production.
SAM-CRD-082	For all customised modules of the system, in particular the data exchanges with the IDMS, the preparation of the card data, the QR code generation and the print station files, the Supplier shall deliver the source code with training to compile, test and deploy it, and shall organise source code walkthroughs with SBS technical teams.

Distribution and delivery tracking

Getting cards to people across the islands: distribution logistics and end to end tracking from production to the person's hands.

ID	Requirement
SAM-CRD-085	The Supplier shall provide a distribution and delivery tracking application running on Android tablets or smartphones, or on an equivalent mobile operating system, with its back end, free of licence and with source code delivered to SBS. Personalised cards shall be packed in boxes at the production site, and the boxes scanned at packing, at pick up by the transporter, and at arrival at the delivery point, so that each movement updates the card management system and the IDMS.
SAM-CRD-086	At the delivery point, the application shall retrieve the card of a person from their reference number, and delivery shall require authentication of the person: biometric authentication online, or offline face verification using the portrait contained in the signed QR code content of the card.

SAM-CRD-087	Delivery shall also be possible in disconnected mode: printed A4 sign off lists shall accompany the boxes, delivered cards shall be recorded on paper when the application is temporarily unavailable, and the application shall allow the deferred recording of these deliveries so that the information reaches the central level.
SAM-CRD-088	The card management system shall expose a status enquiry service usable by authorised back end applications and citizen facing channels (IDMS, online portal, USSD or messaging gateway), and a protected web application allowing authorised SBS agents to search cards and their status.
SAM-CRD-089	The System shall make it possible to know at any time the location and status of any card or batch of cards, from production to delivery, and shall record loss or theft at any point of the chain.
SAM-CRD-090	The Supplier shall report weekly and monthly on production and delivery: number of cards printed and delivered, average personalisation time, average time from request to delivery, incidents and their treatment, through the operational reporting defined elsewhere in this Section, served by the single BI and reporting layer shared across the NDIDS.

1.2.5 Portals and Citizen Channels

The public information portal, the citizen portal and the citizen facing channels are specified in 1.2.3, section 7, Citizen portal and channels, together with the relying party services they depend on. This heading is kept so that the numbering of 1.2 runs without a gap and so that earlier cross references to 1.2.5 resolve.

1.2.6 CRVS: civil registration database and services (SAM-CRV-001 to 087)

Framing note (context, no requirements): the existing digital CRVS system has been in service since 2003 and remains the system of record for the flow during V1. Offices: Apia (13 approved posts) and Salelologa (5). About 80% of births occur in hospital. Paper archives since about 1961; reference volume of about 570,000 records.

1. Scope and phasing

Scope note (arbitration of 28 Jul 2026, file 37, V1/D8). The V1 stock scope (sections 2, 3 and 4, and the paper digitisation sequencing) is part of the base scope. The V2 flow management (section 5), the usage layer services (section 6, with the exceptions stated in SAM-CRV-062) and the migration and decommissioning (section 7) constitute the **CRVS flow option**: their design is included in the base scope, and their delivery is priced as a separate option exercisable by the Purchaser at V1 acceptance. Requirements belonging to the option are marked "OPTION" at section level below; V1 stock requirements stay base scope.

ID	Requirement
SAM-CRV-001	The Supplier shall deliver a civil registration component (CRVS) in two releases. Release V1, in the base scope, delivers the civil registry database and the management of the existing stock of civil status records. Release V2, the CRVS flow option (design in base scope, delivery as a separately priced option exercisable at V1 acceptance), delivers the management of the flow of new vital events and the migration of data from the legacy CRVS system. The detailed functionalities and flows of the civil registration processes will be reviewed in detail and settled at the project inception workshops. The use cases and the data model published in this Section for civil registration are indicative: they state the intent and bound the effort, and will be confirmed and finalised with the selected Supplier during the implementation design workshops.
SAM-CRV-002	During V1 the legacy CRVS system remains the system of record for the registration of new vital events. The V1 database is the authoritative repository of the consolidated stock. The transition of the system of record to the new CRVS shall occur at the V2 cutover, under a documented and reversible plan. Definitions applicable throughout this Section: the consolidated stock database is the bulk loaded working copy of the existing records, and its records are not certified by their loading alone; the certified records of the new base enter only through the certification queue, fed primarily by the enrolment filter (search, select and bind at the kit). No bulk migration of the stock into the certified base is performed under this contract; the treatment of the residual stock is decided by the Purchaser on the basis of the stock analysis.
SAM-CRV-003	The CRVS component shall be functionally separable from the identity components (IDMS, IDVS) with interfaces over documented APIs, so that governance, access rights and legal regimes of civil registration and identity remain distinct.
SAM-CRV-004	The data model shall support at least the following vital events, configurable to the laws of Samoa: live birth, death, fetal death, marriage, divorce, annulment, judicial separation, adoption, legitimation, recognition, change of name. The exact list and attributes shall be confirmed at design stage against the applicable legislation. Fetal death or stillbirth, legitimation, recognition and judicial separation shall be supported as distinct registrable event types, each with its own

	evidence requirement and decision authority, and never as a generic other event category.
SAM-CRV-088	The System shall record a birth notification, whether received through a health facility or a community notification channel, as a distinct notification record, linked to the resulting registration record once it occurs. Notification and registration are two distinct legal acts.
SAM-CRV-005	Each civil status record shall carry a unique, permanent record identifier, the link to the person's SDIN where established, the source of the record (legacy system, enrolment capture, V2 registration), and its certification status. In accordance with section 60(1)(c) of the NDID Act 2024, the System shall record the SDIN or associated token against every birth, death, marriage and change of name record concerning a registered person.
SAM-CRV-006	The CRVS database is the **national reference registry of civil status facts**. Government and authorised third party systems shall be able to consume certified civil status information from it through documented services, in place of paper based exchanges, under the access regime defined by law.
SAM-CRV-007	All CRVS services and interfaces shall follow open standards: REST/JSON with OpenAPI descriptions, OIDC and OAuth 2.0 for access control of online services, verifiable credentials in the families of SAM-CRD-002 (IETF SD-JWT VC and ISO/IEC 18013-5 mdoc) for attestations, and open signature and seal formats for documents.

1b. CRVS DPI architecture: separation of collection and storage

Source: principles of separation of collection and storage for the digitalisation of legal identity, applied to Samoa.

ID	Requirement
SAM-CRV-070	The CRVS shall be delivered as a digital public infrastructure made of **three separable components**: (1) the **central civil registry database**, the national single source of truth for civil status facts; (2) the **interoperable back end** and its submodules (interoperability gateway, APIs, notification and attestation services); (3) the **business workflow engine** (BPMN 2.0 / DMN) driving registration and correction processes. Each component shall expose documented APIs and be replaceable without redesign of the others. Each of the three components shall be either open source, or developed for the Purchaser and delivered with its full source code under the conditions of SAM-IDM-138. The escrow route of SAM-IDM-137 is not available for the CRVS, because SBS is to own the civil registration system and evolve it after handover (SAM-TRF-030 and the capacity building module table).
SAM-CRV-071	The System shall enforce a **strict separation between collection and storage**. No collection channel shall write directly to the registry database: every inbound civil status fact passes through the interoperability gateway of the back end, which authenticates the source, validates and transforms the data to the standard format, records provenance, and hands over to the workflow engine for processing.
SAM-CRV-072	Collection shall support multiple channel types, at minimum: registration of the flow at civil registry offices (V2); health sector notifications of births and deaths (V2); justice decisions affecting civil status such as name changes or adoptions (V2); digitisation of paper registers; migration from the legacy system (V2); and captures from the enrolment operation (V1). New collection channels and third party collection solutions shall be onboardable through the gateway without modification of the central components. Among these channels, the enrolment capture channel is the primary channel that populates the stock of the new base during V1; the other channels complement it.
SAM-CRV-073	The gateway shall define a **standardised, versioned, openly documented data format** for civil status facts, so that collection solutions from different vendors, funded and deployed at different times, can converge into the single national registry.
SAM-CRV-074	The registry shall follow a **digital only approach**: civil status records are held as certified structured digital data, digitally sealed and individually verifiable, not as scanned images. Document scans are archived as supporting evidence linked to records but kept out of the lightweight registry, so that services remain fast and usable over limited network conditions.
SAM-CRV-075	The back end shall implement the standard flow map of the civil registry: inbound declarations, notifications and decisions; outbound attestations and certificates,

	notifications (IDMS and authorised systems), and statistics (national statistics function). All flows run through the gateway APIs under the applicable access regime.
SAM-CRV-076	Interoperability with the identity ecosystem and sectoral systems shall rely on open, published interoperability and data exchange standards for identity and civil registration, adhering to the applicable ISO standards where they exist, consistent with the architecture requirements of VII.1.3 (SAM-ARC-032).

2. V1: Civil registry database and stock management

The V1 core: the civil registry database and the management of the existing stock of records, with certification by authorised registrars as the quality gate.

ID	Requirement
SAM-CRV-010	The System shall provide a central civil registry database holding the consolidated stock of civil status records, dimensioned for at least 600,000 records and their document images, with capacity headroom defined in the sizing requirements.
SAM-CRV-011	The System shall ingest the initial stock by extraction from the existing digital CRVS system, through file based (CSV) batch mechanisms agreed with the Purchaser (the legacy system is unmaintained and offers no API; CSV extraction by BDM staff is the confirmed interface), preserving source identifiers for traceability.
SAM-CRV-012	Each ingestion run shall produce a data quality report: records loaded, records rejected with reasons, duplicate candidates, incomplete records, and referential inconsistencies (for example a death recorded for a person with no birth record).
SAM-CRV-013	The System shall detect duplicate candidate records within the stock using configurable matching rules on biographic attributes, and shall queue them for review and merge by authorised registrars, with full audit of merge and unmerge operations.
SAM-CRV-014	The System shall support linking civil status records to the person's SDIN, in coordination with the IDMS. A person's birth record, once certified, shall be linkable to exactly one SDIN.
SAM-CRV-015	The System shall provide search and retrieval over the stock by name (including customary and matai titles), date and place of event, record identifier, SDIN, and source identifier, with phonetic and approximate matching suitable for Samoan names.
SAM-CRV-016	Corrections to stock records shall follow a controlled workflow: request, supporting evidence, decision by an authorised registrar, and full audit trail retaining prior values. Legal rectifications and administrative corrections shall be distinguished.
SAM-CRV-017	The System shall manage record states, at minimum: draft, provisional (pending certification), certified, corrected, sealed or restricted (as provided by law, for example adoptions), and cancelled, with state transition rules configurable by the Purchaser.
SAM-CRV-018	The System shall provide dashboards on stock coverage and quality: records by event type, year and district, certification status, duplicate queue, correction queue, and progress of stock consolidation over time, served as views of the single BI and reporting layer shared across the NDIDS.
SAM-CRV-019	The System shall store and serve scanned images of source documents attached to records, with integrity protection (hash), and shall support later ingestion of digitised paper archives (from about 1961) without redesign.

Paper register digitisation (sequencing principles)

Scope note: the digitisation operation itself (scanning, typing and verification of the legacy paper registers) is not part of the scope procured under this Contract. The System shall provide the enabling capability (the digitisation workflow and the ability to ingest digitised records later without redesign), and the principles below frame how any future digitisation undertaking would be sequenced. Bidders shall not price a digitisation operation.

ID	Requirement
SAM-CRV-085	Digitisation of paper registers shall not start for an office or register series while that register is still in live use (subject to marginal annotations) or before digital registration is effective for that office. Digitisation proceeds in waves, office by office.
SAM-CRV-086	Digitising a register means **entering its content into the System as certified structured digital records** through a typing and verification workflow (OCR may assist but never replaces human verification), with the page scan attached as archival evidence. The scan alone does not constitute a digital record.
SAM-CRV-087	The Supplier shall provide the tooling and the transition methodology per office: (1) events sent digitally to the central system while paper registration continues; (2) digital

	only registration, with backlog typing of past registers; (3) relocation of closed paper registers for scanning and physical archiving.

3. V1: Feeding the stock from enrolment capture

The primary channel populating the new base: civil status documents captured at enrolment become certified records through the registrar workflow.

ID	Requirement
SAM-CRV-025	The enrolment application captures the birth certificate (and other civil status documents where applicable) presented by the applicant: document image and indexed data. The CRVS component shall receive these captures from the enrolment platform through the standard packet interface.
SAM-CRV-026	For each capture received, the System shall attempt to match it against the stock. On a confirmed match, the capture shall be attached to the existing record. On no match, the System shall create a provisional record flagged for registrar review.
SAM-CRV-027	Provisional records created from enrolment captures shall enter a certification queue where authorised registrars verify them against source archives and either certify, correct or reject them, with reasons recorded.
SAM-CRV-028	The matching, attachment and certification activity shall be traceable end to end: which enrolment transaction produced which capture, which registrar took which decision, and which record version resulted.
SAM-CRV-029	The certification decision shall be notified to the IDMS so that the identity record and the SDIN linkage reflect the certified civil status data.
SAM-CRV-030	The legal status clarification and late civil registration process shall consume the pending enrolment dossiers of persons enrolled without a documentary or CRVS basis (SAM-ENR-011): the captured elements, including any community based attestation (SAM-ENR-013), shall enter the certification queue of SAM-CRV-027 as the clarification file of the person, biometrically anchored through the reserved SDIN bound to the application. On successful late registration, or on acceptance by the Registrar General of an official document, the System shall notify the IDMS so that the status "active, legal status clarification pending" of the SDIN is lifted to full active status (SAM-IDM-028); on definitive failure, the notification shall trigger the deactivation of the SDIN, the number being never reassigned.

4. V1: Interfaces

The exchanges between the CRVS component and the identity system, in both directions: preload out, SDIN write back in, and the event notifications.

ID	Requirement
SAM-CRV-033	Interface with the existing CRVS system: scheduled file based (CSV) extraction for initial and incremental stock synchronisation (the legacy system keeps registering the flow during V1 but is unmaintained: no API, no vendor support; BDM staff produce the extracts). The extraction schedule shall be frequent enough to keep the stock database current until the V2 cutover and to satisfy the statutory death deactivation deadline chain (SAM-IDM-033).
SAM-CRV-034	Interface with the enrolment preload chain: the biographic extracts preloaded into enrolment kits are produced from the stock database once it is commissioned, replacing direct extraction from the legacy system, without change to the kit side interface. The interface also carries the return leg: the SDIN write back from the identity system against the bound record (SAM-ENR-149), with the same retry, reconciliation and audit obligations in both directions.
SAM-CRV-035	Interface with the IDMS: event based notifications in both directions over documented APIs (certified records and corrections towards IDMS; SDIN linkage and death or status information towards CRVS), with delivery guarantees and replay.
SAM-CRV-036	All interfaces shall be exposed as documented, versioned, testable APIs (REST/JSON, OpenAPI descriptions), consistent with the architecture requirements of section VII.1.3.

5. V2: Flow management (future vital events) — OPTION: exercisable at V1 acceptance; design included in base scope

The separately priced option for registering new vital events: designed in the base scope so V1 choices never foreclose it, delivered when Samoa exercises the option.

ID	Requirement
SAM-CRV-040	From the V2 cutover, the System shall support the registration of new vital events at registration offices (Apia and Salelologa at minimum) and through notification channels, becoming the system of record for civil registration.
SAM-CRV-041	The System shall support notification of births and deaths by health facilities (about 80 percent of births occur in hospital) through a secure channel (web application or API), and recording of community notifications for events occurring outside facilities, in line with the procedures defined by the Purchaser. The community notification channel shall support the statutory notifiers of section 21(3) of the NDID Act 2024 (a Sui Tamaitai o le Nuu, a Sui o le Nuu or a Minister of religion) through a simple, mobile friendly channel, and the health facility channel shall meet the notification obligation of the Director General of Health under section 21(2), both channels forming the NDIDS notification system required by the Act.
SAM-CRV-042	Registration workflows (declaration, verification, registration, certificate issuance, late registration with its specific evidence requirements) shall be implemented on the configurable workflow engine (BPMN 2.0 / DMN), delivered as executable, versioned configurations with their source. The Purchaser shall be able to adjust decision rules, statuses, thresholds and notification triggers through DMN configuration without redevelopment; modification of the process models themselves is performed by trained Purchaser staff with the assisted workflow update service of SAM-IDM-127, applied to the CRVS workflows. The Supplier may deliver a simpler configurable implementation at go live, provided the registration workflows are re implemented as executable BPMN 2.0 / DMN models (or an equivalent open modelling standard) before the end of the contract; the DMN configuration autonomy is required from go live.
SAM-CRV-043	At birth registration the System shall call the IDMS identity creation service (SAM-IDM-025), which allocates the SDIN through the **unique number generator** (a standalone component developed by the Supplier, delivered with its full source code, build and deployment documentation to the Purchaser, and operable by the Purchaser independently of any other component) and returns the SDIN and its statutory token together in the same transaction. Every newly registered child receives an SDIN at birth, recorded with its token on the birth record.
SAM-CRV-044	The System shall issue certificates, copies and attestations (birth, death, marriage and other events as provided by law) as controlled documents: numbered, sealed, verifiable, with issuance history per record. Printed documents and PDF documents shall embed the certified information as a signed credential encoded in a QR code, in the profile selected under SAM-CRD-046, signed within the national trust chain and verifiable offline against the national trust anchor, with no proprietary encoding and no URL. From the dates notified in the Savali, every certificate issued shall display the SDIN or the associated token of the person or persons concerned, as required by section 60(1)(d) of the NDID Act 2024. The choice between displaying the SDIN or the token, and the activation date, shall be configurable by the Purchaser.
SAM-CRV-045	OPTION, exercisable when the fee policy is adopted (same treatment as SAM-IDV-074): the System shall support fees management for certificate issuance and other chargeable acts where provided by regulation: configurable fee schedule, receipts, and reconciliation reporting.
SAM-CRV-046	The System shall produce vital statistics consistent with international recommendations (United Nations Principles and Recommendations for a Vital Statistics System), with standard and configurable reports by period, event type, sex, age and geography, and export to the national statistics function of SBS.
SAM-CRV-047	Amendments driven by court decisions (adoption, legitimation, name change, annulment) shall be supported with the sealing and access restriction rules provided by law.

6. Usage layer: online services, verifiable credentials and third party integrations — OPTION: exercisable at V1 acceptance; design included in base scope (exceptions in SAM-CRV-062)

What the civil registry serves outward: certificate credentials with signed QR verification and online status query, and the integration surface for authorised third parties.

ID	Requirement

SAM-CRV-055	The System shall provide online services allowing individuals to request and receive certificates, certified copies and attestations **without physical attendance**: request submission, identity verification through the national identity services (authentication via the IDVS using the SDIN or the statutory token), payment of applicable fees where required, and delivery as sealed PDF documents or verifiable credentials. For minors and for persons registered through assisted registration, online requests may be made by a parent, legal guardian or authorised representative, authenticated through their own SDIN, with the relationship recorded and every such access logged and visible in the citizen facing activity history.
SAM-CRV-056	The delivery channel shall support both self service download and issuance into the citizen's wallet (mobile companion application or cloud wallet), consistent with the credential architecture of the identity components.
SAM-CRV-057	The System shall be able to **issue verifiable credentials directly** from certified civil status records (starting with the birth certificate credential of SAM-CRD-005), in one of the families of SAM-CRD-002 (IETF SD-JWT VC or ISO/IEC 18013-5 mdoc) and issued through OpenID4VCI, within the shared trust infrastructure of VII.1.2.4. The catalogue is limited to the two credential types of SAM-CRD-005; new credential types shall be addable by trained Purchaser staff through a documented, transferred procedure (per the capacity building annex), a no code credential designer not being required.
SAM-CRV-058	Any party receiving a CRVS document or credential shall be able to verify it: offline verification of the signed QR code content, and an online status verification service (validity, revocation) exposed through the IDVS under the relying party regime.
SAM-CRV-059	The System shall support digital integrations with authorised third party systems, starting with **health and justice**, so that civil status interactions happen without physical displacement of individuals: inbound channels (health facility notifications of births and deaths; court decisions affecting civil status) and outbound services (verification and retrieval of certified civil status information under the applicable access regime).
SAM-CRV-060	Third party access to CRVS services shall reuse the relying party onboarding, authorisation, monitoring and audit framework of the IDVS block (registration, service plans, logging visible to the citizen), with CRVS specific data scopes. No third party shall access the CRVS database directly.
SAM-CRV-061	Every online issuance, verification and third party retrieval shall be logged and auditable, and reflected in the citizen facing activity history where the person is identified.
SAM-CRV-062	Phasing: the usage layer services of this section follow the CRVS flow option, with two exceptions delivered in the V1 base scope: (a) the verification of sealed documents issued in V1 where such documents exist; and (b) the issuance of the birth certificate credential from certified stock records (SAM-CRV-057, SAM-CRD-005/008), available from the release of the certified CRVS stock. Certificate verification shall combine two levels: offline verification of the signed QR credential of the document, and an online status query confirming the current validity of the record. Which use case requires which level is configured per relying party policy, confirmed at the design stage.

7. V2: Migration from the legacy system and decommissioning — OPTION: exercisable at V1 acceptance; design included in base scope

Under the option, the treatment of the legacy system: record level tooling rather than bulk migration, and an orderly decommissioning.

ID	Requirement
SAM-CRV-050	There is no bulk migration of the legacy CRVS data. The new CRVS base is constituted through the enrolment filter: records enter it as persons enrol and their records are certified (SAM-CRV-027). The residual legacy stock stays outside the new base pending the analysis of its treatment; rolling migration on demand (record by record, upon a service request touching a legacy record) is the candidate treatment, to be decided after that analysis. The Supplier shall provide the record level migration tooling this requires: mapping, cleansing rules agreed with the Purchaser, per record reconciliation and audit.
SAM-CRV-051	The cutover plan shall include acceptance criteria, a rollback procedure, a freeze window agreed with the Purchaser, and shall guarantee that no registration is lost or duplicated across the transition.
SAM-CRV-052	After cutover the legacy system shall be preserved as a read only archive for an agreed period, and its decommissioning shall be documented. The Supplier shall provide the Purchaser with a complete export of migrated and residual data in open formats.

1.3 Architectural Requirements to be met by the Information System (Architecture and Standards, SAM-ARC-001 to 040)

This chapter fixes the architectural rules that keep the platform sovereign, evolvable and interoperable: modular components with open interfaces, business processes driven by configuration, a single national trust chain, hosting and data sovereignty bounds, mandatory open standards and API management. The intent is a future proof and agile system: bidders should demonstrate how their architecture lets Samoa evolve flows, data and components over time, and replace any part, without redesign and without dependency on one vendor.

1. Architecture principles (SAM-ARC-001 to 008)

The structural rules of the platform: modular components, open interfaces, replaceability and the data separations the law imposes.

ID	Requirement
SAM-ARC-001	The System shall follow a modular architecture in which each major subsystem (enrolment platform, IDMS, ABIS, IDVS, credential and card management, CRVS, portals, relying party management) is a separable component with documented boundaries and interfaces based on open standards. The architecture shall be future proof and agile: able to serve multiple usage scenarios and to evolve business flows and data structures over time, through the component replaceability of SAM-ARC-002 and the configurability of SAM-ARC-009 to SAM-ARC-011. These specifications state capabilities and behaviours; fine grained configuration is settled at the project inception and concertation workshops.
SAM-ARC-002	It shall be possible to replace any individual component (including the biometric matching engine, the card personalisation chain and the workflow engine) by another product meeting the same interfaces, without redesign of the overall System and without impact on the data held in the reference registries. The Supplier shall describe, for each component, the replacement procedure and the interfaces that make it possible.
SAM-ARC-003	The registration and identity core (IDMS, ABIS) shall be architecturally separated from the services layer consumed by relying parties (IDVS). The two shall not share the same runtime data store, shall be deployable and upgradable independently, and shall have distinct availability targets: the IDVS shall be highly available while the IDMS does not require continuous availability.
SAM-ARC-004	The System shall implement the statutory separation of the three data stores (Identity Database, Biometric Database, authentication and transaction log store) as specified in SAM-IDM-066. The architecture documentation shall show this separation explicitly.
SAM-ARC-044	External organisations shall consume identity services only through the IDVS. No direct access to the IDMS shall be exposed outside the platform. No service of the System shall allow population browsing, bulk download of identity data, or the return of raw biometric data to any relying party.
SAM-ARC-005	The reference registries (population register and CRVS registry) shall be the single sources of truth of the System, owned entirely by the Purchaser, exposing application interfaces that the business processes and services consume. No component shall hold an alternative master copy of registry data.
SAM-ARC-006	The architecture shall avoid any single point where all identity data could be exposed: no component shall concentrate biographic data, biometric data and transaction logs in a single accessible store, and network segmentation shall isolate the zones as specified in SAM-CYB-030.
SAM-ARC-007	The Supplier shall deliver and maintain a complete architecture description (logical, application, data, infrastructure and security views), kept current throughout the Contract and handed over as part of skills transfer.
SAM-ARC-008	The architecture and the numbering of subsystems shall allow a later separation of the scope into lots (for example identity and civil registration) without redesign and without renumbering of interfaces.

2. Business process orchestration (SAM-ARC-009 to 011)

Business behaviour lives in configuration, not code: processes and decisions are modelled and modifiable by SBS after training.

ID	Requirement
SAM-ARC-009	A configurable workflow orchestration capability shall span the whole System (enrolment, IDMS, IDVS, credential issuance, CRVS), so that business processes such as updates, corrections and name changes are configured rather than redeveloped.
SAM-ARC-010	All business processes shall be modelled in BPMN 2.0 and business decisions in DMN, or an equivalent open modelling standard. No business step shall be hard coded in application software. The execution of the models may be phased as set out in SAM-IDM-006 and SAM-IDM-078: a simpler configurable implementation is acceptable at go live, provided the processes are re implemented as executable models before the end of the contract.
SAM-ARC-011	The Purchaser shall be able to modify process flows, decision rules, statuses and notifications through configuration, after training, without Supplier intervention and without software redevelopment.

3. Public key infrastructure and trust anchor (SAM-ARC-012 to 019)

One national trust chain signs everything verifiable: these requirements fix the PKI, its custody and its phase one scope serving NDIDS and CRVS.

ID	Requirement
SAM-ARC-012	The Supplier shall deliver and commission a national public key infrastructure serving as the trust anchor of the NDIDS, comprising at least a root certificate authority and an issuing certificate authority, both anchored in hardware security modules.
SAM-ARC-013	The hardware security modules and the cryptographic keys shall be owned by the Purchaser, hosted in Samoa and operated by SBS staff with Supplier support during the transfer period. The signing authority shall not be rented from, or operable only by, the Supplier or any third party. HSM certification requirements are specified in SAM-CYB-031.
SAM-ARC-014	Key generation shall take place in witnessed and recorded key ceremonies under dual control, with the master key material split across at least two authorised holders so that no single person can use or reconstruct it. Ceremony scripts and records shall be delivered to the Purchaser.
SAM-ARC-015	The Supplier shall deliver a Certificate Policy and a Certification Practice Statement (CP/CPS) aligned with international practice, together with the operating procedures, renewal cycles and revocation procedures that allow relying parties in Samoa and abroad to assess the trust chain.
SAM-ARC-016	A single chain of trust anchored in the national PKI shall sign all verifiable artefacts of the System: the verifiable credentials issued to holders, the signed QR code content on the physical card, and the digital seals on CRVS certificates and attestations. No parallel or product specific trust chain shall be introduced. The PKI serves NDIDS and CRVS in phase one. Its design shall not preclude a later whole of government extension; the choices with cross government impact will be reviewed at a PKI workshop with MCIT, the transport authority and the Passport Office, in the concertation workshops of part D.
SAM-ARC-043	SBS is the authoritative source of verified identity. Authentication and verification services are exposed to consumers through the platform service layer, never by direct access to the reference registries. The architecture shall allow a later transfer of the authoritative source role to another designated national authority without re architecture of the System.
SAM-ARC-017	The PKI shall have an availability target at least equal to that of the IDVS and higher than that of the IDMS, since it signs credentials and underwrites every verification, including offline verification.

SAM-ARC-018	The Supplier shall train named SBS staff to operate the PKI (ceremonies, issuance, renewal, revocation, audit) in accordance with the capacity building annex, with operation by SBS demonstrated as an acceptance criterion.
SAM-ARC-019	The enterprise PKI shall be designed as a three tier hierarchy (root certification authority, intermediate or issuing certification authorities, and leaf certificates) dedicated to the internal systems, TLS endpoint security, relying party authentication and digital signatures. Where the solution includes mobile documents, the two tier model those standards require shall be supported alongside it: a certification authority and its document signers, with no intermediate certificate. Both models shall be available from the outset, so that the choice of credential family requires neither a redesign of the trust chain nor a contract variation. The signing of the card QR code content is covered by SAM-ARC-016. Other government credential programmes may later inherit it as a shared national capability, as additional issuing authorities under the NDIDS root, where their trust model allows it. Programmes whose international trust framework requires a self signed national root of its own, for example an ICAO country signing certification authority (CSCA) for travel documents or an issuing authority certification authority (IACA) for mobile driving licences, shall be accommodated as separate root authorities alongside the NDIDS root, with their document signers, revocation lists and link certificates, without redesign of the NDIDS trust chain.

4. Hosting and data sovereignty (SAM-ARC-020 to 026)

Where the system runs and under whose control: reference data, biometrics and keys stay in Samoa, with any cloud use bounded and decided at Cabinet level.

ID	Requirement
SAM-ARC-020	The System shall be hosted on the two existing sites described in VII.4 Background: the SBS server room as primary site and the Vodafone data centre as secondary site, both operated under SBS control. Proposers shall reuse the existing environment and shall not price a greenfield build; the required reinforcement of the primary site is described in the inventories.
SAM-ARC-021	The deployment architecture shall allow the primary and secondary roles of the two sites to be swapped without redesign for the IDVS layer, meaning the promotion of the secondary site to the primary role and not a simultaneous service from both sites, consistent with SAM-CYB-020. For the IDMS, the ABIS, the CRVS and the supporting tooling, the secondary site shall provide an active/passive disaster recovery capability sized to the recovery objectives of SAM-CYB-021, with a documented restore path; full symmetric deployment of these components is not required. The Supplier shall document the swap and restore procedures and demonstrate them during acceptance.
SAM-ARC-022	The reference registries, the biometric data and the cryptographic keys shall remain hosted in Samoa, on infrastructure owned and controlled by the Purchaser, for the duration of the Contract. This implements the hybrid infrastructure orientation of the National Digital Identification Policy (registry on national servers, cloud leveraged for accessibility, resilience and scalability).
SAM-ARC-023	The IDVS may optionally be deployed on cloud infrastructure, only if the Government of Samoa so decides at Cabinet level, and only within these bounds: the cloud instance holds nothing beyond the minimised, tokenised verification dataset of SAM-IDV-002, **excluding biometric verification templates and excluding the storage of authentication records (s.37(3))**: biometric 1:1 verification and the authentication record store remain on the national sites in Samoa; master identity data, the Biometric Database and the signing keys never leave Samoa; and the IDVS remains redeployable on the national sites without redesign. The proposed architecture shall support both deployment options at no additional licence cost.

SAM-ARC-024	The identity platform shall remain logically isolated from the existing SBS systems hosted in the same rooms, with its own network zones and security controls.
SAM-ARC-025	The System shall be deployable on virtualised infrastructure, with replication between the two sites and disaster recovery as specified in VII.1.4 and VII.1.6.
SAM-ARC-026	The Supplier shall conduct a site survey of both sites at project start and shall identify the adequacy works required at the primary site (power continuity, supervision, firewall and storage capacity), consistent with SAM-CYB-023 and the inventories.

5. Mandatory open standards (SAM-ARC-027 to 033)

The standards that make the platform interoperable and exit friendly: identity federation, credentials, biometrics and data exchange.

ID	Requirement
SAM-ARC-027	Federation, authentication and consented data sharing shall implement OpenID Connect (OIDC) and OAuth 2.0. Digital credentials shall be issued through OpenID4VCI and presented through OpenID4VP, both protocols being independent of the credential format. The credential formats of the credentials held on the phone and presented online are limited to the two families of SAM-CRD-002, the IETF SD-JWT VC and the ISO/IEC 18013-5 mobile document (mdoc). The profile of the signed QR code printed on the card and on documents is selected under SAM-CRD-046 and is not restricted to those two families. The System shall provide a credential issuance and signing module whose data model is configurable within those families, so that the credential types selected by the Purchaser can be issued and signed without redevelopment. The Proposer shall state which family it recommends for each channel (credential on the phone, QR printed on the card or on a document, online presentation), the card QR profile being selected under SAM-CRD-046, and shall justify that recommendation for the Samoan context, in particular the acceptance of the credential by relying parties abroad, a large majority of Samoans living overseas. The Purchaser confirms the selection at the technical inception workshops; the selection between the two families is made within the contract price, and no additional charge shall arise from that choice. The Proposer shall also state the technical impact of delivering the other family instead of the one it recommends.
SAM-ARC-042	The architecture shall include a notification hub or broker carrying the subscription based notification services of the functional blocks (SAM-IDM-141, SAM-IDV-107): subscriber registration, per use case authorisation, event delivery and event detail collection. The W3C WebSub pattern is recommended (intent verification, signed delivery, lease renewal, HTTPS callbacks), equivalent mechanisms being accepted. The hub shall keep operating when any single source system is unavailable, with retry, reconciliation and audit of deliveries.
SAM-ARC-041	Consent management is a capability of the IDVS, not an independent component. It protects the request for attributes: every component or service consuming identity attributes passes through the IDVS consent gate. The behaviour is specified in the IDVS block: explicit consent captured for eKYC (SAM-IDV-016), validity limited to a single transaction (SAM-IDV-017), consent assertion validated on every request with rejection when absent (SAM-IDV-024), consent evidence in the audit record (SAM-IDV-029) and consent management by the individual through the portal (SAM-IDV-095).
SAM-ARC-028	Biometric data shall be captured, stored and exchanged in the formats of ISO/IEC 19794 and ISO/IEC 39794. No proprietary biometric format shall be the only storage format of any biometric record.

SAM-ARC-029	The service interfaces exposed to the Purchaser, to relying parties and to other systems shall be RESTful APIs exchanging JSON, specified in OpenAPI, or an equivalent open, published standard. Interfaces internal to a component may use another style where justified, and shall then be documented and specified in an open, machine readable format. Other styles (for example asynchronous messaging) may likewise complement REST where justified, and shall then also be specified in an open, machine readable format. Data definitions and payload schemas, including the credential data models used for verifiable credential issuance, shall be published in an open, machine readable schema language (JSON Schema or equivalent) and kept current with the APIs.
SAM-ARC-030	Business processes and decision rules shall be expressed in BPMN 2.0 and DMN, or an equivalent open, published standard, as specified in SAM-ARC-010.
SAM-ARC-031	Withdrawn. The identifier is not reused.
SAM-ARC-032	Interoperability between identity system components (enrolment, population registry, ABIS, credential management, CRVS) shall rely on open, published interface and data exchange standards, adhering to the applicable ISO data format and exchange standards where they exist (for example ISO/IEC 19794 and ISO/IEC 39794 for biometric data). Other open standards are acceptable provided they are published, versioned and royalty free.
SAM-ARC-033	The Supplier shall keep the implemented standards at current, supported versions throughout the Contract and shall provide a standards roadmap identifying versions in use and planned upgrades.

6. API management (SAM-ARC-034 to 037)

Every service is consumed through managed APIs: gateway, versioning, quotas and security applied uniformly.

ID	Requirement
SAM-ARC-034	Every function of the System shall be exposed through fully documented APIs. Documentation shall include specifications in the OpenAPI format required by SAM-ARC-029, data dictionaries, error catalogues and worked examples, delivered in the Purchaser's repository and kept current.
SAM-ARC-035	APIs shall be versioned with a published deprecation and backward compatibility policy, so that relying parties and internal components are not broken by upgrades.
SAM-ARC-036	Every API shall be testable by the Purchaser and by authorised third parties in a sandbox or test environment that is functionally representative of production, without access to production data.
SAM-ARC-037	No licence fee, royalty or per transaction charge shall be payable to the Supplier or to any third party for the use of the System's APIs by the Purchaser or by relying parties authorised by the Purchaser.

7. Reversibility and exit (SAM-ARC-038 to 040)

The architecture must allow Samoa to leave: exportable data, documented interfaces and no capability that exists only inside a proprietary boundary.

ID	Requirement
SAM-ARC-038	The System shall provide complete data export functions, executable by the Purchaser, covering all registries, biometric data, documents, logs, configurations and workflow definitions, in open, documented, non proprietary formats, at no additional cost. Exports shall be tested during acceptance.
SAM-ARC-039	No core function of the System (registration, deduplication, SDIN generation, verification, credential issuance and signing, CRVS registration) shall depend on an

	external proprietary service, on connectivity outside Samoa, or on any subscription that the Purchaser cannot terminate without loss of the function.
SAM-ARC-040	The SDIN shall be produced by the unique number generator: a standalone, government controlled component developed by the Supplier and delivered with its full source code and documentation, serving both the IDMS (adult enrolment) and the CRVS (birth registration), as specified in SAM-IDM-022 and SAM-CRV-043.

1.4 Systems Administration and Management Functions Required to be met by the Information System (Administration, Backup and Disaster Recovery, SAM-ADM-001 to 040)

This chapter covers how the platform is operated day to day and how it survives incidents: centralised administration and access control, configuration and change management, monitoring, backup and restoration, disaster recovery across the two national sites, and the documentation and handover that let SBS operate autonomously. Bidders should treat operability by the Purchaser's teams as a design requirement, not an afterthought: the operating model is part of what is being procured.

1. Centralised administration and access control (SAM-ADM-001 to 006)

One administration plane governs the platform: centralised accounts, least privilege roles and controlled administrative access.

ID	Requirement
SAM-ADM-001	The System shall provide a centralised administration capability covering all subsystems (enrolment back end, IDMS, ABIS, IDVS, credential and card chain, CRVS, portals), from which authorised administrators manage users, roles, configurations and technical parameters.
SAM-ADM-002	Access control shall be role based (RBAC) and shall apply least privilege throughout: every account is individual, every permission derives from a role, and no shared or generic administrative account shall exist. Role definitions shall be configurable by the Purchaser.
SAM-ADM-003	Administrative access shall require multi factor authentication and shall be possible only from authorised administration zones, consistent with SAM-CYB-032.
SAM-ADM-004	The System shall provide a distinct statistical extraction role, separate from all operational and administrative roles, allowing the Government Statistician to access data in the Identity Database solely for the generation, collection, analysis, certification or publication of statistics under the Statistics Act 2015. This role shall permit extraction and aggregation only, with no write access and no access to biometric data, and every extraction shall be logged.
SAM-ADM-005	Segregation of duties shall be enforced between administration of the platform, administration of security (including key management), and business operations. No single role shall combine these functions.
SAM-ADM-006	User accounts and role assignments shall be reviewed periodically; the System shall produce access review reports listing accounts, roles, last activity and dormant accounts.

2. Configuration and change management (SAM-ADM-007 to 009)

Changes are managed, versioned and reversible, so the platform evolves without surprises.

ID	Requirement
SAM-ADM-007	All configurations (application parameters, workflow definitions, decision rules, infrastructure settings) shall be managed under version control, with the ability to compare versions and to roll back to a previous known good state.
SAM-ADM-008	Configuration changes in production shall follow a documented change procedure with approval, testing in a non production environment and traceability of who changed what and when.
SAM-ADM-009	The Supplier shall deliver and maintain a configuration reference document describing every configurable parameter, its function, its default and its authorised range.

3. Administration logging (SAM-ADM-010 to 011)

Administrative acts are logged and reviewable: who changed what, when, on which component.

ID	Requirement

SAM-ADM-010	Every administrative action (account management, role change, configuration change, deployment, manual data operation) shall be logged with the authenticated administrator, the action, the object affected, the date and time, and the origin. Administration logs shall be tamper evident and shall not be modifiable or erasable by administrators themselves.
SAM-ADM-011	Administration logs shall be retained according to a policy defined with the Purchaser, consistent with the statutory limits applicable to authentication logs (see SAM-CYB-033), and shall be available to the auditor role and to security monitoring.

4. Monitoring and supervision (SAM-ADM-012 to 016)

The operational eyes of the platform: technical and business supervision with alerting the operating teams can act on.

ID	Requirement
SAM-ADM-012	The System shall include a central technical supervision platform covering infrastructure health (servers, storage, network, virtualisation, HSMs), hosted in the supervision cell of the SBS ICT department. This capability is implemented by the central supervision and monitoring platform of the ICT Infrastructure component (SAM-INF-030 to 037).
SAM-ADM-013	Application supervision shall cover the business services themselves: service availability, transaction volumes and error rates, processing queues and backlogs (enrolment packets, deduplication, adjudication, card production), and interface health with external systems.
SAM-ADM-034	Transaction logs shall allow the reconstruction of every biometric decision, including the version stamping of the ABIS configuration in force at decision time (algorithm versions, thresholds, fusion policy). Log management shall meet the obligations of the draft NDID Regulations 2025 (pending commencement), including the two hour log backup and the two year archiving.
SAM-ADM-014	The supervision platform shall provide role appropriate dashboards, including at least: an infrastructure dashboard for the ICT team, an operations dashboard (registration progress, queues, incidents) for management, and service dashboards for the IDVS consistent with the relying party monitoring of the IDVS block.
SAM-ADM-015	The supervision platform shall raise alerts on configurable thresholds (availability, capacity, backlog, security events), delivered through at least two channels (for example console and email or SMS), with an escalation procedure documented in the operations manual.
SAM-ADM-016	Supervision data shall feed the centralised security logging and monitoring specified in SAM-CYB-010; the two capabilities may share a platform but security monitoring shall not be degradable by operations staff.

5. Backup and restoration (SAM-ADM-017 to 020)

Backups exist to be restored: policy, immutable copies and verified restorability, exercised regularly.

ID	Requirement
SAM-ADM-017	The Supplier shall implement a documented backup policy approved by the Purchaser, covering all databases, file stores, configurations, workflow definitions, logs and key material (under HSM backup procedures), with defined frequencies, retention periods and storage locations on both sites. The backup design shall follow the 3-2-1-1-0 pattern: three copies on two media types, one off site, one immutable or air gapped copy, and verified zero error restorability.

SAM-ADM-018	All backups shall be encrypted at rest and during transfer, with keys under Purchaser control. Backups of biometric data shall respect the statutory data separation of SAM-IDM-066.
SAM-ADM-019	Restoration shall be tested at regular intervals, at least quarterly on a sample and at least once a year as a full restoration rehearsal, with results reported to the Purchaser. An untested backup shall be treated as no backup.
SAM-ADM-020	Backup copies shall exist on both sites; at least one copy shall be offline or otherwise protected against a compromise that propagates through the network (ransomware resilient).

6. Disaster recovery on the two sites (SAM-ADM-021 to 024)

The two national sites protect each other: recovery objectives, switchover and the tested ability to run from either.

ID	Requirement
SAM-ADM-021	The System shall implement a disaster recovery capability across the two existing sites (SBS server room as primary, Vodafone data centre as secondary), with data replication between the sites and documented recovery procedures meeting the recovery objectives of SAM-CYB-021. The deployment mode is active and passive: the secondary site holds a synchronised standby of the production data and does not serve production traffic in normal operation, failover being a controlled and documented switch. Simultaneous service from both sites is not required and shall not be priced. Replication shall be configured so that the data lost on failover stays within the recovery point objective of each component stated in SAM-CYB-021.
SAM-ADM-022	Failover to the secondary site and failback shall be tested at the frequency set in SAM-CYB-020, under conditions representative of production. Each test shall produce a report with measured recovery times and corrective actions.
SAM-ADM-023	For the IDVS layer, the architecture shall support the swap of the primary and secondary roles of the two sites as a planned operation (not only as an emergency failover), executable by SBS staff following the documented procedure after transfer. For the IDMS, the ABIS, the CRVS and the supporting tooling, recovery at the secondary site follows the active/passive model of SAM-ARC-021, with a documented restore path meeting the recovery objectives of SAM-CYB-021.
SAM-ADM-024	The disaster recovery plan shall cover, beyond the central platforms, the dependent capabilities: PKI and signing services, card personalisation, enrolment synchronisation, and the offline verification path of SAM-CYB-022.

7. Capacity, patching and environments (SAM-ADM-025 to 030)

The disciplines that keep the platform current and sized: capacity management, patching, and the environment set from development to production.

ID	Requirement
SAM-ADM-025	The Supplier shall implement capacity management: monitoring of storage, compute and network consumption against the sizing baseline of VII.1.5, with quarterly capacity reports and forward projections so that expansion is planned before saturation.
SAM-ADM-026	Patch management shall cover all delivered components (operating systems, middleware, databases, applications, firmware including HSMs and kits), with patching SLAs by severity consistent with SAM-CYB-041 and with prior validation in a non production environment.
SAM-ADM-027	Release management shall be documented: versioned releases, release notes, tested rollback procedure for every deployment, and deployment automation such that a release can be deployed by SBS staff following the procedure.
SAM-ADM-028	The Supplier shall deliver and maintain four environments at least: development, test, pre production and production (the pre production environment serves as the Purchaser facing acceptance environment of part E). Pre production shall be functionally representative of production (same software versions, same configurations, representative data volumes); a permanently duplicated production scale stack is not required. Performance representative sizing for load test campaigns (SAM-PER-021) shall be achieved by temporary reallocation of production class resources, planned with the Purchaser. No development or test activity shall take place in production, except the

	pre commissioning and commissioning tests planned under part E, and production personal data shall not be used in lower environments unless anonymised.
SAM-ADM-029	Power continuity at the primary site shall protect the System against uncontrolled shutdown (UPS bridging, generator, controlled shutdown procedures protecting the HSMs), as specified in SAM-CYB-023. The administration procedures shall include the startup and shutdown sequences of the whole platform.
SAM-ADM-030	The administration and monitoring tooling shall be recoverable at the secondary site within the recovery objectives of SAM-CYB-021, following the active/passive model of SAM-ARC-021, so that administration capability survives the loss of one site; permanent symmetric deployment of the tooling is not required.

8. Documentation and transition to SBS operations (SAM-ADM-031 to 033)

Operating knowledge is a deliverable: documentation and the transition that puts SBS teams in command of daily operations.

ID	Requirement
SAM-ADM-031	The Supplier shall deliver a complete operations documentation set (operations manual, runbooks for routine and emergency procedures, monitoring handbook, backup and restoration procedures, DR plan), kept current in the Purchaser's repository throughout the Contract.
SAM-ADM-032	All administration, supervision, backup and disaster recovery operations shall be progressively transferred to SBS staff in accordance with the capacity building annex of this Section, using the pairing model and the competency depth scale defined there. The acceptance criterion is execution of each operation by SBS staff without Supplier assistance.
SAM-ADM-033	By the end of the transfer period, the Supplier's role shall be limited to the agreed support tier, with SBS operating the System day to day. The Supplier shall report on transfer progress against the plan at each project review.

1.5 Performance Requirements of the Information System (Performance and Sizing, SAM-PER-001 to 028)

Note to Proposers. The volumes below are the sizing baseline of the System. Values marked are working assumptions being confirmed with SBS and will be finalised before contract signature; Proposers shall size and price against the figures stated here.

1. Reference volumes (SAM-PER-001 to 008, 026 to 028)

The sizing baselines of the platform: population, enrolment intake and verification volumes as collected from Samoa's own institutions.

ID	Requirement
SAM-PER-001	The System shall be sized for a provisioned baseline capacity of 250,000 registered persons (phase 1 target confirmed by SBS), with a biometric gallery of 99,000 enrolled adults by the end of 2029 and an intermediate target of 60,000 by December 2027, and shall be extensible to 800,000 persons in total through the priced increment option of SAM-PER-030.
SAM-PER-002	The enrolment intake shall be sized for the full mass campaign fleet: 50 enrolment kits operating at a planning rate of 40 enrolments per kit per day, plus 10 enrolment tablets operating at a planning rate of 10 enrolments per tablet per day (outreach conditions), giving a peak daily intake envelope of approximately 2,100 enrolment packets per day, sustained over the campaign period.
SAM-PER-003	The adjudication capability shall be sized for approximately 10,000 manual adjudication cases over the mass enrolment wave, processed on 5 to 10 dedicated workstations, without the adjudication backlog blocking the enrolment pipeline.
SAM-PER-004	The IDVS shall be sized for a verification and eKYC volume of transactions per day, with an order of magnitude in the tens of thousands of transactions per day at maturity, and a peak hourly load to be confirmed at the project inception workshops.
SAM-PER-005	The CRVS component shall be sized for a record stock of approximately 600,000 civil registration records (births, deaths, marriages, including the migrated legacy stock), growing with annual vital events of approximately 8,000 per year.
SAM-PER-006	Storage shall be sized from a data volume per enrolled person of 15 MB (biographic data, biometric data, scanned documents), projected at 60,000, 99,000 and 250,000 persons, plus logs and backups over a growth horizon of ten (10) years.
SAM-PER-007	Sizing shall account for continuous registration after the mass wave: a steady state intake of 150 enrolments and identity updates per day through fixed and mobile capture points.
SAM-PER-008	The Supplier shall state in its proposal, for each subsystem, the sizing assumptions used, the resulting infrastructure dimensioning on the two sites, and the margin held against the baseline volumes above.
SAM-PER-026	The card personalisation chain and the card stock shall be sized for a total production volume of 250,000 National ID Cards over the contract, covering the Version 1 cohort, the continuous issuance and the replacements over the five years following the mass campaign, consistent with the daily production rate of SAM-PER-017; the whole blank card stock is delivered in a single delivery before the card chain operational acceptance (inventory Table 5.4,250,000 cards).
SAM-PER-027	The reference site set for card production and delivery is: one card personalisation centre in Apia (a second production line in Salelologa as a priced option, per SAM-PER-017), and card delivery points across the two islands where cards are handed over to holders with the distribution and delivery tracking application of SAM-CRD-085 and 086. The production equipment, the logistics services and the consumables shall be sized for this site set.
SAM-PER-028	The CRVS component shall be sized for two civil registration offices (Apia, approximately 13 approved posts; Salelologa, approximately 5), plus the health facility and community notification channels of SAM-CRV-041, and shall be extensible by configuration to additional registration points without redevelopment.

2. Response times (SAM-PER-009 to 014)

What fast means, service by service, measured at the platform boundary under stated load.

ID	Requirement

SAM-PER-009	The end to end response time of an online 1:1 verification shall not exceed 2 seconds under nominal load, measured at the IDVS service boundary, as specified in SAM-IDV-007.
SAM-PER-010	eKYC and demographic verification responses shall not exceed three (3) seconds under nominal load at the IDVS service boundary.
SAM-PER-011	Interactive operator searches in the IDMS and CRVS (by SDIN, token, name, date of birth, phonetic and approximate matching) shall return first results in no more than three (3) seconds under nominal load.
SAM-PER-012	The automated processing of one enrolment packet (reception, verification, quality checks, routing to deduplication) shall complete in no more than fifteen (15) minutes, excluding the biometric deduplication itself and any manual step.
SAM-PER-013	Screen to screen navigation and standard page loads of the back office applications shall not exceed two (2) seconds for 95 percent of interactions under nominal load.
SAM-PER-014	All response time commitments shall be defined at a stated percentile (at least the 95th) and under a stated load, and shall be measurable by the supervision platform of VII.1.4.

3. Throughput (SAM-PER-015 to 017)

The sustained rates the platform must hold: deduplication intake, verification load and card production.

ID	Requirement
SAM-PER-015	Biometric deduplication throughput shall absorb the peak daily intake of SAM-PER-002 (approximately 2,100 enrolment packets per day) without the processing backlog exceeding the limit set in SAM-IDM-019, at a gallery size of 99,000, and shall maintain equivalent service at 250,000 records.
SAM-PER-016	The IDVS shall sustain its peak hourly load with headroom of at least 50 percent above the target peak without architectural change, as specified in SAM-IDV-006.
SAM-PER-017	The card personalisation chain shall sustain a production rate of 2,000 cards per day at the Apia centre (plus Salelologa if the production line option is exercised), sufficient to absorb the Version 1 cohort backlog within the M6b to M6c window of the Implementation Schedule (VII.2).

4. Scalability (SAM-PER-018 to 020)

Growth is absorbed by adding capacity on the existing architecture, with the scaling path documented.

ID	Requirement
SAM-PER-018	The System shall scale from the 2027 intermediate target to the full lifetime population (250,000 registered persons) without architectural change, without component replacement and without any additional licence procurement by the Purchaser, as specified in SAM-IDM-003.
SAM-PER-019	Scaling shall be achievable by adding capacity (compute, storage, nodes) on the existing two site architecture; the Supplier shall document the scaling path and the capacity thresholds that trigger it, feeding the capacity management of SAM-ADM-025.
SAM-PER-030	Verification side sizing shall use the collected baseline volumes: Passport Office 320 to 410 identity checks per day; Electoral Office 102,000 verifications over 15 months with event peaks; 5,500 to 6,000 births per year feeding the civil registration flow. The overall provisioned baseline is 250,000 registered persons (phase 1 target confirmed by SBS; the permanent resident population is about 300,000), and the System shall be extensible through the priced increment option to 800,000 persons in total, including the diaspora. The increment option is quoted firm in the proposal per the schedule of Section IV and its prices remain guaranteed for activation by the Purchaser during the contract. These

	baselines are sizing inputs; the Supplier shall state the headroom of its dimensioning.
SAM-PER-029	Offline and degraded mode behaviour is a contractual obligation: for each service tier, the fallback behaviour and the maximum acceptable degradation shall be defined in the service levels of part F. Services supporting continuous relying party operations, such as electoral registration, shall continue operating locally without time limit during a central outage, with automatic reconciliation on recovery.
SAM-PER-020	Licences and pricing shall cover the full lifetime volumes above; no licence in the proposal shall be capped below the 250,000 person baseline or below the stated transaction volumes, and every licence shall accommodate the activation of the increment option up to 800,000 persons at the guaranteed prices quoted in Section IV, without renegotiation.

5. Load testing and verification of sizing (SAM-PER-021 to 023)

Sizing claims are proven under load before acceptance, on representative volumes.

ID	Requirement
SAM-PER-021	Load and endurance tests demonstrating the volumes, response times and throughput of this subsection shall be executed before Operational Acceptance, on the pre production or production environment, as part of the test programme of part E (see SAM-TST block).
SAM-PER-022	Load test scenarios shall reproduce at least: the peak enrolment intake of SAM-PER-002 (approximately 2,100 packets per day) concurrent with deduplication at the target gallery size, the IDVS peak hourly load, and a site failover under load. Results shall be reported against each requirement of this subsection.
SAM-PER-023	The measurements of this subsection shall serve as the performance baseline of the service levels of part F; degradation below the baseline during operations shall be handled under the SLA regime.

6. Confirmation of final figures (SAM-PER-024 to 025)

How the working assumption figures of this chapter are confirmed and frozen with SBS.

ID	Requirement
SAM-PER-024	The sizing values of this subsection are working assumptions. They are confirmed with the Purchaser and finalised before contract signature.
SAM-PER-025	Should a confirmed value differ from the baseline by more than 20 percent, the Supplier shall re state the affected sizing during the design phase without change to the contract price, within the volume bounds published at bid time. This re basing applies to all sizing parameters of the System, including the IDMS and ABIS sizing parameters, and not only to the enrolment intake. The Purchaser's separate right to vary the contracted quantities at the time of Contract award is governed by ITP 44 and the Proposal Data Sheet, which list the variable quantities against the baselines of this subsection (SAM-PER-001, 002, 017, 026 to 028).

1.6 Cyber Security (SAM-CYB)

Framing note. The NDIDS is designated Critical Information Infrastructure (CII) of Samoa. This Section draws the consequences of that designation and of the cybersecurity framework already in force in Samoa, in particular the Government of Samoa Information Security Policy and the applicable information security standards issued under it, on which the emerging Critical Information Infrastructure Protection framework will build. The legal and regulatory instruments the System shall comply with are listed in Section VII.1.1. The competent national authority is the Ministry of Communications and Information Technology.

Standards and certification provisions applying to the whole of this Section. ISO 22301 is guidance: a documented and exercised continuity plan is mandatory, and no certification and no formal evidence of alignment is required. ISO/IEC 39794-5 is required as a capability with a transition allowance: ISO/IEC 19794-5 is accepted at go live with a committed migration to ISO/IEC 39794-5 by a date agreed with the Purchaser, and the biometric interchange citations of this Section are read with the same allowance. OWASP ASVS applies at Level 2 as the baseline of the System and at Level 3 for the authentication and for the PKI and HSM interfaces. Assurance relies on the certifications the proposed products already hold rather than on new platform level certification campaigns, as stated in SAM-CYB-134.

1.6.1 Critical Information Infrastructure and national alignment

The obligations that follow from the NDIDS being Critical Information Infrastructure: the security requirements already in force in Samoa, the designation itself, and the governance, risk and documentation duties attached to it.

ID	Requirement
SAM-CYB-001	The NDIDS is designated as Critical Information Infrastructure (CII) of Samoa. The Supplier shall design, implement, document and operate the System so that it can meet the obligations attached to that designation, including regulatory audits, inspections and reporting to the competent national authority, being the Ministry of Communications and Information Technology, throughout the Contract. Those obligations are read in three layers. First, the cybersecurity requirements already in force in Samoa, being the Government of Samoa Information Security Policy and the Information Security Standards issued under it, which apply from the effective date of the Contract under SAM-CYB-006. Second, the requirements specific to this procurement, which are those of this Section. Third, the enhanced requirements expected under the Critical Information Infrastructure Protection framework once it is established, which the System shall be able to accommodate without a redesign. The Supplier shall not create a parallel security regime for the System where a national one applies.
SAM-CYB-002	The Supplier shall maintain an Information Security Management System covering all Contract activities, certified against ISO/IEC 27001 (or equivalent) for the Supplier's relevant scope, and shall apply it to the System from design through operations and skills transfer.
SAM-CYB-003	The Supplier shall perform and maintain a documented risk assessment of the System (ISO/IEC 27005 or equivalent), reviewed at least annually and after any major change or incident, and shared with the Purchaser.
SAM-CYB-004	The Supplier shall support the Purchaser in national cyber crisis exercises and in cooperation with regional mechanisms (e.g. PaCSON), including at least one joint incident response exercise per year during the operation and support period.
SAM-CYB-005	All security documentation (architecture, configurations, procedures, runbooks) shall be treated as sensitive, kept current, held in the Purchaser's repository, and handed over as part of skills transfer.
SAM-CYB-006	The Supplier shall comply with the Government of Samoa Information Security Policy and with the applicable information security standards issued under it, for all Contract activities and for the System, from the effective date of the Contract. The Supplier shall state in its proposal how each applicable standard is met, and shall design the System so

	that the enhanced obligations expected under the Critical Information Infrastructure Protection framework, once that framework is established, can be met through configuration, procedure and documentation rather than through a redesign of the System. Where a provision of this Section and a provision of the Information Security Policy differ, the more demanding of the two applies, and the Supplier shall report the difference to the Purchaser rather than resolve it alone.
SAM-CYB-100	The Supplier shall adopt a documented risk assessment methodology aligned to ISO/IEC 27005, use the D8a Cycle 1 risk baseline as the initial risk register, and update that register at least annually and after any major change or incident, resolving the method and baseline SAM-CYB-003 defers to D8a.
SAM-CYB-101	The Supplier shall treat the standards baseline of this Section together with SAM-CYB-100 to SAM-CYB-134 as the detailed control set and accreditation target SAM-CYB-052 defers to D8a, and run a documented gap assessment against the World Bank cybersecurity guidelines within 60 days of the contract effective date.

1.6.2 Security monitoring, incident detection and response

Detecting and reporting security incidents: monitoring, triage and the notification duties toward SBS and national authorities.

ID	Requirement
SAM-CYB-010	The Supplier shall implement centralised security logging and monitoring (SIEM or equivalent) covering IDMS, IDVS, enrolment back end, card personalisation chain and supporting infrastructure, with alerting and documented triage procedures. One converged, open source based platform may satisfy both this security monitoring and the operational monitoring of SAM-INF-030, provided the security views, their retention and their integrity cannot be degraded or altered by operations roles (see SAM-ADM-016 and SAM-INF-034); a separate commercial SOC stack is not required. The operation of that monitoring is by the Purchaser: the ICT supervision cell of SBS watches the alerts and applies the triage procedures, the Supplier supporting it during the operation and support period under the service levels of part F and the joint exercises of SAM-CYB-004, and transferring the procedures under the capacity building programme. A permanently staffed security operations service, meaning a team dedicated to continuous monitoring and analysis, is not part of this procurement and shall not be priced in the proposal; should the Purchaser establish one later, whether its own, shared or regional, the Supplier shall give it access to the platform, its interfaces and its documentation at no additional charge.
SAM-CYB-011	The Supplier shall notify the Purchaser of any significant cyber incident without undue delay and at the latest within 24 hours of detection, and shall provide the information needed for the Purchaser to meet the statutory personal data breach notification of 72 hours (NDID Act ss.47 to 50) and any CII reporting obligation to the Ministry of Communications and Information Technology.
SAM-CYB-012	The Supplier shall maintain an incident response plan aligned with the Purchaser's obligations, including containment, forensics preservation, recovery and post incident review, tested at least annually. The Supplier shall maintain, and hand over to the Purchaser, a register of all personal data breaches as required by section 50(4) of the NDID Act 2024, and shall provide the elements needed for the Registrar General to notify affected individuals without undue delay and in plain and clear language where the breach presents a high risk to their rights (section 49), including an assessment of the effectiveness of the encryption and pseudonymisation applied to the affected data (section 50(3)).
SAM-CYB-013	Security monitoring, alerting, escalation, coordination and incident response for the System shall operate under arrangements agreed between the Purchaser and the Ministry of Communications and Information Technology acting through SamCERT, the Purchaser not being expected to carry the full incident response lifecycle on its own. The Purchaser is the single point of contact of the Supplier for those arrangements: the Supplier shall raise every security alert, escalation and incident with the Purchaser, and shall not report directly to SamCERT. The Supplier shall take part in establishing those arrangements within the first ninety (90) days of the Contract, shall align its own monitoring, alerting, escalation and incident response procedures with the SamCERT operating model and its standard operating procedures, and shall provide, through the Purchaser and on its instruction, the interfaces, feeds, documentation and points of contact that role requires, at no additional charge. The roles, responsibilities, procedures and interfaces between the Purchaser, SamCERT and the Supplier shall be documented,

	kept current and exercised through the annual exercises of this Section. This requirement does not move to the Supplier any duty that the law of Samoa places on a public authority.
SAM-CYB-033	Authentication transaction log retention is specified in SAM-IDV-065 (configurable by SBS, capped at the 2 year legal maximum of NDID Act s.37(3), automatic deletion or irreversible anonymisation); security logs retention shall be defined consistently with that limit and with investigation needs.
SAM-CYB-108	The Supplier shall retain security and monitoring logs (SIEM, network, administrative action logs) for 12 months online plus a further 12 months archived, within the two year statutory cap on authentication logs (NDID Act s 37(3)) and consistent with investigation needs, resolving the retention period SAM-CYB-033 defers to D8a.
SAM-CYB-116	The Supplier shall implement anomaly detection on enrolment and verification volumes per operator, per device and per registration point, with automated alerting to SBS and the Supplier's security operations function on deviation from an agreed baseline.

1.6.3 Resilience and continuity (CII grade)

This subsection covers the operational resilience of the System as a whole and not only its resilience to a cyber attack. It is kept under Cyber Security because the recovery objectives, the continuity plan and the exercises are the same whether the cause is an attack, a physical failure or a technical failure. The disaster recovery design itself is in SAM-ARC-021 and SAM-ADM-021 to 024, and the site and power prerequisites are in SAM-INF-020 to 024.

Continuity worthy of national infrastructure: the system withstands component loss, site loss and adverse conditions.

ID	Requirement
SAM-CYB-020	The System shall operate across the two existing sites (SBS server room as primary, Vodafone data centre as disaster recovery site). The ability to swap the primary and DR roles without redesign applies to the IDVS layer; the IDMS, the ABIS, the CRVS and the supporting tooling follow the active/passive disaster recovery model of SAM-ARC-021, sized to the recovery objectives of SAM-CYB-021 with a documented restore path. Failover and failback procedures shall be documented and exercised through at least one full failover and failback exercise per year, the first during Operational Acceptance; this exercise may be combined with the annual crisis exercise of SAM-CYB-004 and SAM-CYB-012. Restore testing keeps its own cadence (quarterly samples and one full restoration per year, SAM-ADM-019).
SAM-CYB-021	Recovery objectives: The starting proposal applies: IDVS RTO 4 hours and RPO 15 minutes; IDMS RTO 24 hours and RPO 1 hour; enrolment field operations tolerant to central unavailability through offline mode. .
SAM-CYB-022	Verification of identity shall degrade gracefully: offline verification of the signed QR code content on cards and credentials shall remain possible when the IDVS is unavailable.
SAM-CYB-023	Power continuity at the primary site: UPS bridging, generator autonomy, environmental monitoring, and controlled shutdown procedures protecting cryptographic modules against uncontrolled power loss (HSM zeroisation risk). Site adequacy works at the SBS server room shall be identified in the Supplier's site survey. UPS protection is in the Supplier scope and any standby generator is a Purchaser prerequisite, per the ICT Infrastructure component (SAM-INF-020 to 024).
SAM-CYB-024	The Supplier shall deliver and maintain a documented business continuity plan for the operated services, exercised through the annual exercises of this Section. No ISO 22301 certification, and no formal evidence of alignment with ISO 22301, is required.
SAM-CYB-122	The Supplier shall test and document the automatic generator and UPS changeover at least twice per year, with results reported to SBS within ten business days of each test; UPS protection is Supplier scope and any standby generator is a Purchaser prerequisite per SAM-CYB-023, this requirement covering the joint test only.
SAM-CYB-123	The Supplier shall define and implement a data backup retention and disposal schedule, applicable to every backup copy of NDIDS data regardless of hosting location, consistent with the data minimisation principle of section 27 of the Act.
SAM-CYB-124	The Supplier shall adopt the fixed recovery objectives: IDVS RTO 4 hours and RPO 15 minutes; IDMS RTO 24 hours and RPO 1 hour; enrolment field operations tolerant to central unavailability through offline mode; validated at the first Operational Acceptance failover exercise required by SAM-CYB-020.

1.6.4 Architecture security

Security built into the design: segmentation, encryption, key custody and hardened interfaces.

ID	Requirement
SAM-CYB-030	Security by design and defence in depth shall be applied as an architecture wide principle, across four layers, so that the failure of a single control does not expose the System. Network: segmentation between the enrolment, IDMS, ABIS and biometric store, IDVS and administration zones, with no direct exposure of the IDMS to external networks. Application: secure design, input validation, hardened configuration and the secure development lifecycle of SAM-CYB-053. Identity and access: individual accounts, least privilege, multi factor authentication and the access management requirements of Section 1.6.7. Data: encryption at rest and in transit, key management under SAM-CYB-031 and SAM-CYB-110, and minimisation of what each interface exposes, the IDVS exposing only the statutory token of the SDIN or per transaction tokenised identifiers (NDID Act s.31, s.32(2)). The Supplier shall present its security architecture layer by layer, stating for each layer the controls proposed, the threats they answer and the residual risk it asks the Purchaser to accept.
SAM-CYB-031	Encryption of personal and biometric data at rest and in transit using current, non proprietary algorithms; cryptographic keys generated and held in HSMs certified FIPS 140-3 Level 3 (or equivalent), under Purchaser control, with dual control key ceremonies, within the consolidated HSM footprint of SAM-INF-040 (one operational resilient pair serving all issuance and card and credential signing, plus the root CA device with its dual control backup; no per component HSM silo).
SAM-CYB-102	The Supplier shall submit, within 30 days of the contract effective date, a plan and a dedicated budget line for the establishment and operation of the PKI trust anchor and associated Hardware Security Modules, consistent with the consolidated HSM footprint fixed by SAM-CYB-031 and SAM-INF-040.
SAM-CYB-103	The Supplier shall demonstrate, wherever its biometric matching engine (ABIS) specification or reference architecture is proprietary or vendor specific, conformance to open standards (ISO/IEC 39794-5, ISO/IEC 19795 series, ISO/IEC 24745) sufficient to avoid single vendor lock in, and document and submit for SBS approval any deviation.
SAM-CYB-104	The Supplier shall conduct an independent security and data quality assessment of any legacy source system its enrolment process integrates with (including the SBS civil registration system), and not treat records from an unsupported or unpatched legacy system as authoritative without independent validation controls (duplicate detection, integrity verification, manual supervisory review) applied before that data enters the NDID register.
SAM-CYB-106	The Supplier shall design verification and data exchange interfaces to support future integration, on the same security and assurance terms as this Section, with relying parties not yet engaged as of this RFP, including Passport and Immigration and the financial sector.
SAM-CYB-109	The Supplier shall not store cryptographic key material, including backup encryption keys, on removable media, general purpose shared drives, or any location outside an approved key management system or HSM.
SAM-CYB-110	The Supplier shall implement a documented key management lifecycle (generation, distribution, rotation, revocation, destruction) covering the cryptographic modules and the key material of the trust services, consistent with ISO/IEC 19790 or FIPS 140-3 and with the practices of NIST SP 800-57, and shall deliver a Key Management Plan that SBS operates and maintains after transfer, subject to SBS audit at any time. Certificate specific provisions (policies, validity and rollover) are carried by the CP/CPS of SAM-INF-045.
SAM-CYB-111	The Supplier shall apply ISO/IEC 27017 and ISO/IEC 27018 controls to any cloud environment used under the bounded IDVS cloud option SAM-ARC-023 permits, in addition to that option's own limits (no biometric templates, no authentication record store, master identity data and signing keys never leaving Samoa).
SAM-CYB-119	The Supplier shall review and document firewall rules on a fixed schedule of at least once per quarter, not solely on ad hoc or personnel change events.
SAM-CYB-120	The Supplier shall maintain an inventory of all external network connections to any NDIDS system component, updated at every change and reviewed with SBS at least quarterly.

SAM-CYB-133	The Supplier shall grant SBS or its nominated auditor the right to witness or audit any HSM or PKI key generation ceremony conducted under SAM-CYB-031.

1.6.5 Supply chain, personnel and physical security

Trust in what is delivered, who delivers it and where it runs: component provenance, vulnerability management, personnel vetting and the physical security of the facilities hosting the System.

ID	Requirement
SAM-CYB-040	Supply chain risk management: the Supplier shall provide a Software Bill of Materials (SBOM) for delivered software, disclose the origin of critical hardware and software components, and notify the Purchaser of any change of control or sourcing affecting critical components.
SAM-CYB-041	Vulnerability management: documented patching SLAs by severity, monitoring of advisories for all components of the SBOM, and a coordinated vulnerability disclosure channel.
SAM-CYB-042	Personnel with privileged or physical access to CII components shall be individually identified, bound by confidentiality undertakings, and vetted to the extent permitted by the laws of Samoa and of the Supplier's jurisdiction; the Purchaser may refuse access to named individuals.
SAM-CYB-121	The Supplier shall ensure that every facility hosting NDIDS production systems provides, at minimum, badge controlled access, CCTV coverage and a visitor log.
SAM-CYB-127	The Supplier shall implement continuous vulnerability scanning of all NDIDS infrastructure and application components, at least weekly for internet facing components and monthly for internal components, with results reported to SBS on the cadence agreed in the Security Test Plan.
SAM-CYB-131	The Supplier shall remediate security findings from any test under this Section within the following minimum service levels, measured from confirmed identification and scored under CVSS v3.1 or later: Critical (9.0 and above) within 5 calendar days; High (7.0 to 8.9) within 15 calendar days; Medium (4.0 to 6.9) within 30 calendar days or the next scheduled release, whichever is sooner; Low (below 4.0) within the next scheduled release.

1.6.6 Secure development, assurance and testing

Security built through a defined process and then proven, not asserted: the secure development framework, independent testing, reviews and the assurance evidence the Purchaser receives.

ID	Requirement
SAM-CYB-050	Independent penetration testing by a third party firm (not the Supplier) before Operational Acceptance and at least annually thereafter; the Supplier shall remediate findings according to severity based SLAs.
SAM-CYB-051	Security acceptance criteria shall be part of the Operational Acceptance Tests (hardening verification, access control tests, failover test, restore test from backups).
SAM-CYB-052	The control set of this Section, being the requirements of Sections 1.6.1 to 1.6.9 read with the standards provisions stated at the head of this Section, is the accreditation target of the System. The Supplier shall keep it as a single control register, map each control to the evidence that demonstrates it, and update the register at each major release and whenever the Purchaser adopts a national cyber guideline or standard during the Contract, under the gap assessment of SAM-CYB-101.
SAM-CYB-053	The Supplier shall follow a defined Secure Software Development Framework, being the NIST Secure Software Development Framework (SP 800-218) or an equivalent secure development lifecycle, shall evidence in its proposal that the framework is established in its organisation, and shall demonstrate its application to the System through design, development, integration, release and maintenance. The controls of this Section that belong to that lifecycle shall be operated as part of it and not as isolated activities, in particular the static and dynamic application security testing and the manual secure code review of SAM-CYB-128, the vulnerability management of SAM-CYB-041 and SAM-CYB-127, the remediation service levels of SAM-CYB-131 and the security test planning of SAM-CYB-126. The Supplier shall deliver, at each major release, evidence of the

	security activities performed, of their results and of how each finding was disposed of. Where custom development is carried out with the resources of the Purchaser or of a local partner, the same framework applies to that work.
SAM-CYB-118	The Supplier shall submit the biometric matching engine, whether proprietary or open, to independent SBS commissioned testing of its containment, isolation and template protection approach under the vendor testing obligations, regardless of the underlying vendor or licensing model.
SAM-CYB-126	The Supplier shall submit a Security Test Plan for SBS approval within 30 days of the contract effective date, covering every testing obligation of this Section, updated at each major release or material architecture change.
SAM-CYB-128	The Supplier shall integrate static and dynamic application security testing into its build and release pipeline, and conduct manual secure code review of every security critical module (authentication, biometric interface, PKI and HSM integration, consent and access control) prior to each production release, benchmarked against OWASP ASVS Level 2 as the system baseline and Level 3 for the authentication and PKI and HSM interfaces.
SAM-CYB-129	The Supplier shall conduct presentation attack detection testing conformant to ISO/IEC 30107-3 prior to go live; where COTS capture devices already hold a valid PAD certification issued by a laboratory accredited for biometric testing under the NIST National Voluntary Laboratory Accreditation Program (NVLAP) or an equivalent accreditation scheme, that certification is accepted as evidence for those devices; re testing is required on any material change to the capture devices or the PAD subsystem, not on a fixed annual cadence.
SAM-CYB-130	The Supplier shall evidence the biometric matching engine's algorithmic performance through current NIST FRVT or FATE results, and conduct one operational performance test on representative Samoa enrolment data prior to go live (false match, false non match, failure to enrol and failure to acquire rates); re testing is required on any material change to the biometric engine, not on a fixed annual cadence.
SAM-CYB-132	The Supplier shall cooperate fully, at no additional cost for a reasonable frequency and scope, with independent security testing (penetration testing, source code audit, biometric performance and PAD testing) that SBS or a third party nominated by SBS may commission on any part of the solution at any time during the contract term, and not treat the exercise of that right as a breach of any warranty or support obligation.
SAM-CYB-134	The Supplier shall evidence, in its technical proposal, the certifications its proposed products already hold, including NIST FRVT or FATE results for the biometric matching engine, independent ISO/IEC 30107-3 PAD certification for capture devices, FIPS 140-3 or ISO/IEC 19790 certification for the HSMs, and ISO/IEC 27001 for the organisation; the RFP relies on these existing product certifications rather than requiring new platform level certification campaigns.

1.6.7 Identity and access management

This subsection gathers the access management requirements that were spread across this Section. The vetting of personnel holding privileged or physical access is in SAM-CYB-042, and the administration and role separation requirements of the platform itself are in SAM-ADM-001 to 006.

ID	Requirement
SAM-CYB-032	Privileged access management: least privilege, individual accounts, MFA for all administrative access, session recording for critical operations, and periodic access reviews.
SAM-CYB-043	Remote access from outside Samoa for support purposes shall be disabled by default, activated case by case under Purchaser approval, individually authenticated, logged, time limited and monitored.
SAM-CYB-107	The Supplier shall prohibit remote administrative access to any NDIDS production environment from personal or unmanaged devices, and provide managed, SBS approved endpoints or a hardened virtual desktop for all remote administrative sessions, supplementing SAM-CYB-043 for domestic device use.
SAM-CYB-115	The Supplier shall implement dual control (maker checker) for every registration desk operation capable of creating, amending or deactivating an identity record, with every operator action logged against an individually attributable account under SAM-CYB-032.

1.6.8 Biometric security

This subsection gathers the requirements specific to the security of the biometric chain. The performance of the biometric engine is covered by Section VII.1.2.2 and its testing by SAM-CYB-129 and SAM-CYB-130.

ID	Requirement
SAM-CYB-105	The Supplier shall design its solution so that authentication factors and technical parameters, including facial verification, are configurable to conform to the National Digital ID Regulations 2025 as finalised, without re architecture, and update its configuration within 30 days of the Regulations' commencement or amendment.
SAM-CYB-112	The Supplier shall implement presentation attack detection at every biometric capture point, for enrolment and verification, conformant to ISO/IEC 30107 Parts 1 to 3, at a minimum of PAD level 1 at every capture point and PAD level 2 at enrolment capture points.
SAM-CYB-113	The Supplier shall implement biometric template protection consistent with ISO/IEC 24745, such that stored biometric references are irreversible and are renewable or revocable without physical re enrolment of the data subject, wherever technically feasible; this qualifier is deliberate and shall not be read as an absolute obligation where the technology does not yet support it.
SAM-CYB-114	The Supplier shall implement enrolment fraud controls comprising liveness detection, deduplication checks against the existing register, and supervisor (maker checker) verification of every new enrolment record prior to activation.
SAM-CYB-117	The Supplier shall design, document and maintain an ABIS compromise containment plan (rate limiting and anomaly detection on match queries, and a defined procedure to revoke and reissue affected biometric templates without full re enrolment of the affected population, wherever technically feasible), in addition to the network segmentation SAM-CYB-030 requires.

1.6.9 Privacy and data protection by design

This subsection carries the overarching privacy and data protection requirement of the System. It does not replace the data protection controls carried elsewhere in this Request for Proposals; it requires the Supplier to show them working together.

ID	Requirement
SAM-CYB-060	Privacy and data protection shall be built into the design and the operation of the System and shall not be obtained by later correction. The Supplier shall demonstrate in its proposal, and shall maintain throughout the Contract, how the principles of the National Digital Identification Act 2024 and of the National Digital ID Regulations 2025 are given effect by design: lawfulness and purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, accountability, and the rights of the data subject. The demonstration shall bring together in one coherent framework, without restating them, the data protection controls this Request for Proposals already carries in its architecture, encryption and key management, consent, logging and retention, biometric, breach management and backup requirements, and shall state for each principle the design decision taken, the control that gives it effect and the evidence that the control works. The Supplier shall support the Purchaser in preparing and in updating the data protection impact assessment of the System, and privacy and data protection by design shall be part of the acceptance evidence required by SAM-CYB-051.

C. Service Specifications, Supply and Install Items (Implementation Services, SAM-SVC-001 to 060)

This chapter specifies the services that turn the specifications into a running system: design workshops with SBS, development and configuration, integration with existing and future systems, data preloading, documentation, training delivery, the Supplier's team and project management, and warranty and post acceptance support. Detail deferred by the technical chapters lands here: the project inception workshops, the relying party concertation workshops and the cross government PKI workshop are part of the procured services.

Scope and price boundary of the deferred details: outcomes of the design and concertation workshops that remain within the capabilities, behaviours and volumes stated in this Section VII are part of the contract scope and price; only outcomes exceeding those stated capabilities, behaviours or volumes follow the contract change procedure.

2.0 Overview: main activities and responsibilities (non exhaustive)

The lists below give bidders a consolidated view of the work ahead. They are indicative and non exhaustive: the requirements of Section VII and the Contract prevail, and the Preliminary Project Plan of Section IV asks each Proposer to state its own assessment of these responsibilities.

The Supplier's main activities under the project include, non exhaustively:

- detailed design, and the workshop programme (project inception technical workshops, relying party concertation workshops, cross government PKI workshop);

- supply, installation, configuration and integration of all subsystems of Section VII.1, on the national sites;

- delivery and deployment of the enrolment fleet, the card personalisation chain and the ICT infrastructure of part D;

- preloading of the CRVS reference data and establishment of the interfaces in both directions;

- testing from the early proof of concept through the Operational Acceptance Tests of part E;

- support to the mass registration campaign (field support, hotline, spares logistics);

- operation of the recurrent services and support through warranty and the post acceptance period, per the service levels of part F;

- training, skills transfer and capacity building per annex to 2.4, executed along the project and completed before the end of the financing period;

- documentation, in both languages where required, and the knowledge base;

- relying party onboarding support and the relying party pilot;

- project management, reporting and quality assurance;

- exit management and reversibility at the end of the Contract.

The Purchaser retains, non exhaustively, and further to GCC Clause 10 and the Agreed Project Plan:

- the premises and sites: server rooms, card personalisation premises, enrolment and registration sites, with their fit out where allocated to the Purchaser in the inventory tables;

- the legal milestones (Purchaser prerequisites P1 to P5 of VII.2), which condition specific Supplier milestones and open time extension rights where late;

- the staffing of operations: enrolment operators, adjudication operators, registrars and the staff designated for skills transfer, and their availability;

- the connectivity links between sites and to the internet (unless priced as an option) and the standby generation allocated to the Purchaser in the inventory;

- timely decisions, approvals, and access to premises, systems and information;

- the coordination of government stakeholders and relying parties, including the workshop calendars;

- the ownership of policies and configuration decisions reserved to SBS throughout Section VII (thresholds, assurance policies, fee schedules and similar);

- the treatment of personal data as controller, within the frame of the NDID Act 2024.

Framing note (context, no requirements): the advisory Consortium performs the quality review of the Supplier's work on behalf of SBS; the requirements below therefore give the Purchaser and its advisers the corresponding access rights. The existing environment (SBS server room, Vodafone site) is described in VII.4: the services run on this existing environment, not greenfield.

2.1 Analysis and detailed design

The design phase turns Section VII into build ready specifications, through the workshop programme with SBS and the stakeholders.

ID	Requirement
SAM-SVC-001	The Supplier shall conduct detailed specification and design workshops with the Purchaser (SBS) at the start of the contract, on site in Apia. The workshops shall cover every subsystem of Section VII, the operating procedures, and the recurring purchases (consumables, licences, spare parts) so that SBS can verify it is free to replace any consumable or component later. SBS staff designated for skills transfer shall take part in all workshops. Beyond these design workshops, the Supplier shall support the project inception technical workshops (detailed functionalities, flows and interaction elements of the Section VII blocks), the post procurement relying party concertation workshops (authentication modalities and attribute sharing per use case, per the IDVS block), and the cross government PKI workshop with MCIT, the transport authority and the Passport Office.
SAM-SVC-002	The Supplier shall deliver detailed functional and technical specifications covering all requirements of Section VII, with a traceability matrix from each SAM requirement to the design element and later to the test cases that verify it.
SAM-SVC-003	All business processes (enrolment, adjudication, identity lifecycle, card issuance, civil registration, relying party onboarding) shall be modelled in BPMN 2.0 and DMN and delivered as executable, versioned configurations of the workflow engine, with their source, so that after handover SBS can adjust decision rules, statuses, thresholds and notification triggers through DMN configuration, and evolve the process models themselves with the assisted workflow update service of SAM-IDM-127.
SAM-SVC-004	The Supplier shall produce the detailed design of the national ID card (layout, security features, machine readable code) in compliance with VII.1.2.4 and the NDID Act 2024. The design, once approved, is the exclusive property of the Purchaser.
SAM-SVC-005	The design deliverables shall include, at minimum: the system architecture document, the data models, the interface specifications (OpenAPI), the security

	design, the sizing and capacity plan, and the deployment plan on the two existing sites (SBS server room and Vodafone data centre).
SAM-SVC-006	No development, configuration or procurement of equipment shall start before the corresponding design deliverable has been formally approved by the Purchaser (design gate). The Purchaser's review period shall be defined in the agreed project plan.
SAM-SVC-007	The Supplier shall keep the specifications and the traceability matrix updated throughout the contract; every approved change request shall be reflected in them before implementation.

2.2 Development, configuration and integration

The build itself: development where needed, configuration wherever possible, and the integration of all components into one platform.

ID	Requirement
SAM-SVC-008	The Supplier shall provide and maintain the project environments: development, test, pre production and production, consistent with the architecture of VII.1.3. Test and pre production environments shall be representative of production and shall remain available to the Purchaser throughout the contract.
SAM-SVC-009	The source code of all custom and open source components, and all configurations and parameter sets, shall be maintained in the Purchaser's own source code repository, under version control, with automated build and test pipelines (continuous integration) operational in that repository from the start of development.
SAM-SVC-010	The Purchaser and its designated advisers may review the code, the configurations, the pipelines and the development practices at any time, and may attend or replay any build. The Supplier shall respond to review findings within the timescales of the agreed quality plan.
SAM-SVC-011	Configuration shall be preferred over custom development wherever the required behaviour can be achieved by configuration of the delivered platforms. Any custom development shall be justified and its maintainability by SBS addressed in the skills transfer plan (annex to 2.4).
SAM-SVC-012	Every release shall be reproducible from the repository: tagged sources and configurations, documented build procedure, release notes listing changes, fixed defects and known limitations.
SAM-SVC-013	The Supplier shall operate a defect and issue tracking tool shared with the Purchaser, covering the whole contract (development, tests, deployment, warranty), with severity levels and resolution targets agreed in the quality plan.
SAM-SVC-014	Development and configuration shall follow secure development practices consistent with VII.1.6, including dependency management and the production of a software bill of materials (SBOM) for each release.

2.3 Integration with existing and future systems

The bridges to Samoa's existing landscape and the systems to come, built on the open interfaces of Section VII.

ID	Requirement
SAM-SVC-015	The Supplier shall integrate with the existing legacy CRVS system (in service since 2003) for the extraction of the civil registration stock, in read only mode, without modification of the legacy system beyond what is agreed with the Purchaser. The legacy system remains the system of record for new vital events during V1 (see VII.1.2.6).
SAM-SVC-016	All integrations delivered under this contract shall be exposed through documented, versioned APIs (REST/JSON, OpenAPI) so that future government systems and relying parties can integrate without Supplier involvement, under the relying party framework of VII.1.2.3.
SAM-SVC-017	The Supplier shall provide and maintain an integration test environment (sandbox) usable by third parties for the certification of their integrations, as required by VII.1.2.3, from the opening of the relying party onboarding process.

SAM-SVC-055	The Supplier shall provide relying party onboarding support services: an onboarding toolkit and documentation, integration support through the sandbox of SAM-SVC-017, and template agreements for relying parties covering at minimum permitted use, information provided, security and data protection, service availability, support, fees and responsibilities. Onboarding follows the per use case authorisation regime of the IDVS block.
SAM-SVC-018	For each integration with an external system, the Supplier shall deliver an interface specification agreed with the counterpart organisation, covering data content, security (encryption in transit, endpoint authentication), availability expectations, and a fallback that isolates each system if the channel fails.
SAM-SVC-019	Integrations required at later phases (per the Implementation Schedule) shall be designed for from the start: the platform shall not require redesign to add a mandated sector integration under section 14(4) of the NDID Act 2024.

2.4 Training (delivery requirements)

The substance (depth, types of training, pairing, assessment, link to payment) is set by Annex 2.4. Here: the delivery requirements.

ID	Requirement
SAM-SVC-032	All training under this contract is part of the contract price. The training programme, audiences, depth targets and assessment methods are defined in the skills transfer plan required by Annex 2.4, which is the governing document for the substance of the training.
SAM-SVC-033	The Supplier shall apply a train the trainer approach for high volume audiences (enrolment operators, card production operators): the Supplier trains and certifies SBS trainers, provides the training kits, and supervises the first cascaded sessions.
SAM-SVC-034	All training materials shall be handed over to the Purchaser in editable form, and all delivered sessions shall be recorded and lodged in the shared knowledge base of the contract.
SAM-SVC-035	Every training activity shall end with a systematic assessment of the trainees against the stated objectives, with certificates issued and results reported to the project executive committee, as inputs to the scored transfer assessment of Annex 2.4.
SAM-SVC-036	The Supplier shall provide training environments (including kits and card printers reserved for training and dry runs) so that training and rehearsals never run on production data or production equipment.

2.5 Data migration and preloading

The data work that precedes operations: CRVS preloading and the reference data the platform starts with.

ID	Requirement
SAM-SVC-020	The Supplier shall deliver a data migration and preloading strategy and plan as a design deliverable, covering: extraction from the legacy CRVS, transformation and cleansing rules, loading into the new CRVS stock database, preloading of biographic data onto the enrolment kits, dry runs, reconciliation, and fallback. The plan is subject to Purchaser approval before any production data is processed.
SAM-SVC-021	The Supplier shall implement the preloading of biographic data from the existing digital CRVS system onto the enrolment kits, so that during enrolment an operator enters a name and receives candidate matches from the existing records for cross checking (preloading without pre assigned numbers: the SDIN is generated on the IDMS side).
SAM-SVC-022	The Supplier shall execute the ingestion of the CRVS stock into the new civil registry database per VII.1.2.6, preserving source identifiers for traceability, with at least one complete dry run on a representative extract before the production run.
SAM-SVC-023	Data quality shall be measured, not asserted: every migration and preloading run shall produce a quality report (records processed, loaded, rejected with reasons, duplicate candidates, incomplete records, referential inconsistencies) against quantified acceptance thresholds agreed with the Purchaser in the migration plan.

SAM-SVC-024	Cleansing and transformation rules shall be documented, approved by the Purchaser, and applied in a traceable way: for every modified record the original value shall remain retrievable.
SAM-SVC-025	The Supplier shall train SBS on the data models and extraction procedures of its own systems (including the biometric engine and the card personalisation software), per the data migration milestone obligations of Annex 2.4 (SAM-TRF-024, SAM-TRF-038).
SAM-SVC-026	All migration and preloading operations on personal data shall comply with the NDID Act 2024 and the security requirements of VII.1.6: encrypted transfers and media, access limited to named staff, no production data in development environments, and secure destruction of intermediate copies, evidenced to the Purchaser.

2.6 Documentation

The documentation set delivered with the system, kept current through every change.

ID	Requirement
SAM-SVC-027	The Supplier shall deliver and maintain the full documentation set: technical documentation (architecture, data models, interfaces, security), operations documentation (installation, administration, supervision, backup and restore, disaster recovery, incident response), and user documentation per role (enrolment operator, adjudicator, registrar, relying party manager, card production operator).
SAM-SVC-028	All documentation shall be written in English, delivered in editable format, held in the Purchaser's repository and knowledge base, and updated at every release. Documentation is part of the acceptance scope of each milestone.
SAM-SVC-029	The troubleshooting guide is specified in Annex 2.4 (SAM-TRF-022): the Supplier shall deliver it as part of the documentation set of this Section.
SAM-SVC-030	The usability of documentation and training content by an SBS employee working alone is governed by Annex 2.4 (SAM-TRF-020), which applies to the whole documentation set of this Section.
SAM-SVC-031	Citizen facing and enrolment operator facing materials shall be suitable for bilingual use (English and Samoan); the Purchaser provides or validates the Samoan versions, from editable sources delivered by the Supplier.

2.7 Supplier's team

The people the Supplier commits: key experts, continuity obligations and on site presence during the critical phases.

ID	Requirement
SAM-SVC-037	The Supplier shall mobilise at minimum the following six Key Experts, whose experience is evaluated under Section III and whose CVs are submitted on the Section IV forms: Project Manager; ID Solution Architect and Biometrics / ABIS Specialist; Cyber Security and Data Protection Expert; Enrolment Operations Manager; Card Personalisation Manager; Deputy Local Project Manager, based in Samoa for the whole duration of the Contract, who also leads local capacity building and acts as Training and Skills Transfer Lead.
SAM-SVC-038	The Project Manager, or a designated alternate with authority to decide, shall be present on site in Samoa during the critical phases: design workshops, installation and commissioning, start of mass enrolment, operational acceptance tests, and the relying party pilot. On site presence requirements per phase shall be stated in the project plan.
SAM-SVC-039	Replacement of a Key Expert requires the Purchaser's prior written approval and a replacement with equal or better qualifications; the Supplier shall ensure an overlap period sufficient for handover within the Supplier's team.
SAM-SVC-040	The Supplier shall involve local Samoan technical resources in its teams, including as subcontractors who may later join SBS. These local resources assist during installation and through the first months of operation, and provide continuity when the Supplier's foreign staff are absent.
SAM-SVC-041	The working language of the project is English. All deliverables, meetings, reports and training are in English.

2.8 Project management

How the project is run and reported: governance, planning, risk and the cadence agreed with SBS.

ID	Requirement
SAM-SVC-042	The Supplier shall hold a kick off meeting within (indicatively two) weeks of the contract effective date, presenting the project plan, the mobilisation, and the outline of the skills transfer and reversibility plans (see annex to 2.4).
SAM-SVC-043	Project governance shall comprise at minimum: a steering committee (strategic decisions, plan amendments), and a project executive committee meeting at least monthly (progress, risks, skills transfer reporting, decisions). The Supplier prepares the material and the minutes of both.
SAM-SVC-044	The Supplier shall submit a monthly progress report covering: progress against the baseline schedule and milestones, deliverable status, risks and issues with mitigation, skills transfer execution, quality indicators, and a rolling plan for the next period.
SAM-SVC-045	The Supplier shall maintain the project baseline schedule aligned with the Implementation Schedule of Section VII, and shall report any forecast slippage on a critical milestone as soon as it is known, with a recovery plan.
SAM-SVC-046	The Supplier shall maintain a risk register shared with the Purchaser, reviewed at every executive committee, with owners, scores and mitigation actions.
SAM-SVC-047	The Supplier shall deliver and apply a quality plan covering reviews, testing gates, configuration management, documentation standards and defect management, consistent with part E (Testing and Quality Assurance).
SAM-SVC-048	The Purchaser may be assisted by advisory consultants. The Supplier shall give them the same access as the Purchaser to deliverables, environments, tests and committees, and shall respond to their quality findings under the quality plan.

2.9 Warranty and post acceptance support

What the Supplier owes after acceptance: warranty, support and the recurrent services carrying the platform in operation.

ID	Requirement
SAM-SVC-049	The Supplier shall provide a warranty on the whole system (software, configurations, equipment) from Operational Acceptance, for the period stated in the SCC, covering the correction of defects at no additional cost.
SAM-SVC-050	During the warranty and support period the Supplier shall operate a support service (helpdesk, incident intake, escalation) meeting the service levels of part F, with penalties as per the SCC.
SAM-SVC-051	The Supplier shall provide reinforced on site support during the mass enrolment campaign and during the first year of operation of the card production centres, dimensioned in the project plan.
SAM-SVC-052	Post acceptance support shall be organised as a progressive transition to operation by SBS: from Supplier led with SBS observing, to SBS led with Supplier on call, following the depth targets and assessments of Annex 2.4. Support statistics shall evidence this progression.
SAM-SVC-053	The Supplier shall guarantee the availability of spare parts and consumables for the delivered equipment for the duration stated in the SCC, and shall establish the licence and support contracts for third party components in the name of SBS.
SAM-SVC-054	At the end of the support period the Supplier shall execute the exit and reversibility obligations of Annex 2.4 (reversibility plan, refresh training, handover of all materials, confirmation that every transfer activity is complete).

Annex to 2.4: Skills Transfer and Capacity Building (SAM-TRF-001 to 040)

Framing note (context, no requirements): what falls to the Supplier (everything below) is paid within the contract price; what lies beyond the System (SBS monitoring, relying party engagement, sustainability model, cyber awareness, data protection, public policy work) is funded separately by the project and is never billed by the Supplier.

1. Objective and general principles

Why this annex exists: Samoa's autonomy and the durability of the platform beyond the financing period, organised as measurable transfer.

ID	Requirement
SAM-TRF-001	The skills transfer obligations of this Annex shall bring the SBS teams to the point where they can operate, support, maintain and evolve the System on their own before the contract ends. The test is not whether training was delivered; the test is whether the Purchaser can run the System without the Supplier.
SAM-TRF-002	Samoa has a small pool of qualified technical staff, and the Supplier shall take this as its own constraint rather than as the Purchaser's problem. The Supplier is responsible for defining the profiles it needs on the Purchaser side, for assessing the candidates SBS presents against those profiles, and for executing the transfer.
SAM-TRF-003	Where a motivated candidate falls short of the prerequisites, the Supplier shall propose an upskilling path rather than reject the person.
SAM-TRF-004	All activities in this Annex are part of the contract price. The Supplier shall not charge any of them against the Purchaser's capacity building allocation, which is reserved for activities beyond the System.

2. The skills transfer plan

The plan that makes transfer concrete: named people, named modules, agreed depth and dates.

ID	Requirement
SAM-TRF-005	The Supplier shall deliver a skills transfer plan as an annex to the project plan, within four weeks of the contract effective date, and shall present it in outline at the kick off meeting.
SAM-TRF-006	The skills transfer plan is a living document, amendable by the steering committee. Its execution shall be reported at every project executive committee.
SAM-TRF-007	The plan shall contain, at a minimum: (a) the list of systems, processes, equipment and services subject to skills transfer, following the work lot breakdown of the contract, so that responsibility can be assigned and tracked lot by lot; (b) the success criteria for each transfer activity and the method used to assess them; (c) the resources involved on the Supplier side and to be mobilised on the Purchaser side, including any profiles the Purchaser has not yet anticipated; (d) the skills prerequisites for the Purchaser resources, each classified as mandatory, desirable or optional; (e) the transfer activities themselves, with their content and the setting in which they are run; (f) the schedule of transfer activities, integrated into the overall project schedule while remaining separately trackable.

3. Pairing, and the work lot as the unit of transfer

Transfer happens by doing: SBS staff paired with Supplier staff, work lot by work lot.

ID	Requirement
SAM-TRF-008	Each work lot shall have a named owner on the Supplier side and a named owner on the Purchaser side, and Purchaser and Supplier resources shall work in pairs on each lot.
SAM-TRF-009	The Supplier owner of a lot is also responsible for the reversibility plan of that lot, which the Purchaser lot owner reviews and approves.

SAM-TRF-010	The Purchaser lot owner is expected to be active, proposing improvements to the transfer and taking part in defining the success criteria, not receiving a service passively. The Supplier shall organise the transfer to enable this active role.

4. Depth of competency scale

A shared scale for how deep each competency must go, so transfer is measurable rather than declarative.

ID	Requirement
SAM-TRF-011	A single depth of competency scale shall be used across the whole contract, so that the target depth per subsystem can be stated, argued and verified. The scale below applies.
SAM-TRF-012	The Supplier shall propose a target level on the scale for each subsystem and module, based on its criticality, the expected maintenance frequency and the complexity of the technology. SBS reviews the proposal and may require a greater depth in the name of its independence; the Supplier prices the transfer accordingly.
SAM-TRF-013	The target is not uniform across the System. A proprietary biometric matching engine sits at operations and support depth. The reference registries, the business workflows and the number generator, which are the components Samoa must own, sit at the top of the scale.

Depth of competency scale (single scale for the whole contract): five named bands for software, ordered from the shallowest to the deepest, plus one separate hardware and vendor management track that applies to equipment and third party contracts and does not rank against the software bands.

Band	The Purchaser team can
1. Operate	Access the software or the equipment, use it, start and stop it, and confirm that it is working.
2. Supervise and support	Run a sanity check, troubleshoot, supervise and monitor.
3. Deploy	Redeploy from a delivered build, roll back to a previous version, compile and archive a custom software component.
4. Evolve	Modify the user interface, the API services, the source code and the data model of custom components, and add new functionality.
5. Full source mastery (top of the scale)	Master the architecture and the full source code of a custom component, including its external libraries.
H. Hardware and vendor management (separate track)	Diagnose equipment faults, read the architecture and network diagrams, raise and follow support tickets, and manage licence renewals.

5. Types of training

The training formats mobilised, from formal sessions to side by side operations.

ID	Requirement
SAM-TRF-014	The Supplier shall run three types of training. Operations: operate, monitor, report incidents; start and stop the platform, recover from errors, fail over to disaster recovery, measure performance, report against service levels; applies to every component, open or proprietary. Support: investigate incidents, gather the right evidence, triage, install updates and patches, run first line diagnosis; applies to every component, open or proprietary. Maintenance and evolution: fix defects and evolve the platform; understand the architecture and the source code, debug it, evolve the APIs, the data models and the interfaces, run the build, the tests and the non regression campaigns; applies to open source and custom components.
SAM-TRF-015	Proprietary components are exempt from maintenance and evolution depth, which is exactly why a proprietary choice must be justified: for each proprietary component proposed, the Supplier shall justify the choice against an open alternative and state how the Purchaser will nonetheless retain sufficient autonomy. This justification is part of the Proposal and of the design deliverables.

SAM-TRF-016	The asymmetry is deliberate and shall be respected in the design: a proprietary component on which Samoa never reaches maintenance depth is acceptable for a secure core such as biometric matching; it is not acceptable for the business workflows or the reference registries.

6. How the transfer is executed

The execution discipline: transfer runs along the project, inside real work, not as a course at the end.

ID	Requirement
SAM-TRF-017	On the job training is necessary and not sufficient. Every work lot shall be preceded and followed by formal transfer, structured as follows: preparation of training material and documentation covering the theory, the technical procedures and the business processes; delivered sessions, in person or online, recorded by the Supplier and lodged in the shared knowledge base of the contract; on the job training across the project phases, favouring dry runs by the Purchaser team outside the production system; a review session with questions, clarification and update of the training content in the light of what did not land; systematic assessment of the staff who received the transfer, with certificates issued and the training objectives measured; and formal presentation and closure of the transfer activity at the project executive committee.
SAM-TRF-018	Immersion is required during the development phases: the Purchaser's technical staff and architects shall spend time inside the Supplier's technical teams, at the Supplier's cost, to absorb the development, build, test and deployment environments and to establish the working relationships that will carry the later troubleshooting.

7. Knowledge base and source code

What Samoa keeps: the knowledge base, the documentation and the source code and build chain of the sovereign components.

ID	Requirement
SAM-TRF-019	All contract knowledge shall be held in a single shared portal (the knowledge base): documents, guides, training material, session recordings, and the tools and platforms used for development, build, test, acceptance and deployment. The knowledge base is a living resource, maintained throughout the contract and handed over to the Purchaser.
SAM-TRF-020	Given the volatility of technical staff in a small administration, the training content shall be usable by an SBS employee working alone, so that a new joiner can be brought up to speed without recalling the Supplier.
SAM-TRF-021	The source code of open source and custom components shall be delivered to SBS in the Purchaser's own repository, integrated with automated build and test pipelines, and commented in English (see SAM-SVC-009).
SAM-TRF-022	The Supplier shall produce a troubleshooting guide, lodged in the knowledge base, structured so that it can be maintained by SBS thereafter.
SAM-TRF-023	**The acceptance test of the transfer is practical.** The ability of the SBS team to build, test, troubleshoot and deploy a new version of the software is itself an acceptance criterion of the contract: not a training report, but a working deployment performed by the Purchaser's team, observed and evidenced.

8. Skills transfer across the contract milestones

Transfer obligations attached to each milestone, so progress is verified as the project advances.

ID	Requirement
SAM-TRF-024	The Supplier shall execute, at each contract milestone, at minimum the transfer obligations of the table below, and shall report completion at the corresponding milestone review.

Milestone	Supplier obligation
Kick off	Present the skills transfer and reversibility plans in outline. Identify the complex subsystems that will need long term external expertise. Define the Purchaser profiles needed. Identify the Purchaser champions on the critical subjects: biometrics, kits, support, printing.
Design workshops	Cover operation and maintenance, card personalisation, software and equipment, procedures and use cases, and the list of recurring purchases, so that SBS can verify it is free to replace any consumable or component later.
Development	Immerse the Purchaser technical team in the Supplier environments, at the Supplier cost.
Subsystem acceptance	Establish licence and support contracts in the name of SBS, and train the named SBS owner on their lifecycle. Deliver specific hardware maintenance training, spare parts and audit procedures.
Deployment	Involve local Samoan technical resources in the Supplier teams, including as subcontractors who may later join SBS. These local resources assist during installation and through the first months of operation, and they are the continuity when the Supplier foreign staff are absent.
Testing	Involve the Purchaser team in writing the test books. The tests are executed by SBS operators, observed and recorded by SBS, with the Supplier accompanying and explaining.
Pilot and go live	Complete a minimum transfer on operations and troubleshooting before go live. The credibility exposed at go live is that of the administration, not that of the Supplier.
Data migration	Train SBS on the data models and the extraction procedures of the Supplier own systems, including the biometric engine and the card personalisation software, so that SBS can extract its own data and migrate away in the future.
Reversibility	Execute the reversibility plan. Hand over recordings, manuals and documentation. Refresh the training for the team, or the third party, that will take over. Confirm every transfer activity has been completed.
Contract end and after	Deliver the acceptance evidence for every transfer activity, including the recurring maintenance procedures: daily maintenance, supervision, incident response, hardware security module key ceremonies, licence and certificate renewals, audits, backups and disaster recovery drills. Identify the services that must remain outsourced, and propose the transfer of local resources to SBS or to local subcontractors.

9. Relying party use cases and pilot

Real integrations as the graduation exercise: SBS staff onboard relying parties under accompaniment, then alone.

ID	Requirement
SAM-TRF-025	At least five relying party use cases shall be developed jointly with the Purchaser's staff during implementation, so that SBS staff have handled real integrations before the Supplier leaves and can continue onboarding relying parties independently afterwards. These use cases are part of the contract scope and price.
SAM-TRF-026	The Supplier shall run a pilot period of around six months, during which an initial group of three to five relying parties is integrated and operated on the platform, with SBS staff performing the onboarding steps under Supplier accompaniment. [Exact duration and window: see the Implementation Schedule, VII.2]
SAM-TRF-027	By the end of the pilot, the relying party onboarding process (registration and contract, service plan, certification, monitoring, billing configuration) shall have been executed end to end by SBS staff without Supplier hands on involvement, as part of the scored transfer assessment.

10. Scope expected per module

Module by module, the depth of competency SBS teams must reach.

ID	Requirement
SAM-TRF-028	The Supplier shall carry the skills transfer down to the module level, not as a general promise. For each module of the System, the Supplier shall propose the depth of ownership target on the scale of clause 4, the training and on the job transfer needed to reach it, and the assessment that verifies it. The table below is the minimum ambition per module: it is the floor, not the ceiling.

Module	Capacity building scope expected (minimum)
Reference registries	Full ownership. SBS owns the population register and the civil registration database outright, and can search, update and manage records over their lifecycle, so the national data is retained even if a system changes later.
Civil registration system	Own and be trained on the source code, so SBS can operate the civil registration system and evolve it after handover.
Business processes and orchestration	Own and maintain the business workflows on the open orchestration engine, so processes evolve over time, for example a new branch or a diaspora process, without calling a vendor.
Unique identifier generator	Own and maintain the standalone unique number generator (SDIN generator, SAM-IDM-022), delivered with its full source code and documentation, since it is the core key of the whole system.
Card issuance and printing	Build local capacity for card personalisation and printing operations, on a transition model where the supplier trains and supervises before production passes to local teams.
Digital system hosting	Build local capacity to host and operate the system, including the infrastructure, the supervision and the recurring maintenance.
Relying party management	Own and maintain the relying party management application, because that is where the sustainability and fee model lives.
Identity verification and credentials	Operate and monitor the verification services and credential issuance, with the opportunity to use open source bricks where they serve ownership.

ID	Requirement
SAM-TRF-029	Card production: the transfer shall reach **complete autonomy of the Apia production site** and, where the Salelologa production line option (SAM-CRD-076) is exercised, **of both sites, each able to operate autonomously**, following a transition model proven in comparable national programmes, where the Supplier trains and supervises before card production passes to the local teams: Supplier operated with SBS observing, then SBS operated under Supplier supervision, then SBS operated alone with the Supplier on call. Autonomy of each commissioned production site is verified in the scored transfer assessment.
SAM-TRF-030	Civil registration: the transfer shall cover the operation of the CRVS component and its source code (per the module table above), so that SBS runs civil registration as a core business process with no external party needed.
SAM-TRF-031	Hosting and operations: the transfer shall cover the operation of the infrastructure on the two sites (SBS server room and Vodafone data centre), including supervision, backups, disaster recovery drills with role swap between sites, and the hardware security module key ceremonies and renewals.
SAM-TRF-032	The capacity building effort concentrates where sustainability is won: printing operations, digital system hosting, business flow maintenance and evolution, and the maintenance of the source code of the tailored components. The secure core, such as the biometric matching engine, is operated and supported rather than owned to code depth, which is an acceptable and deliberate exception.

11. Assessment and link to payment

The scored assessment that verifies the transfer, with remediation and the link to payment.

ID	Requirement
SAM-TRF-033	The execution of the skills transfer shall be verified by a scored assessment against a published grid, covering at minimum: the depth reached per module against the agreed targets, the practical deployment criterion of SAM-TRF-023, the autonomy of the card production sites (SAM-TRF-029), the relying party onboarding autonomy (SAM-TRF-027), the completeness of the knowledge base, and the assessed competency of the named Purchaser staff. The detailed scored grid (criteria, weights, expected evidence) is set out in the SCC (Section IX, annex to the SCC, §4).
SAM-TRF-034	A share of the contract price, indicatively ten per cent, is held back and released against the scored assessment of the transfer, with a defined pass threshold and a

	remediation window before the holdback is lost. The mechanism, the percentage, the threshold and the assessor are defined in the SCC (Section IX).
SAM-TRF-035	Where the assessment falls below the pass threshold, the Supplier shall execute a remediation plan at its own cost within the remediation window, followed by a reassessment, before any release of the holdback.

12. Exit management and reversibility

The final proof of autonomy: an exit that Samoa can execute, documented and rehearsed.

ID	Requirement
SAM-TRF-036	The skills transfer is the operational substance of exit management: the reversibility plan per work lot (SAM-TRF-009) shall demonstrate how SBS, or a third party designated by SBS, takes over each lot at contract end without service interruption.
SAM-TRF-037	At the reversibility milestone the Supplier shall execute the reversibility plan, hand over all recordings, manuals and documentation, refresh the training for the team or third party that takes over, and confirm that every transfer activity has been completed.
SAM-TRF-038	The Supplier shall deliver the data extraction capability of SAM-TRF-024 (data migration milestone) as a tested, documented procedure, executed at least once by SBS staff, covering all data including the biometric data and the card personalisation data, in open or documented formats.
SAM-TRF-039	At contract end the Supplier shall deliver the acceptance evidence for every transfer activity, identify the services that must remain outsourced with the reasons, and propose the transfer of the local resources involved (SAM-SVC-040) to SBS or to local subcontractors.
SAM-TRF-040	No proprietary element (format, tool, procedure or dependency) shall prevent the Purchaser from exercising the reversibility of a lot. Any residual dependency shall be listed in the reversibility plan with its mitigation, consistent with the justification obligation of SAM-TRF-015.

D. Technology Specifications, Supply and Install Items (Enrolment kits and central enrolment services, SAM-ENR-071 to 144)

1. Kit composition and functions

What each enrolment kit contains and does: the capture devices, the processing unit and the accessories that condition capture quality in the field.

ID	Requirement
SAM-ENR-071	The Supplier's proposal shall describe in detail the design and the physical, technical and functional characteristics of all enrolment equipment, including 3D visuals of the physical organisation of the kits (photographs of prototypes are encouraged), an explanation of the internal layout and its use in each situation (storage, transport, set up, operations, locked overnight charging, maintenance), and the technical datasheets of all internal components.
SAM-ENR-072	The Supplier shall deliver two types of enrolment equipment: (a) fifty (50) portable enrolment kits in a case format ("enrolment kits"), used both in fixed enrolment sites and for mobile deployments; and (b) ten (10) ultra mobile rugged tablets ("enrolment tablets") for outreach to remote communities. Both types shall run the same enrolment software and produce identical enrolment packages with identical metadata. The two equipment types are complementary by design: the tablets capture the same full data set as the kits and suit door to door outreach and constrained sites (hospitals, places of detention, remote communities) for smaller groups, while the kits require site setup but deliver a higher sustained throughput and controlled capture conditions in organised sessions. The fleet composition reflects this operating model.
SAM-ENR-073	Each enrolment kit shall be a single integrated case containing all equipment needed for enrolment: fixed elements secured to the case, external accessories removable, and consumables, wear parts and batteries demountable. All components shall be integrated with no loose cables and shall be operable from inside the case. Accessories shall be held immobile during transport and the complete kit, including all accessories, shall close and travel as one unit.
SAM-ENR-074	The processing unit of each enrolment kit shall be a laptop computer with a screen of at least 14 inches and an English (QWERTY) keyboard, with at minimum a mid range professional processor (Intel Core i5 class or equivalent), 16 GB of RAM and 1 TB of SSD storage, running a currently supported version of Windows (version 11 minimum), or an equivalent desktop operating system, with endpoint protection, the Proposer showing compatibility with the enrolment software and a support horizon covering the Contract period, and a Bluetooth mouse (with a spare battery) for comfortable operator input. Local storage shall be sized to retain the encrypted enrolment packages of several days of operations. The laptops shall be delivered with warranty and spare parts arrangements stated in the proposal, chargers fitted with the Samoa plug type on 220 to 240 V supply, and an operating system edition whose support horizon covers the contract period, the hardware support horizon being aligned with the operating system end of life.
SAM-ENR-075	Each enrolment kit shall include an optical tenprint fingerprint scanner of type FAP60 minimum (larger capture classes are welcome), certified against FBI PIV / EBTS Appendix F image quality specifications, capturing four fingers, then four fingers, then two thumbs. The proposal shall describe the cleaning, upkeep and hygiene arrangements for this sensor. Fingerprint data format, storage and exchange shall follow ISO/IEC 39794-4 (preferred) with read compatibility with ISO/IEC 19794-4, per SAM-ENR-135.
SAM-ENR-076	Each enrolment kit shall include a fixed, quickly adjustable camera of at least 10 megapixels with an integrated LED ring light, able to produce ICAO compliant facial images without any external light source. The kit shall carry all accessories needed to condition the capture environment, including a uniform background (either a foldable popup background panel with its support, or a photo backdrop cloth with eyelets), fitting inside the kit or a companion backpack for transport; the final backdrop design will be selected during the design phase. Portrait capture shall comply with the latest ICAO Doc 9303 portrait guidance, with image data formats per SAM-ENR-135.
SAM-ENR-077	Each enrolment kit shall include a document scanner able to scan supporting documents up to A4 format at a minimum of 5 megapixels and an optical resolution of at least 300 dpi, higher resolutions being welcome.

SAM-ENR-078	Both equipment types shall provide a dedicated means to capture, store and digitise the handwritten signature of the enrolled person (a signature pad housed in the enrolment kit, consistent with SAM-ENR-079; the touch screen for the tablet) for later printing on the identity card.
SAM-ENR-079	Both equipment types shall embed a GPS receiver recording the location of each enrolment, WiFi connectivity, and mobile data connectivity (4G or better, with fallback to 3G/2G where coverage requires): for the laptop based kits through a USB 4G dongle (locally procurable) with a dedicated housing space in the kit, and for the tablets through an integrated SIM slot.
SAM-ENR-080	Both equipment types shall allow the operator to capture the biographic data of a person (with preloading of biographic records from the existing digital CRVS, as specified in the functional requirements), to scan supporting documents, and to record the consent of the person as specified in SAM-ENR-019.
SAM-ENR-081	Both equipment types shall capture the facial portrait, the ten fingerprints and the signature of the enrolled person. Iris capture is not required. No biometric data shall be captured from persons under 18 years of age; the enrolment software shall enforce this rule based on the declared or preloaded date of birth.
SAM-ENR-082	At the end of each enrolment, the equipment shall produce an enrolment receipt bearing the provisional SDIN bound to the application, clearly marked as provisional (pending verification), and the application reference number, per SAM-ENR-041 to 043, to be scanned into the enrolment package and handed to the individual. The application reference shall be unique across the country and shall support later retrieval of the enrolment status. The receipt shall be printed on the spot by a compact thermal printer (58 mm class): integrated in or connected to the kit, and connected by Bluetooth for the tablets, the printer and its consumables being part of each unit's inventory.
SAM-ENR-083	The enrolment kit shall allow the operator and the enrolled person to be seated around a table, in an L shape or face to face; the enrolment tablet shall allow enrolment with both persons standing or seated face to face, without any table.
SAM-ENR-084	Every enrolment unit shall operate offline by default: full enrolment capability shall be available with no network connection, and data collected offline shall be structured in the same format as data transmitted online.

2. Ruggedness, power and environment

Samoan field conditions drive these requirements: heat, humidity, transport and unstable power, with autonomy for full working sessions.

ID	Requirement
SAM-ENR-085	All enrolment equipment shall withstand a drop from a height of 1 metre.
SAM-ENR-086	The enrolment kit cases shall be certified IP67 minimum and shall be robust to frequent handling, in particular repeated opening and closing; the design shall avoid parts that wear through friction or torsion. The cases shall protect the equipment during transport on rough roads and on inter island ferries.
SAM-ENR-087	Each enrolment kit shall weigh no more than 15 kg fully packed (a lower weight is preferred) and shall be fitted with a carrying handle.
SAM-ENR-088	Setting up or packing an enrolment kit shall take less than 5 minutes. The only site prerequisites shall be a table and two chairs: everything else needed for good enrolment conditions (light, uniform background, power) shall be provided by the kit itself. No equipment shall need to be plugged or unplugged for daily use, and all connections shall be firm enough to prevent accidental disconnection.
SAM-ENR-089	All enrolment equipment shall operate with full autonomy, without mains power, for at least one full field day of 8 hours of continuous enrolment operations.
SAM-ENR-090	Each enrolment kit shall be rechargeable through a sealed external socket while closed and locked, and shall be protected against power surges. Where a stable mains supply is available the kit may be powered directly from the mains without being opened.
SAM-ENR-091	The internal power system of the equipment shall be rechargeable from the mains, from a generator or from solar panels. External sources shall charge the internal power system, not the peripherals directly, so as to isolate the equipment from unstable supply. Where solar panels are used, they shall be delivered with the matching inverter or charge regulator, and the bidder shall describe the connection arrangement, consistent with SAM-ENR-092 and SAM-ENR-093.

SAM-ENR-092	Each enrolment unit shall be delivered with one power bank (or equivalent energy storage) sized, together with the internal battery of the unit, to sustain two days of operations, itself rechargeable from mains, generator or solar panels and transportable with the equipment. No second internal battery is required. Indicators visible from outside the closed kit, and by the operator when the kit is open, shall show the charging state and battery level.
SAM-ENR-093	The Supplier shall price, as an option, solar recharge sets for the outreach teams (indicative quantity: ten to twelve (10 to 12) sets), each able to recharge the power bank during field operations, offering a good compromise between power output and transportability, and carried with or attached to the equipment. The power bank of SAM-ENR-092 remains delivered with every unit; solar sets are not required per kit.
SAM-ENR-094	All equipment shall be specified for continuous operation in a humid tropical maritime climate (high temperature, high humidity, salt laden air) and for regular transport by road and by ferry between Upolu and Savai'i, including protection against rain and sea spray during loading and unloading.
SAM-ENR-095	Closed kits shall be stackable on at least 3 or 4 levels, shall tolerate storage in any position without damage, and shall allow connection to power for battery upkeep while stored. The Supplier shall provide stacking and palletisation recommendations for safe storage and transport on standard pallets.

3. Ultra mobile tablets

The outreach complement to the kits: same data, same quality standards, packaged for door to door and constrained sites.

ID	Requirement
SAM-ENR-096	Each enrolment tablet shall be a compact all in one rugged Android tablet (Android version 15 minimum, or the latest long term supported Android version available on rugged tablets at the time of delivery), or an equivalent rugged tablet and mobile operating system, the Proposer showing the same sensor support, security updates and a support horizon covering the Contract period, with a screen of at least 8 inches used in portrait mode for comfortable form entry. It shall include all sensors needed to capture biometrics, scan documents and enter data, and shall require no cable connection to any other equipment during use, so that one person can operate it hand held.
SAM-ENR-097	The enrolment tablet shall include a fingerprint scanner of type FAP60 minimum, certified against FBI PIV / EBTS Appendix F image quality specifications, capturing four fingers, then four fingers, then two thumbs. The proposal shall describe the cleaning, upkeep and hygiene arrangements for this sensor. Fingerprint data format, storage and exchange shall follow ISO/IEC 39794-4 (preferred) with read compatibility with ISO/IEC 19794-4, per SAM-ENR-135.
SAM-ENR-098	The rear camera of the enrolment tablet shall serve for both portrait capture and document scanning: at least 16 megapixels, with autofocus and an LED flash, producing sharp ICAO compliant portraits and legible document scans. Portraits shall meet the ICAO inter eye distance of at least 240 pixels per ISO/IEC 39794-5:2020, consistent with SAM-IDM-098.
SAM-ENR-099	The enrolment tablet shall be rated at least IP65 and shall have passed MIL-STD-810H testing, with evidence of the applicable drop, vibration, humidity, water and temperature test reports and certifications. Its battery shall sustain at least 8 hours of operations in total, with the support of one additional power bank (SAM-ENR-092).
SAM-ENR-100	Each enrolment tablet shall be delivered with a soft, waterproof carrying bag comfortable enough to be carried for hours on foot, holding the tablet and all its accessories, including the Bluetooth receipt printer of SAM-ENR-082 and, where that option is selected, the photo backdrop cloth of SAM-ENR-076. The tablet shall require no set up time (take it out of the bag and switch it on) and no site prerequisites of any kind.

4. Central enrolment services

The central services behind the fleet: package reception, fleet management, SDIN pool provisioning and remote deactivation.

ID	Requirement

SAM-ENR-101	The Supplier shall deliver a central enrolment service that receives signed enrolment packages directly from the enrolment kits and tablets over the mobile data network or any available Internet connection, through a mutually authenticated VPN. Kits shall queue packages locally while offline and synchronise automatically as soon as connectivity is available (store and forward). Given the geography of Samoa, no intermediate regional server tier is required.
SAM-ENR-102	The central enrolment service shall verify the integrity and authenticity of every package received by checking its cryptographic signature, and shall reject and flag any package that fails verification.
SAM-ENR-103	Every enrolment unit shall be registered with the central enrolment service before use, and may be deactivated temporarily or permanently. Packages produced by a unit during a deactivation period shall be rejected by the central service, and accepted again after reactivation.
SAM-ENR-104	Every enrolment operator shall be registered with the central enrolment service, and may be deactivated temporarily or permanently. Packages produced by an operator during a deactivation period shall be rejected by the central service.
SAM-ENR-105	The central enrolment service shall track the processing status of every enrolment package end to end and make it available to authorised field and supervision staff by application reference (for example: pending transmission, received, transmission error, rejected (incorrect format or data), submitted to IDMS, rejected by IDMS, identity activated, under investigation, potential duplicate). Statuses and the associated operator guidance shall be configurable and updated centrally. The final status list shall be agreed with the IDMS block.
SAM-ENR-106	The central enrolment service shall store the statistical data of all enrolments for performance analysis of the campaign, including at least: date and time, total duration and duration of each step, measured biometric quality, capture incidents, enrolment unit, operator, team, site and GPS location.
SAM-ENR-107	A business intelligence and monitoring capability shall be deployed over these statistics, with dashboards, reports and threshold based alerts supporting the monitoring of operations and the evaluation of the agreed service levels, allowing degradations or losses of service to be anticipated and identified.
SAM-ENR-108	The central enrolment service shall prepare and load onto the enrolment units, before deployment and at each resupply, preload extracts of biographic records from the authoritative CRVS source designated in VII.1.2.6 (the legacy system, then the stock database once commissioned, per SAM-CRV-034), under access controls and encryption approved by the Purchaser. The preload shall also include the reserved SDIN pool of each unit, provisioned per SAM-ENR-140 to 143: SDINs are pre generated centrally by the standalone unique number generator (SAM-IDM-022), bound provisionally at capture, and activated only after biometric deduplication (SAM-IDM-026); the CRVS biographic preload of this requirement is unchanged by the pool mechanism. Preloaded data no longer needed shall be securely erased from the units, with erasure confirmations collected centrally as specified in SAM-IDM-051.
SAM-ENR-109	Each enrolment unit shall retain its encrypted enrolment packages locally for several days of operations. As a fallback for areas with no usable coverage, packages shall be exportable to encrypted removable media (SD card or equivalent), and the central enrolment service shall provide a controlled facility to ingest packages from such media with the same integrity checks as network transfers.
SAM-ENR-110	The enrolment system shall transmit validated enrolment packages to the IDMS through the exchange protocol agreed in joint technical workshops with the IDMS supplier under the technical governance of the Purchaser, including the registration of stations and operators with the IDMS and the management of the signature and encryption secrets used for enrolment data.
SAM-ENR-111	As the enrolment platform and the IDMS are delivered under a single turnkey contract, enrolment packages shall flow directly from the enrolment units into the IDMS reception chain (SAM-IDM-075), without a separate central temporary storage layer. The residual central enrolment services (fleet management and supervision, reserved SDIN pool provisioning per SAM-ENR-140 to 144, remote deactivation) shall be hosted on the shared platform infrastructure of the ICT Infrastructure block, and the Supplier's offer shall include all hardware and software needed for them, with a justification of the proposed sizing. Software licences for infrastructure components shall cover at least 3 years.

5. Deployment, installation and logistics

Getting the fleet operational across the islands: delivery, installation, site setup and the logistics of moving equipment safely.

ID	Requirement
SAM-ENR-112	The Supplier shall assemble the kits at the place of manufacture and avoid final assembly in Samoa as far as possible.
SAM-ENR-113	In Samoa, the Supplier shall install the software, load the CRVS preload extracts and the cryptographic secrets (keys and certificates provided by the Purchaser) on each unit, and commission the system under the supervision of the Purchaser. Every kit and tablet shall pass a central functional test before field deployment.
SAM-ENR-114	All equipment shall be delivered palletised to the Purchaser's designated site in Apia, with packing lists and stacking recommendations.
SAM-ENR-115	The Supplier shall produce a deployment plan, validated by the Purchaser, covering the distribution of the 50 kits and the 10 tablets to approximately 24 field teams across Upolu and Savai'i, including road and ferry transport arrangements, charging and storage points, and the rotation of equipment between fixed sites and outreach operations.
SAM-ENR-116	The Supplier shall deliver a full documentation set in English (first use guide, user guide for the kit and its software, installation and update guide, administrator guide, upkeep and maintenance guide), plus laminated quick reference sheets kept inside each kit (with key content also available in Samoan) and video tutorials loaded on the equipment for operator self training, diagnostics and maintenance. Operating procedures shall be explained in both the documentation and the training.
SAM-ENR-117	The Supplier shall train trainers who will in turn train the enrolment operators, shall deliver all training content in editable format to the Purchaser, and shall remain available to retrain or train new operators as needed. The detailed training and skills transfer requirements are specified in the capacity building block of this RFP (cross reference; not developed here).
SAM-ENR-118	Enrolment operations will be run by Government teams. The Supplier shall deliver a turnkey platform and remain responsible for support and maintenance of the system and equipment throughout the Contract, and shall monitor the performance and data quality of enrolment through package metadata (daily enrolment counts, durations by step, biographic, biometric and scan quality, exception rates), reporting any anomaly against the agreed service levels to the Purchaser, globally and per operator and site.

6. Spares, maintenance and test environment

Keeping the fleet alive: spares strategy, maintenance arrangements and the reference units for the test environment.

ID	Requirement
SAM-ENR-119	All delivered equipment shall be supported and maintained by the Supplier for the duration of the Contract, including fault investigation, repairs, part replacement and software updates. The Supplier shall hold in Samoa a stock of spare parts sufficient to keep the fleet operational. The 50 kit fleet is sized above the simultaneous field deployment of approximately 24 teams; replacement capacity for defective units is provided by this fleet slack, and no separate pool of complete spare kits is required.
SAM-ENR-120	Consumables shall be exchangeable rapidly, within a defined switchover time stated by the Supplier in its proposal, without tools and without stopping the unit; wear parts (hinges, straps and similar) shall be accessible and replaceable in the field without unscrewing or dismantling the kit. Internal batteries of the units are not required to be field replaceable (battery replacement by a technician is acceptable); the power bank is the field replaceable energy element (SAM-ENR-092). Field replaceable peripherals (camera, scanners) shall be repairable on site, and each kit shall carry the tools needed for these operations.
SAM-ENR-121	Repairs shall be organised on two levels: field repairs, following documented procedures taught in training (symptom, confirmation, impact assessment, immediate workaround, definitive fix); and workshop repairs at a central repair point in Samoa operated by the Supplier or its partner. Equipment that cannot be repaired at either level shall be taken back and exchanged under warranty where applicable.

SAM-ENR-122	A preventive maintenance guide shall cover cleaning and upkeep, consumables to change regularly, preferred storage and transport conditions, battery life good practice, and the audit procedures used to assess the condition of each kit and trigger preventive repairs.
SAM-ENR-123	Software and per unit configurations shall be loadable remotely (including in bulk over a local WiFi provisioning server) and updatable in the field from portable media without returning the units, through a secure protocol guaranteeing the integrity and authenticity of every update.
SAM-ENR-124	A diagnostic tool on each unit shall collect information on installed software (versions, status, deployment history), peripheral health, battery condition and usage statistics (number of enrolments, scans, power cycles), and report it to the central enrolment service.
SAM-ENR-125	In addition to the operational fleet, the Supplier shall deliver one enrolment kit and one enrolment tablet, fully operational and integrated with the IDMS test environment, for the Purchaser's test and integration environment.

7. Security of the enrolment platform

The security of the capture chain end to end: hardened devices, encrypted data from capture, and controlled software deployment.

ID	Requirement
SAM-ENR-126	Every operator shall authenticate individually both on the operating system of the equipment and in the enrolment application before any enrolment operation.
SAM-ENR-127	Biometric and biographic data shall be encrypted and signed at the point of capture, protecting against data injection and against theft or alteration of enrolment data by a man in the middle at any point between the sensor and the central enrolment service.
SAM-ENR-128	Once an enrolment is completed, the data stored on the unit shall be unmodifiable by design.
SAM-ENR-129	All local storage on laptops and tablets shall be fully encrypted, and the platform shall support the remote blocking and remote wiping of a lost or stolen unit, in combination with its deactivation at the central enrolment service.
SAM-ENR-130	Each kit shall be fitted with a key lock (two sets of keys delivered) and with an anti theft device allowing the kit to be secured to a fixed object.
SAM-ENR-131	The enrolment platform shall implement confidentiality, integrity and availability controls together with non repudiation and authentication, minimise its attack surface, and keep complete audit trails of all security relevant events. The Supplier shall notify the Purchaser immediately of any security breach, preserve the evidence and cooperate with any investigation.
SAM-ENR-132	The enrolment software (kit applications and central services) shall pass security testing covering at least the OWASP Top 10 vulnerabilities before deployment and after each major release, consistent with the umbrella security testing requirements of VII.1.6 and SAM-TST-011, which prevail where more demanding. The security testing report of each release shall state the testing scheme applied and the qualifications of the testing party; no formal product certification is required beyond the umbrella requirements of VII.1.6.
SAM-ENR-133	The processing of personal data by the enrolment platform shall comply with the applicable data protection provisions of the laws of Samoa, including the NDID Act, and with the privacy principles agreed for the NDIDS programme.

8. Standards

The biometric and data standards the capture chain must meet, aligned on the ISO 39794 family with read compatibility with 19794.

ID	Requirement
SAM-ENR-134	All fingerprint scanners shall be certified against the FBI PIV / EBTS Appendix F image quality specifications for their FAP class, with FAP60 as the minimum class for both kits and tablets (larger capture classes are welcome). No specific make or brand is required or accepted as a specification.
SAM-ENR-135	Captured biometric data shall conform to open international standards: facial images to ISO/IEC 39794-5:2020 (preferred), with read compatibility with ISO/IEC 19794-

	5, and ICAO portrait quality requirements; fingerprint images to ISO/IEC 39794-4 (preferred), with read compatibility with ISO/IEC 19794-4, and standard compression (WSQ or JPEG 2000), consistent with SAM-ENR-033. Systems relying on ICAO standards must read ISO/IEC 39794-5 by 1 January 2026 and complete the switch by 1 January 2030; the delivered System shall meet this migration path from the outset.
SAM-ENR-136	The enrolment package format shall be fully documented and based on open standards, so that packages can be processed by the IDMS and by any future system without dependence on the Supplier (no vendor lock in).
SAM-ENR-137	The central enrolment services shall follow a service oriented, multi tier architecture. Their components shall satisfy the transverse rule of SAM-IDM-137: open source, or proprietary with full source code delivered, or packaged software specific to the System covered by the escrow arrangement of SCC GCC 15.5. Standard Software widely available on the market, such as operating systems and database management systems, is treated as stated in SAM-IDM-137. The governing test is the Purchaser's ability to operate, modify and replace them without dependence on the Supplier, not the licensing model as such. The system shall use PostgreSQL or another open source database, or an equivalent database, the Proposer showing that the Purchaser can export and reuse the data and schema without licence dependence and that its support covers the Contract period, and shall support switching between connected and disconnected modes so that field operations continue without a permanent Internet connection.
SAM-ENR-138	All licensed software delivered under this block shall follow the transverse perpetual licence rule of SAM-IDM-132. The only exception is the set of infrastructure licences of the central enrolment services covered by SAM-ENR-111 (minimum three years), as expressly motivated in SAM-IDM-132.

9. Fleet delivery commitment

The delivery lead time is contractual: bidders commit a ceiling that becomes a milestone obligation.

ID	Requirement
SAM-ENR-139	The Proposer shall state in its proposal a firm, committed ceiling on the delivery lead time for the complete enrolment fleet (kits and tablets) and for the enrolment capture application, counted from contract effectiveness. This ceiling becomes contractual at award and shall be reflected in milestone M2 of the Implementation Schedule (VII.2). The detailed delivery schedule may be refined at the end of the design phase, within the committed ceiling, which shall not be extended. The realism and firmness of this commitment are evaluated under feature B2 of Section III.

10. Reserved SDIN pool provisioning

How reserved numbers reach the kits for offline work: central generation, per unit pools and the accounting that prevents any reuse.

ID	Requirement
SAM-ENR-140	The central enrolment service shall provision each enrolment unit, before deployment and throughout operations, with a reserved pool of pre generated SDINs obtained from the standalone unique number generator (SAM-IDM-022). Each range reserved to a unit shall be recorded in the central pool register and shall never be provisioned to another unit. Pool sizes shall be configurable per unit type and per deployment profile, sized on the expected enrolment rate and the expected time between connections.
SAM-ENR-141	The System shall replenish the reserved SDIN pool of each unit online whenever connectivity is available: replenishment shall be automatic, incremental and transparent to the operator, shall not interrupt enrolment operations, and shall use the same mutually authenticated and encrypted channel as the transmission of enrolment packages (SAM-ENR-101).
SAM-ENR-142	The System shall monitor the pool level of every unit, with configurable low pool thresholds raising alerts both to the operator on the unit and to the central supervision (SAM-ENR-107), so that replenishment or unit rotation can be organised before exhaustion. The behaviour of a unit whose pool is exhausted while offline shall be

	documented, and the supervision dashboards shall report pool levels, consumption rates and replenishment history per unit.
SAM-ENR-143	The reserved SDIN pool shall be stored on the unit in encrypted, tamper evident form, cryptographically bound to the identity of the unit, so that a reserved SDIN is usable only by the unit to which it was provisioned. The pool shall be covered by the remote blocking and remote wiping functions of SAM-ENR-129; the numbers held by a lost, stolen or decommissioned unit shall be reconciled in the central pool register (returned to reserve or permanently retired, per the policy approved by the Purchaser).
SAM-ENR-144	The System shall report to the central pool register, and through it to the unique number generator, every number voided after provisional binding (duplicate found at deduplication, application rejected) and every number withdrawn from a pool. Voided numbers shall be permanently retired and shall never be assigned to any person, in accordance with sections 31(7) and 31(8) of the NDID Act 2024. The System shall produce reconciliation reporting across the full pool lifecycle: provisioned, bound, activated, voided and retired, returned to reserve.
SAM-ENR-145	The enrolment fleet (kit laptops and tablets) shall be managed through a mobile device management (MDM) or unified endpoint management solution providing at minimum: device inventory and health monitoring, enforcement of the encryption and security policies, remote lock and remote wipe of lost or stolen units (in combination with SAM-ENR-129), and protection of locally stored secrets, including the reserved SDIN pools of SAM-ENR-143, in a secure vault; the revocation of the pool of a lost or stolen unit shall be triggered together with its deactivation at the central enrolment service.

D. (continued) ICT Infrastructure component (SAM-INF-001 to 048)

Component note. The ICT Infrastructure component groups everything the System runs on: hosting and compute on the two national sites, networks, power protection, the central supervision and monitoring platform, and the PKI trust services consumed by every other component. Architecture principles remain in VII.1.3 (SAM-ARC-012 to 026); this component is their supply and delivery counterpart.

1. Component scope, hosting and compute

The infrastructure footprint on the national sites: compute, storage and virtualisation for every subsystem, allocated between Supplier scope and Purchaser prerequisites.

ID	Requirement
SAM-INF-001	The Supplier shall deliver, install and commission the ICT Infrastructure component: hosting and compute infrastructure on the two national sites (SBS server room as primary, Vodafone data centre as disaster recovery site), networks, power protection, the central supervision and monitoring platform, and the PKI trust services, together with the related installation, migration and commissioning services.
SAM-INF-002	The hosting infrastructure shall support all System components (enrolment central services, IDMS, ABIS, IDVS, CRVS, card personalisation chain, PKI, monitoring) with the separations required by VII.1.3 and by section 38(4) of the NDID Act 2024.
SAM-INF-003	Compute and storage shall be virtualised on a platform manageable by SBS, sized per VII.1.5 with the headroom defined there. The infrastructure shall support the primary and DR role swap of SAM-CYB-020 for the IDVS layer without redesign; for the IDMS, the ABIS, the CRVS and the supporting tooling, the DR site shall carry active/passive compute and storage capacity sized to the RTO/RPO of SAM-CYB-021, with a documented restore path (SAM-ARC-021).
SAM-INF-004	The Supplier shall perform a site survey of both sites within weeks of contract effectiveness, covering space, power, cooling, physical security and cabling, and shall identify the adequacy works required at the SBS server room. The survey report allocates each work item to the Supplier scope or to the Purchaser prerequisites per the inventory tables.
SAM-INF-005	Backup infrastructure (hardware and software) shall be delivered on both sites, supporting the backup and restoration requirements of VII.1.4.
SAM-INF-006	Racks, cabling, KVM and physical access accessories shall be included for both sites, reusing the existing rack capacity at the SBS server room identified in the Background materials.
SAM-INF-007	The infrastructure shall be delivered with its full configuration documented as code or as exportable configuration files, held in the Purchaser's repository, so that SBS can rebuild any environment.
SAM-INF-008	Development, test, pre production and production environments shall be provided per VII.1.4 (SAM-ADM-028); non production environments may share hardware but never production data unless anonymised. The pre production environment shall be functionally representative of production; performance representative sizing for load test campaigns is achieved by temporary reallocation of production class resources, not by a permanent duplicate stack.

2. Network

The connectivity inside and between sites, and toward the relying parties, with security zoning per the architecture chapter.

ID	Requirement
SAM-INF-012	The Supplier shall deliver the local networks of both hosting sites, including switching, routing, firewalls and load balancing, implementing the network segmentation required by SAM-CYB-030 (enrolment, IDMS, ABIS and biometric store, IDVS, CRVS, administration and monitoring zones).
SAM-INF-013	The Supplier shall specify the inter site connectivity requirements (bandwidth, latency, redundancy, encryption) between the SBS server room and the Vodafone

	data centre, and shall integrate with the links contracted by the Purchaser. The links themselves are a Purchaser prerequisite unless priced as an option.
SAM-INF-014	Network equipment shall be delivered for the card personalisation premises (Apia and Salelologa), the adjudication and investigation offices and the supervision cell, connecting them securely to the central services.
SAM-INF-015	All inter site and external traffic shall be encrypted in transit; site to site VPN termination and certificate based device authentication shall use the PKI trust services of this component.
SAM-INF-016	Network management shall be integrated into the central monitoring platform (SAM-INF-030), with configuration backup and change tracking for every network device.

3. Power protection

Clean continuous power for the platform: UPS in Supplier scope, standby generation per the inventory allocation.

ID	Requirement
SAM-INF-020	The Supplier shall supply, install and commission UPS protection at the primary site (and complement the DR site where the survey identifies a gap), sized from the site survey with a capacity headroom of at least thirty (30) percent, covering at minimum: the controlled shutdown of all components, and the protection of cryptographic modules against uncontrolled power loss (HSM zeroisation risk).
SAM-INF-021	UPS autonomy shall bridge the start of the standby generation where present, and otherwise sustain a documented graceful shutdown sequence. Autonomy targets: at least fifteen (15) minutes at full load where standby generation is present, and at least sixty (60) minutes where it is not, in both cases sufficient to complete the documented graceful shutdown sequence.
SAM-INF-022	**Generator boundary**: the supply of any standby generator is outside the Supplier scope (Purchaser prerequisite, triggered if the site survey concludes it is necessary). The Supplier shall specify the generator requirements (capacity, transfer switching, fuel autonomy), integrate the delivered generator into the power chain, and monitor it through the central monitoring platform.
SAM-INF-023	Environmental monitoring (temperature, humidity, water, smoke, door contacts, power quality) shall be installed in both server rooms and in the personalisation premises, integrated into the central monitoring platform with alerting.
SAM-INF-024	The complete power chain (mains, UPS, generator where present, distribution) shall be documented, with tested shutdown and restart procedures handed over to SBS as part of skills transfer.

4. Central supervision and monitoring platform

The single pane from which SBS operates the whole platform, technical and business views together.

ID	Requirement
SAM-INF-030	The Supplier shall deliver a **single central supervision and monitoring platform covering the entire System**: infrastructure (compute, storage, network, power, environment), applications (enrolment central services, IDMS, ABIS, IDVS, **CRVS**, card personalisation chain, PKI) and services (APIs, interfaces, queues), on both sites. One converged, open source based platform may also serve the security monitoring of SAM-CYB-010, under the conditions of SAM-INF-034.
SAM-INF-031	The platform shall provide dashboards for the SBS supervision cell (site S2), role based views (operations, management, security liaison), and configurable alerting (thresholds, escalation chains, notification channels).
SAM-INF-032	The platform is the **authoritative measurement tool of the service levels of part F**: it computes the SLA indicators automatically, produces the monthly reports and gives SBS direct access to the raw measurements, as required by SAM-SLA-001.
SAM-INF-033	The enrolment kit fleet management data (kit status, synchronisation, incidents, from the enrolment platform) shall feed the central monitoring platform, which remains the single operational picture; fleet management itself stays within the enrolment component.

SAM-INF-034	The platform shall expose its events to the security logging and monitoring chain of VII.1.6 (SIEM) without duplicating it: operational monitoring and security monitoring are distinct consumers of the same instrumented sources. They may be served by one converged, open source based platform, provided the security views, their retention and their integrity cannot be degraded or altered by operations roles (SAM-CYB-010, SAM-ADM-016).
SAM-INF-035	The platform shall keep a history of measurements sufficient for capacity management (VII.1.4) and for the annual SLA recalibration (SAM-SLA-020); retention of any personal data in monitoring events shall follow the legal block.
SAM-INF-036	The platform shall be operable by SBS at the end of skills transfer (administration, new probes, new dashboards) without Supplier intervention, and is covered by the transfer evaluation grid (operations criterion).
SAM-INF-037	The platform shall be built on established products with the licensing, reversibility and source or escrow obligations of the Contract; an open source based platform is acceptable and welcome.

5. PKI and trust services

The hardware and services of the national trust chain: HSM custody, signing services and their availability obligations.

ID	Requirement
SAM-INF-040	The Supplier shall deliver the **PKI of the NDIDS**: an offline root CA and an online issuing CA, with keys generated and held in HSMs certified FIPS 140-3 Level 3 or equivalent, owned and controlled by SBS, hosted on the national sites. The HSM footprint is consolidated: **one operational resilient HSM pair** serving the issuing CA and all issuance, card and credential signing needs of the System, plus **one root CA HSM device** with a dual control backup (backup token set); no separate HSM silo per component or per site is required.
SAM-INF-041	The PKI shall expose **signature and encryption services through documented APIs to every component of the System**, covering at minimum: signing of the card QR code content; issuance and sealing of verifiable credentials (OpenID4VCI chain); sealing of CRVS certificates, attestations and PDF documents (PDF 2.0, ISO 32000-2, with PAdES conformant signatures); signing of enrolment packets and device authentication; internal TLS certificates. A timestamping authority is not part of the mandatory service list (the offline QR model does not use it); it is noted as a possible Version 2 extension of the PKI.
SAM-INF-042	**No component shall implement its own isolated cryptographic silo**: every signing, sealing and certificate need of the System shall consume the PKI trust services, so that one national trust chain covers the card, the digital credentials and the CRVS documents (SAM-ARC-016).
SAM-INF-043	The PKI shall provide validation services (OCSP and CRL) reachable by online verifiers and suitable for the offline verification model of the signed QR code content (long lived signing keys, published trust anchors).
SAM-INF-044	Key lifecycle management shall be delivered: generation ceremonies under dual control with documented scripts, rotation, revocation, backup and recovery of key material, all executed with SBS staff and transferred to them.
SAM-INF-045	The Supplier shall deliver the Certificate Policy and Certification Practice Statement (CP/CPS), structured per IETF RFC 3647, and the ceremony documentation, as SBS property. The CP/CPS shall be assessed against that structure at acceptance.
SAM-INF-046	The PKI shall be **sized for the NDIDS but designed to be extensible** to further government uses (additional issuing CAs, additional certificate profiles) without redesign of the root of trust, in line with the open question of a government wide PKI.
SAM-INF-047	PKI operations (enrolment of subscribers, certificate issuance, revocation) shall be integrated into the central monitoring platform, and PKI security events into the VII.1.6 chain.
SAM-INF-048	The signing keys protecting long lived artefacts (cards, credentials, sealed CRVS documents) shall have, for each key pair type and usage, a documented private key usage period, a documented public key certificate validity period, and documented rollover and link certificate arrangements, so that artefacts remain verifiable for their full lifetime (10 years and beyond for cards). These periods and rules shall be stated in the CP/CPS of SAM-INF-045. Where an authority for travel documents or mobile

	driving licences is added later, the corresponding ICAO guidance on country signing and document signer key periods applies.

E. Testing and Quality Assurance Requirements

This chapter defines how quality is demonstrated before Samoa relies on the system: the test strategy including the early proof of concept phase, the Supplier's internal testing, performance, security, disaster recovery and accessibility campaigns, commissioning, and the Operational Acceptance Tests that gate the milestones. Bidders should note that acceptance is evidence based throughout: what is not demonstrated on the agreed environments with agreed data is not accepted.

4.1 Test strategy and planning

The Master Test Plan governs everything that follows, and includes the early proof of concept phase that validates critical choices before mass build.

ID	Requirement
SAM-TST-001	● The Supplier shall deliver, within eight (8) weeks of Contract effectiveness and before the start of any development or configuration activity, a Master Test Plan covering all test levels (unit, integration, system, end to end, performance, security, accessibility, disaster recovery, pre commissioning, Operational Acceptance), the test organisation and roles, the entry and exit criteria of each level, the test environments and tools, and the test calendar aligned with the Implementation Schedule (VII.2). The Master Test Plan is subject to Purchaser approval and shall be kept current throughout the Contract.
SAM-TST-029	● **The test strategy shall include an early proof of concept phase, run before the start of mass build activities: a limited scope demonstration of the end to end chain (enrolment capture, deduplication, activation, verification) on real equipment with test data, allowing SBS and the Supplier to validate the critical design choices while they are still inexpensive to change. The early POC scope and exit criteria shall be proposed in the Master Test Plan and agreed at the design stage; its findings feed the design baseline. The early POC phase appears as a milestone in the Implementation Schedule of VII.2.**
SAM-TST-030	● **Before the OAT V1 system, the Supplier shall demonstrate the full ISO/IEC 18013-5 proximity interoperability of the mobile document issued by the System, and not only its issuance: presentation from the delivered wallet (SAM-CRD-007) against at least two independent reader implementations, not supplied by the Supplier, its subcontractors or the provider of its**

	credential platform, selected with the Purchaser. The test covers device engagement, data retrieval, issuer signature validation against the published trust list, release of the requested attributes only, and status check. The results form part of the acceptance criteria of SAM-TST-019.
SAM-TST-002	● The Supplier shall maintain a requirements traceability matrix mapping every requirement of Section VII (by SAM identifier) to one or more test cases, and every test case back to its requirements. The matrix shall be delivered with each test campaign report and shall demonstrate, before each Operational Acceptance, that every requirement in the scope of the release is covered by at least one executed test.
SAM-TST-003	● The Supplier shall provide and operate dedicated, segregated test environments, drawn from the environment set of SAM-ADM-028 (development, test, pre production, production), including at least the test environment and the pre production environment used as the Purchaser facing acceptance environment, functionally representative of production (same software versions, representative data volumes, both sites simulated or exercised where relevant; performance representative sizing for load tests per SAM-ADM-028). No test activity shall take place in the production environment except the pre commissioning and commissioning tests planned under this Section.
SAM-TST-004	● All test data containing personal data shall be anonymised or synthetic. Production personal data shall not be used in test environments. Biometric test datasets used for accuracy and end to end testing shall be either synthetic, or collected with documented consent for testing purposes, and shall be destroyed at the end of the campaigns with a destruction certificate.
SAM-TST-005	● The Supplier shall automate regression testing for the core functional chains and the published APIs, and shall run the automated regression suite before every release deployed to the acceptance or production environments. The automated test assets shall be delivered in the Purchaser's repository as part of skills transfer.

4.2 Supplier internal testing

What the Supplier must have tested before presenting anything for acceptance.

ID	Requirement
SAM-TST-006	● The Supplier shall perform unit testing of all developed or configured components, with documented results, before promoting any component to integration testing.
SAM-TST-007	● The Supplier shall perform integration testing covering all interfaces between subsystems (enrolment clients, IDMS, ABIS, SDIN generation, CRVS, IDVS, card personalisation, portals) and with external systems in scope, including negative and error handling cases at every interface.
SAM-TST-008	● The Supplier shall execute and document end to end tests of the complete identity chain before each Operational Acceptance: enrolment (online and offline modes), secure packet transport, deduplication, adjudication, SDIN generation and activation, credential issuance, card personalisation and delivery, and verification of the issued identity through the IDVS (online) and through the signed QR code content (offline). The end to end campaign shall include lifecycle scenarios (correction, update, deactivation on death, token rotation) and exception scenarios (minors, assisted registration, degraded biometrics).

4.3 Performance and load testing

The campaigns proving the sizing chapter under representative load.

ID	Requirement
SAM-TST-009	● The Supplier shall perform load and performance tests demonstrating that the System meets the performance and sizing targets of VII.1.5 and the service levels of part F, including at least: enrolment packet ingestion at peak field throughput, deduplication throughput, IDVS verification response time under nominal and peak load, and portal response times. Test scripts, load profiles and raw results shall be delivered to the Purchaser.
SAM-TST-010	● The performance campaign shall include stress and endurance scenarios: sustained operation at peak load, behaviour beyond peak (graceful degradation, no data loss), and recovery of accumulated backlogs (e.g. deduplication queue after an ABIS outage) within the timeframes set in part F.

4.4 Security testing

Security testing from release candidate checks to independent penetration testing.

ID	Requirement
SAM-TST-011	● Every release candidate shall pass the Supplier's internal security testing: vulnerability scanning of infrastructure and applications, verification of hardening baselines, and review of access control configurations. Results shall be part of the release documentation.
SAM-TST-012	● Before each Operational Acceptance, an independent penetration test shall be performed by a third party firm as required by SAM-CYB-050, and all findings shall be remediated or formally accepted by the Purchaser according to the severity based remediation timelines. The security acceptance criteria of SAM-CYB-051 form part of the Operational Acceptance criteria.

4.5 Disaster recovery testing

The recovery capability is exercised for real before the platform is accepted.

ID	Requirement
SAM-TST-013	● Before Operational Acceptance of the platform release, the Supplier shall demonstrate a full failover of the System from the primary site to the disaster recovery site and a controlled failback, meeting the recovery objectives of VII.1.6, as well as a complete restore of the System from backups. These tests shall thereafter be repeated at the frequency set in SAM-CYB-020 during the recurrent services period.

4.6 Accessibility and usability testing

The portals and applications are tested with real users, including for accessibility.

ID	Requirement
SAM-TST-014	● The Supplier shall conduct usability testing of the enrolment application and back office applications with actual SBS operators before field deployment, covering the standard workflows and the main exception workflows, and shall incorporate the findings before the start of mass registration.
SAM-TST-015	● Citizen facing channels (portals, notifications, wallet application, receipts) shall be tested for accessibility against WCAG 2.1 level AA and for correct operation in both

	English and Samoan, including with users representative of vulnerable groups where practicable.

4.7 Pre commissioning and commissioning

The installation checks that precede any operational use of a production site.

ID	Requirement
SAM-TST-016	● For each production installation (data centre sites, personalisation sites, field kits), the Supplier shall perform pre commissioning tests verifying correct installation, configuration, connectivity, security baseline and monitoring coverage, documented in site specific pre commissioning reports approved by the Purchaser before the equipment or subsystem enters service.
SAM-TST-017	● Commissioning of the production platform shall include verified data flows across both sites, activation of backups and replication, activation of monitoring and SLA measurement (part F), and a documented go live checklist jointly signed by the Supplier and the Purchaser.

4.8 Operational Acceptance Tests (OAT)

The acceptance gates of the contract: staged OAT campaigns tied to the milestones, on agreed environments and data.

ID	Requirement
SAM-TST-018	● Operational Acceptance shall be organised in three Operational Acceptance Tests, aligned with the milestones of the Implementation Schedule (VII.2): (a) the **OAT V1 system** (milestone M4), covering the enrolment to credential chain (enrolment, deduplication, SDIN, core IDMS, digital credential issuance) and the CRVS stock database, and the ISO/IEC 18013-5 proximity interoperability test of SAM-TST-030; (b) the **OAT V1 card chain** (milestone M6b), covering the card personalisation chain, the demonstration of the non proprietary security features (SAM-TST-022) and the QR code readability evidence (SAM-TST-023); and (c) the **OAT V2 services** (milestone M8), covering the opening of the IDVS to relying parties and the portals. If the CRVS option is exercised, a further OAT CRVS (milestone M11) covers the civil registration flow, the legacy migration and the cutover. Each OAT scope shall be defined in the Master Test Plan.

SAM-TST-019	● Each OAT shall be executed against measurable acceptance criteria approved by the Purchaser in advance, derived from the requirements of Section VII, the performance targets of VII.1.5 and the service levels of part F. Acceptance criteria shall be objective (pass or fail, or measured value against threshold); subjective criteria are not acceptable.
SAM-TST-020	● OAT campaigns shall be executed in the acceptance environment (and in production for pre commissioning related items) using anonymised or synthetic datasets at representative volumes, following test scripts delivered in advance. Purchaser representatives shall witness the execution; the Supplier shall provide daily execution logs and a consolidated OAT report per campaign.
SAM-TST-021	● For the platform live milestone (OAT V1 system, milestone M4), the OAT shall include a supervised pilot period of production operation (duration set in VII.2) during which the System runs the real workload with SLA measurement active; Operational Acceptance is pronounced only if the availability and performance measurements over the pilot period meet the targets of part F.

4.9 Card chain acceptance

The card production chain has its own acceptance: quality, throughput and durability evidence.

ID	Requirement
SAM-TST-022	● Acceptance of the card subsystem shall include a demonstration, on production equipment, that every security feature of the approved card design is produced by the delivered equipment and consumables without recourse to proprietary elements available from a single source, in accordance with the non proprietary security features requirements of VII.1.2.4. The Supplier shall personalise an agreed batch of specimen cards for this demonstration.
SAM-TST-023	● Card acceptance shall include durability and readability evidence: (a) test reports against ISO/IEC 10373-1 and ISO/IEC 24789-1 and ISO/IEC 24789-2 (or equivalent) supporting the ten (10) year durability requirement, from an accredited laboratory, for the proposed card body and personalisation process; and (b) on site verification that the signed QR code content of specimen cards is read and

	verified successfully with the verification application on reference devices, and with at least one independent verifier built only from the published specifications and verification keys, under representative lighting and wear conditions. Editions of the standards cited here apply per the general rule of Section VII: the edition in force at the proposal deadline unless a dated edition is stated, the material part named where it matters.

4.10 Defect management during acceptance

How defects found in testing are classified, fixed and retested without gaming the acceptance.

ID	Requirement
SAM-TST-024	● All defects found during testing and acceptance shall be recorded in a defect tracking tool accessible to the Purchaser, with a severity classification agreed in the Master Test Plan (at minimum: S1 critical, S2 major, S3 minor, S4 cosmetic), reproduction steps, status and resolution history.
SAM-TST-025	● Blocking criteria: no Operational Acceptance shall be pronounced with open S1 or S2 defects in the scope of the release. S3 defects may be deferred with a Purchaser approved remediation plan and deadline; S4 defects shall be listed and tracked. Any regression introduced by a fix reopens the affected test scope.
SAM-TST-026	● After each failed or partially failed campaign, the Supplier shall deliver a corrective action plan within five (5) working days and bear the costs of re testing, including the Purchaser's reasonable witnessing costs, as further specified in the SCC.

4.11 Continuous quality assurance

Quality assurance as a permanent discipline across releases and changes.

ID	Requirement
SAM-TST-027	● The Supplier shall operate a documented quality management system for the project (ISO 9001 or equivalent), including peer reviews of designs and code, definition of done per deliverable type, and quality gates before each release. Quality records shall be auditable.

SAM-TST-028	● The Purchaser may, at any time and with reasonable notice, conduct or commission quality audits of the Supplier's test and development activities, including access to test results, defect data, code quality metrics and the requirements traceability matrix. The Supplier shall provide the requested evidence within ten (10) working days.

F. Service Specifications, Recurrent Cost Items (Service Levels and Recurrent Services)

This chapter defines the contractual service levels of the running platform and the recurrent services that sustain it: what is measured and how it is reported, the availability and response targets per service tier, support and maintenance obligations, and the penalty regime. Service levels bind the outcomes relying parties and citizens experience; bidders should propose an operating and support model sized for Samoa's context, including the offline and degraded behaviour obligations stated in VII.1.5.

5.1 Measurement and reporting framework

How service levels are measured, by whom, and how results are reported and audited.

ID	Requirement
SAM-SLA-001	● All service levels defined in this Section shall be measured automatically by the System itself or by the monitoring tooling delivered by the Supplier, without manual data collection. The Supplier shall deliver an SLA dashboard showing the current and historical value of every service level in near real time, with direct, unrestricted read access for the Purchaser (SBS) to the dashboard and to the underlying raw measurement data. Any custom scripts needed to complete the automated measurement shall be developed by the Supplier and delivered as part of the System. Measurement is performed by the central monitoring platform of the ICT Infrastructure component (SAM-INF-032), which is the authoritative measurement tool of these service levels.
SAM-SLA-002	● The service level regime applies from Operational Acceptance of the platform release (OAT V1 system, milestone M4) and throughout the warranty and recurrent services period. The card service levels (SAM-SLA-014 to SAM-SLA-016) enter into force at the Operational Acceptance of the card chain (OAT V1 card chain, milestone M6b). Unless stated otherwise per service level: measurement interval is monthly (24 hours a day, 7 days a week), reporting is monthly with a quarterly consolidated report, and planned downtime approved in advance by the Purchaser is excluded from availability calculations. Planned downtime shall not exceed eight (8) hours per month per subsystem, scheduled outside peak service hours. Unavailability caused by a declared disaster that is handled within the recovery objectives (RTO/RPO) of SAM-CYB-021 is likewise excluded from the availability calculation,

	but shall be fully tracked, measured and reported in the monthly service report.

5.2 Service level definitions

The service levels themselves: availability and performance targets per service tier.

Availability formula (used by all availability service levels): Availability % = {1 − [(total downtime − planned downtime) / (total time − planned downtime)]} × 100, measured monthly.

ID	Service level	Definition and measurement	Target	Penalty basis
SAM-SLA-003	IDVS availability	Availability of the verification, authentication, eKYC and credential status services measured at the IDVS service boundary by an automated probe executing a reference transaction at least every 60 seconds from an independent monitoring point. The IDVS is the critical component: relying party services depend on it. Unavailability attributable to Purchaser furnished facilities (power supply, hosting environment, telecommunication links) is excluded from the Supplier's availability measurement, provided the Supplier detects, reports and documents the event; this attribution rule applies to every availability service level of this table.	≥ 99.5% monthly	Severity 3 if < 99.5%; severity 5 if < 99.0%
SAM-SLA-004	IDMS availability	Availability of the IDMS core applications (registry, workflow, adjudication, SDIN services) measured by automated health checks every 60 seconds on each core service.	≥ 99% monthly	Severity 2 if < 99%; severity 4 if < 97%
SAM-SLA-005	CRVS availability	Availability of the CRVS applications and of the certificate and attestation retrieval	≥ 99% monthly	Severity 2 if < 99%; severity 4 if < 97%

		services, measured as for the IDMS.		
SAM-SLA-006	Verification response time	End to end response time of online verification transactions measured at the IDVS service boundary, computed over all production transactions of the month at the 95th percentile (per SAM-PER-014).	< 2 seconds (95th percentile) under nominal load	Severity 1 if breached one month; severity 3 if breached two consecutive months
SAM-SLA-007	Deduplication throughput and backlog	Daily count of enrolment packets fully deduplicated (ABIS 1:N completed) versus packets queued, and age of the oldest unprocessed packet. Measured daily, reported monthly. The System shall absorb the daily intake of the enrolment operation as sized in VII.1.5 (the full fleet: 50 kits plus the 10 enrolment tablets at their planning rates, per SAM-PER-002) with headroom for backlog recovery.	98% of packets received on day D deduplicated by end of day D+1; queue age never > 72 h	Severity 1 per day of breach; severity 3 if queue age > 72 h
SAM-SLA-008	ABIS operational accuracy	Continuous monitoring of the biometric chain in production: false positive rate measured as adjudication confirmed no HIT cases divided by ABIS HIT cases over the period; FMR/FNMR verified through periodic accuracy campaigns on ground truth datasets provided or approved by the Purchaser (protocol as per VII.1.2.2). Residual duplicate rate measured through audit sampling of the activated registry.	Operating point held at the SBS configured thresholds (SAM-IDM-018); FPIR and FNIR monitored monthly against the contracted outcomes (FPIR at most 0.01%, FNIR at most 1%); residual duplicate rate below 0.1%	Breach of duplicate rate: severity 3; accuracy campaign failure: remediation plan + severity 3
SAM-SLA-009	CRVS to registry synchronisation latency	Elapsed time between the registration or certification of a life event in the CRVS and its effect on the identity registry (e.g. death deactivation flow, record linkage), measured automatically on every synchronised event. During Version 1 (legacy CRVS still the	≤ 7 days for 100% of events; deactivation on death always within the statutory 28 days (NDID Act s.32(1))	Severity 2 if any event exceeds 7 days in the month; severity 5 if a statutory deadline is missed

		register of record), latency is measured from the receipt of the legacy CRVS extract by the System, the extract cadence being outside the Supplier's control; the full scope (measurement from the event registration itself) applies from the CRVS option cutover (M11), if the option is exercised.		
SAM-SLA-010	Record correction turnaround	Elapsed time from registration of a correction request (any channel, including the citizen portal per SAM-IDV-098) to completion of the correction workflow, measured by the case management module.	≤ 15 days for 95% of requests, 100% within 30 days [95% proposed]	Severity 1 if < 95%; severity 3 if < 85%
SAM-SLA-011	Incident detection and recovery (MTTD / MTTR)	Mean Time To Detect: elapsed time between occurrence (or first observability) of an incident and its detection by monitoring. Mean Time To Recover: elapsed time between detection and service restoration. Computed monthly over all severity 1 and 2 incidents from the incident management tool.	MTTD ≤ 24 h ; MTTR ≤ 72 h	Severity 2 per metric breached in the month
SAM-SLA-012	Authentication lock and preference change execution	Every authentication lock or unlock request and every notification or contact preference change submitted by an individual (portal, service centre) shall be executed: measured as requests effective in the IDVS authorisation layer versus requests submitted, with propagation time. Consent in the NDIDS is per transaction (single use, SAM-IDV-017); there are no standing consents to revoke.	100% of requests honoured, effective within 24 h of submission [24 h proposed]	Any missed lock request: severity 5
SAM-SLA-013	Complaints handling	Grievance cases managed in the complaints module (unique reference number, per Policy §14.5): time to	Acknowledgement ≤ 3 working days for 100% of complaints; resolution ≤ 30 days	Severity 1 if acknowledgement target missed; severity 2 if resolution < 95%

		acknowledgement and time to resolution measured automatically per case.	for 95% of complaints [95% proposed]	
SAM-SLA-014	Card personalisation throughput and turnaround	Weekly count of cards personalised versus the production plan set by the Purchaser (dynamic, based on printer pool in operation), and elapsed time from record validated for issuance to card ready for delivery.	Weekly plan met at ≥ 90%; 95% of cards personalised within 10 working days of validation	Severity 1 if plan < 90%; severity 2 if turnaround missed
SAM-SLA-015	Card personalisation reject rate	Cards rejected at quality control for Supplier attributable personalisation defects, divided by cards produced over the month. Rejected cards are reprinted at Supplier cost.	≤ 0.5% monthly	Severity 1 if > 0.5%; severity 3 if > 1%
SAM-SLA-016	Card delivery to issuance point	Elapsed time from card ready for delivery to card available at the designated issuance centre (Apia, Salelologa or field site), and stock of cards older than the threshold not yet delivered, measured in the card lifecycle module.	95% of cards available at the issuance point within 10 working days of personalisation	Severity 1 if < 95%; severity 2 two consecutive months
SAM-SLA-017	Storage and backup compliance	Adherence to the approved backup schedule (successful completion of scheduled backups) and absence of storage data loss, verified by automated backup reports and periodic restore tests.	100% of scheduled backups successful or rerun within 24 h; no data loss beyond the RPO of SAM-CYB-021	Severity 2; any data loss beyond the RPO: severity 5
SAM-SLA-018	Outbound event delivery (write back and notifications)	Elapsed time between an event in the identity system (SDIN allocation, status change, effect of a registered death) and the delivery of the corresponding write back or notification message to the subscribed system (CRVS return leg and notification services per SAM-IDM-141), measured on the supervision platform.	95% of events delivered within 24 h, 100% within 72 h	Severity 1 if below 95%; severity 2 if breached two consecutive months

5.3 Support and maintenance service levels

The response and resolution obligations of the support organisation.

ID	Requirement
SAM-SLA-021	● During the warranty period and the recurrent services period, the Supplier shall operate a support service with the following response and resolution targets, measured automatically from the ticketing tool (accessible to the Purchaser). Targets apply 24 hours a day, 7 days a week for severity 1; working hours (Samoa time) for lower severities.

Severity	Definition	Response time	Workaround	Resolution time
S1 Critical	Production service down or major security incident (IDVS, IDMS, CRVS, personalisation stopped)	1 hour (24/7)	4 hours	24 hours
S2 Major	Significant degradation, key function unavailable, no acceptable workaround	1 hour	8 hours	72 hours
S3 Minor	Degraded function with workaround, no service interruption	4 working hours	3 working days	Next maintenance release
S4 Cosmetic	No operational impact	1 working day	n/a	Planned release

5.4 Penalties

The financial consequences of missed service levels, capped and reported transparently.

ID	Requirement
SAM-SLA-019	● Penalty mechanics. Each service level breach is assigned a severity level (0 to 5) as stated in its Penalty basis. Penalties are computed quarterly by applying the percentage corresponding to each severity level (severity 1 = 1%, severity 2 = 2%, severity 3 = 3%, severity 4 = 4%, severity 5 = 5%) to the amount invoiced for the recurrent services of the quarter in which the breach occurred; penalties for all breached service levels in a quarter are cumulative. The applicable penalty rate shall be computed automatically by the SLA management solution from the measured data (SAM-SLA-001). The aggregate cap on service level penalties, and their relationship with liquidated damages on milestones, are set in the SCC. No bonus or earn back mechanism applies. In case of breaches persisting over two consecutive quarters, the Purchaser may issue a formal notice requiring a written remediation plan, without prejudice to its other contractual rights.

SAM-SLA-020	● SLA reporting and review. The Supplier shall deliver a monthly service report (measured values, breaches, incidents, penalties accrued, corrective actions) and attend a quarterly service review with the Purchaser. Service level targets shall be confirmed at the end of the supervised pilot period (SAM-TST-021); thereafter, targets may be recalibrated once a year by agreement of the Parties within the limits set in the SCC, in particular after the end of the mass registration phase.

VII.2 Implementation Schedule, Sites and Holidays

(a) Implementation Schedule Table

All milestone weeks count from the Effective Date of the Contract (assumed around March 2027; the absolute dates in the comment column are indicative only and will be fixed at contract award). The Implementation Schedule is phased in two releases: Version 1 delivers enrolment, the identity core up to continuous registration, digital credential issuance and the National ID Card chain (card production for the Version 1 cohort); Version 2 delivers the usage layer (IDVS opening to relying parties, relying party pilot) and, if the CRVS option is exercised, the civil registration flow with legacy migration and cutover. Where a range is shown, the later date is the contractual deadline, and liquidated damages, where they apply, are assessed against it. The earlier date is the Purchaser's target date and does not create any right to negotiate. The card chain milestones are carried in Version 1 as M6b and M6c. The numbering of M7 to M12 is kept stable to preserve cross references.

The schedule includes an early proof of concept phase ahead of the mass build activities (SAM-TST-029): a limited scope demonstration of the end to end chain, whose milestone precedes the field capture start. Its position in the milestone sequence shall be proposed by the Supplier and agreed at the design stage.

No.	Milestone	Week from Effective Date	Liquidated damages milestone (Y/N)	Comment (indicative absolute date,)
M1	Detailed design validated (system design, card design, enrolment workflow, site fit out specifications, agreed in the technical workshops)	Week 8	N	~May 2027
M2	Enrolment kits and tablets delivered in country, capture application installed, tested and accepted (pre commissioning)	Week 10 to 14	**Y**	~June 2027. Main schedule lever; the delivery lead time is a negotiation priority
M3	Field capture start (mass registration wave opens)	Week 14	N	~June/July 2027. Requires M2 plus Purchaser prerequisites P1 and P2 below
M4	Platform live: deduplication, SDIN generation and notification, first authentication capability, digital credential issuance (VC) live, CRVS stock database commissioned (Operational Acceptance Test V1 system passed) End to end scope: enrolment through IDMS processing to card issuance (payment milestone M4).	Week 36	**Y**	~November 2027
M5	60,000 persons enrolled and	Week 44	**Y**	Before 31 December 2027. Shared milestone: the

	processed (PDO milestone)			Supplier is liable for system capacity and availability, the Purchaser for field operations (see note 3)
M6	Continuous registration open (kits redeployed to permanent offices, service centre workstation configuration)	Week 44	N	~December 2027
M6b	Card chain commissioned: Apia personalisation centre operational, card production started for the Version 1 cohort (Operational Acceptance Test V1 card chain passed)	Week 40 to 44	**Y**	~December 2027. Requires prerequisite P4 (s.34(5) regulation) for QR personalisation
M6c	Version 1 cohort card production and delivery complete: cards produced and delivered for the enrolled cohort whose legal identity is confirmed	Week 52 to 56	N	~March/April 2028; target before the PDO date. Cards are delivered only after confirmation of legal identity (SAM-CRD-051)
M7	CRVS base components delivered: registration database and interoperable back end operational, stock preload executed, SDIN write back demonstrated (payment milestone M7)	Week 40 to 48	N	~January 2028
M8	IDVS authentication and verification services open to registered relying parties (Operational Acceptance Test V2 services, first release)	Week 70	N	~mid 2028, Version 2 start
M9	Relying party pilot completed: 3 to 5 relying parties in production, at least 5 co developed use cases, transfer evaluation passed	Week 96	N	~early 2029; 5 services integrated in year 2 per the National ID Policy KPI
M10	**If the CRVS option is exercised**: CRVS flow live (registration of new vital events) and legacy data migration completed and reconciled	Week 100	N	~early 2029; weeks recomputed from the option exercise date if later
M11	**If the CRVS option is exercised**: CRVS cutover: new system becomes the national	Week 104	**Y** (only if the option is exercised)	~March 2029

	register of record, legacy system archived; CRVS to identity interface live (Operational Acceptance Test CRVS passed)			
M12	**Final skills transfer assessment (scores the section 4 grid and releases the transfer retention)**	At the latest 26 weeks after Operational Acceptance V2	**N**	Inside the financing period

Notes to the Implementation Schedule

1. **Purchaser prerequisites (legal milestones outside the Supplier's responsibility).** The following legal steps condition certain milestones. They are the Purchaser's responsibility; if a prerequisite is late, the dependent Supplier milestone is extended day for day and no liquidated damages accrue for that delay:

- **P1.** Commencement order by the Minister bringing Part 3 (registration) of the National Digital Identification Act 2024 into force (s.1(2)), and publication in the Savali of the mass registration period and modalities (s.20(2)). Prerequisite to M3.
- **P2.** Regulation under s.31(3) fixing the length of the SDIN and token and the checksum formula. Prerequisite to SDIN generation within M4; the system shall be configurable pending this regulation.
- **P3.** Commencement order for Part 6 (SDIN, credentials, authentication) and publication of the relying party list (s.40(6)). Prerequisite to M8.
- **P4.** Regulation under s.34(5) on the machine readability of credentials, including the QR code. This is a hard Version 1 prerequisite: printed machine readable features (QR code, MRZ) are readable as soon as a card is printed and cannot be activated later on a chipless card (SAM-LEG-022), so no card bearing such features may be personalised before the regulation is in force. P4 therefore gates the start of card personalisation and the card OAT of M6b.
- **P5.** Savali publications for continuous registration (s.22(2)) and for the feeding of the Identity Database from civil registration and passports (s.28(2)). Prerequisites to M6 and to the CRVS preloading dependencies of M3.

2. Milestones marked Y in the liquidated damages column are subject to the liquidated damages rate and cap stated in the SCC (GCC 27). All other milestones are contractual but carry no liquidated damages. For M11, liquidated damages apply only if the CRVS option is exercised; if the option is not exercised, M10 and M11 fall away.

3. Milestone M5 depends jointly on Supplier performance (M2, M4, system throughput and availability) and on the Purchaser's field operations (staffing, community mobilisation, logistics). Liquidated damages under M5 apply only where the shortfall is attributable to the Supplier's scope.

4. The Operational Acceptance Tests attached to M4 (OAT V1 system), M6b (OAT V1 card chain), M8 (OAT V2 services) and M11 (OAT CRVS, if the option is exercised) are described in part E, Testing and Quality Assurance.

(b) Site Table

No.	Site	Role	Existing condition and works required

S1	SBS building, Apia: main server room	Primary hosting site for the identity platform (IDMS, ABIS, IDVS node, CRVS)	Exists. Secured, access controlled, air conditioned, with space for one additional rack; already runs SBS production and a replica environment. Works required: uninterruptible power of 20 to 30 kVA backed by a generator starting within 5 to 10 seconds, supervision and monitoring, additional firewall capacity, additional storage. The identity platform stays logically isolated from existing SBS systems. Scope split between Supplier and Purchaser to be settled in the inventory tables
S2	SBS building, Apia: supervision cell	Central monitoring platform and operational dashboards	To be established in dedicated space near the server room. Monitoring platform supplied as part of the identity solution
S3	Apia: card personalisation centre	Card personalisation and printing, blank and printed card storage	To be created; accommodation identified by the Purchaser. Layout designed with the selected Supplier at project start
S4	Apia: registration offices, adjudication office (5 to 10 workstations) and investigation office (2 to 4 staff)	Continuous registration, manual adjudication, fraud investigation	Accommodation identified by the Purchaser; workstations and software supplied by the Supplier
S5	Salelologa (Savai'i): registration and card delivery site	Continuous registration office and card delivery and collection point (base scope). A second card production line at Salelologa is a priced option, not base scope: in base scope all cards are produced in Apia and delivered to Salelologa	Existing BDM registration office; delivery and collection point to be fitted out. Spares people on Savai'i a ferry journey to collect a card. Production line fit out only if the option is exercised
S6	Vodafone data centre	Disaster recovery site; the architecture shall allow role swapping with S1	Exists, remotely operated by the SBS ICT team which retains control. Already hosts the civil registration replica and backups (20 TB backup server, offsite copies)
S7	Itinerant enrolment sites (both main islands, Upolu and Savai'i)	Mass registration field sites: community halls, churches, schools, following the census field model (about 24 teams, one area at a time)	No fixed infrastructure; the kits are self sufficient (table and two chairs only). Logistics by road and inter island ferry; travel distance for communities kept to about 5 to 10 km

(c) Table of Holidays

Public holidays of Samoa. List drawn from standard national observance, to be confirmed with SBS before contract signature; the SCC state how holidays affect the time computation.

No.	Holiday	Date
1	New Year's Day	1 January (and 2 January, customary)
2	Good Friday	movable (March/April)
3	Easter Monday	movable (March/April)
4	ANZAC Day	25 April
5	Mother's Day holiday	Monday after the second Sunday of May
6	Independence Day	1 June
7	Father's Day holiday	Monday after the second Sunday of August
8	White Sunday holiday (Lotu a Tamaiti)	Monday after the second Sunday of October
9	Christmas Day	25 December
10	Boxing Day	26 December

Note: field enrolment planning shall also respect Sunday observance and village protocols; the operational calendar is agreed with the Purchaser during the design phase.

VII.3 System Inventory Tables

Chaining note. These inventory tables feed the Price Schedules of Section IV (each line below must map to a priced line) and the Implementation Schedule of VII.2 (delivery of the enrolment fleet is milestone M2; platform items support M4; card chain items support M6b and M6c). Lines marked "option" are priced options exercisable by the Purchaser, quoted separately in the Price Schedules. Proposers shall price the quantities stated here, and the Purchaser will adjust at award if needed. "Recurrent" indicates whether the item carries recurrent costs (licences, subscriptions, maintenance, consumables) to be quoted in the Recurrent Cost Schedule, with the duration shown.

Table 1. Enrolment kits and tablets

Item	Description	Unit	Quantity (Supply & Install)	Recurrent (Y/N, duration)
1.1	Portable enrolment kit, case format (laptop, FAP60 minimum optical tenprint scanner, camera, document scanner, signature capture, GPS, USB 4G dongle, 58 mm thermal receipt printer, power autonomy with one power bank, no second battery). Spare capacity is provided by fleet slack (SAM-ENR-119): no separate hot spare line	kit	50 (firm)	Y, maintenance 2 years post acceptance
1.3	Laboratory and training kit (reference kit for the test environment, training and integration, kept at the central site)	kit	1	Y, same terms
1.4	Ultra mobile rugged enrolment tablet (FAP60 minimum, rear camera capture, Bluetooth 58 mm receipt printer, backpack bag)	tablet	10	Y, maintenance 2 years post acceptance
1.4b	Laboratory and training tablet (reference tablet for the test environment, training and integration, kept at the central site; per SAM-ENR-125)	tablet	1	Y, same terms
1.5	Spare parts lot (batteries, power banks, sensors, cables) sized for 2 years of field operations	lot	1	N
1.6	Central enrolment services (kit fleet management, package	system	1	Y, support 2 years

	reception, synchronisation, monitoring), hosted at the primary site			
1.7	Enrolment consumables year 1 (receipt paper, cleaning supplies)	lot	1	Y, yearly reorder option
1.8	Solar recharge set for outreach teams (panels, connectors, transport packaging; per SAM-ENR-093)	set	12 (option, indicative 10 to 12)	N

Table 2. IDMS and ABIS platform

Item	Description	Unit	Quantity (Supply & Install)	Recurrent (Y/N, duration)
2.1	IDMS software (population register, identity lifecycle, SDIN generation by the standalone unique number generator delivered with full source code and documentation per SAM-IDM-022, workflow orchestration BPMN 2.0/DMN)	system	1	Y, support and updates under perpetual licence + support 2 years
2.2	ABIS support and updates under perpetual licence, gallery sized for 250,000 (baseline, extensible to 800,000 under the increment option) identities (lifetime volume per SAM-PER-001; no licence capped below 250,000 per SAM-PER-020) with growth path	licence	1	Y, duration of the contract + 2 years support
2.3	Servers and virtualisation for IDMS/ABIS, primary site (SBS)	lot	1	Y, hardware maintenance 2 years
2.4	Storage, primary site (enrolment packages, biometrics, documents; sizing per person)	lot	1	Y, maintenance 2 years
2.5	Adjudication workstations (manual adjudication, about 10,000 complex cases, throughput in the hundreds per day during the mass wave)	workstation	8 (range 5 to 10)	N
2.6	Investigation workstations	workstation	3 (range 2 to 4)	N
2.7	Test and pre production	environment	1	Y, support 2 years

	environment (shared across subsystems, may be virtualised)			

Table 3. IDVS (identity verification services)

Item	Description	Unit	Quantity (Supply & Install)	Recurrent (Y/N, duration)
3.1	IDVS software (1:1 verification, eKYC with consent, OTP, QR verification, credential status, OIDC/OAuth 2.0 federation, OpenID4VCI/VP issuance, relying party management, portals)	system	1	Y, support and updates under perpetual licence + support 2 years
3.2	IDVS redundant nodes, primary site (SBS)	node	2	Y, maintenance 2 years
3.3	IDVS redundant nodes, secondary site (Vodafone DC), active for high availability and role swap	node	2	Y, maintenance 2 years
3.4	Relying party portal and sandbox environment (documentation, test keys, certification)	environment	1	Y, support 2 years
3.5	Billing integration on a pluggable open source ERP, configuration not custom development. Priced option, exercised when the fee policy is adopted; metering and quotas remain base scope within 3.1	system	1 (option)	Y, support 2 years if exercised

Note: the cloud wallet is deferred to Version 2 and carries no priced line in this table; the architecture must permit it without redesign (VII.1.2.4).

Table 4. CRVS platform (three DPI components)

Item	Description	Unit	Quantity (Supply & Install)	Recurrent (Y/N, duration)
4.1	Component 1: national civil registration database (single source of truth registry, initial load from the existing digital CRVS stock). **Base scope, Version 1** (stock database, milestone M4)	system	1	Y, support 2 years
4.2	Component 2: interoperable back end (standardised and versioned	system	1	Y, support 2 years

	interoperability gateway, APIs, notification and attestation services serving the Version 1 stock database and the legacy sync, VC in QR issuance). **Base scope, Version 1**			
4.3	Component 3: business flow engine (BPMN/DMN configured registration flows). **Priced option** (CRVS flow, exercisable at Version 1 acceptance); design in base scope	system	1 (option)	Y, support 2 years if exercised
4.4	CRVS office workstations and scanners (Apia and Salelologa, capture and certification of records). **Priced option**, delivered with the CRVS flow option	workstation	6 (option)	N

Table 5. Card chain

Item	Description	Unit	Quantity (Supply & Install)	Recurrent (Y/N, duration)
5.1	Card personalisation printers, laser engraving, polycarbonate, desktop class operated in a pool, Apia centre (3 in the pool plus 1 reserve)	printer	4 (firm)	Y, maintenance and 2 years support
5.2	Additional card personalisation printers (priced option, capacity extension)	printer	2 (option)	Y, same terms
5.2b	Salelologa production line: printer installation, site fit out, secure storage (priced option; in base scope Salelologa is a delivery and collection point only, per VII.2 site table)	line	1 (option)	Y, same terms if exercised
5.3	Card and credential signing: served by the consolidated operational HSM pair of Table 7 (SAM-INF-040); no separate card HSM line	n/a	n/a (see 7.2)	n/a
5.4	Blank polycarbonate cards, whole contract volume delivered in a single delivery (no	card	250,000	Y, single delivery; unit price kept for the ITP 44(c) variation

	chip, ID1, no thicker than 0.76 mm; non proprietary security features). Volume basis (7 Sep 2026, on the instruction of SBS): the contract card volume is aligned on the provisioned baseline of 250,000 persons of SAM-PER-001; it covers the full locally living population, five years of issuance following the end of the mass enrolment campaign (new eligibles, replacements, renewals) and the wastage and reject allowance; overseas residents are served digital first, with no card provision. The stock is supplied once before the card chain operational acceptance (SAM-CRD-069); the unit price of the Unit Rates Schedule applies to the award variation of ITP 44(c) and to any later order.			
5.5	Printing films, laminates and other personalisation consumables, year 1	lot	1	Y, yearly reorder
5.6	Quality control equipment (verification readers, durability sampling)	lot	1	N
5.7	Card personalisation system software (personalisation data preparation, queue management, printer driving)	system	1	Y, support 2 years
5.8	Card management software (card lifecycle: issuance, delivery, activation, loss, replacement)	system	1	Y, support 2 years
5.9	Quality control software (personalisation QC, reject tracking, per SAM-SLA-015)	system	1	Y, support 2 years
5.10	Consumables stock management software (blank cards, films, laminates; alerts on stock thresholds)	system	1	Y, support 2 years

5.11	Card design application (design and versioning of the card templates within the legal constraints of VII.1.1)	system	1	Y, support 2 years
5.12	Delivery tracking software (card ready to issuance point tracking, per SAM-SLA-016)	system	1	Y, support 2 years

Table 6. ICT Infrastructure component: data centre, network and power

Tables 6 and 7 together form the ICT Infrastructure component (SAM-INF-001 to 048).

Item	Description	Unit	Quantity (Supply & Install)	Recurrent (Y/N, duration)
6.1	Rack and in rack fit out, SBS main server room (one rack space available)	rack	1	N
6.2	Rack and fit out, Vodafone DR site	rack	1	Y, hosting terms per Purchaser agreement with Vodafone
6.3	Network equipment, hosting sites (firewalls, switches, VPN for kit synchronisation, inter site link equipment) (SAM-INF-012, SAM-INF-013)	lot	1	Y, maintenance 2 years
6.4	Backup infrastructure (extension of the existing 20 TB replication scheme, offsite copies) (SAM-INF-005)	lot	1	Y, maintenance 2 years
6.5	Uninterruptible power 20 to 30 kVA with generator autostart (5 to 10 s) and clean shutdown procedures for the HSMs, SBS room. Supplier supply, installation and commissioning (SAM-INF-020); sizing and autonomy confirmed by the site survey Ruling of 1 Sep 2026 (hosting boundary): room level power protection is Purchaser furnished; the Supplier's scope is limited to in rack power protection delivered with its turnkey racks. Not priced by proposers, pending final confirmation.	lot	1	Y, maintenance 2 years

6.6	SBS server room adequacy works (cooling on protected supply, fire protection, access control complement) Ruling of 1 Sep 2026 (hosting boundary): these works are a Purchaser prerequisite, not Supplier scope. Not priced by proposers.	lot	1	N. The allocation between Supplier scope and Purchaser prerequisite is settled by the site survey report of SAM-INF-004.
6.7	Central supervision and monitoring platform, single platform covering the entire System including the CRVS and the card chain, authoritative for SLA measurement (SAM-INF-030 to 037)	system	1	Y, support 2 years
6.8	Network equipment for the card personalisation premises (Apia and Salelologa), the adjudication and investigation offices and the supervision cell (SAM-INF-014)	lot	1	Y, maintenance 2 years
6.9	Standby generator — Purchaser furnished, if required by the site survey (SAM-INF-022). **Client prerequisite, not priced**; the Supplier specifies, integrates and monitors it	n/a	n/a	N
6.10	DR site compute and storage, sized for active/passive recovery of the IDMS, ABIS and CRVS within the RTO/RPO of SAM-CYB-021 (SAM-INF-003, SAM-ARC-021). Only the IDVS layer is deployed symmetrically on both sites (Table 3, lines 3.2 and 3.3)	lot	1	Y, maintenance 2 years

Table 7. ICT Infrastructure component: PKI and trust anchor

Item	Description	Unit	Quantity (Supply & Install)	Recurrent (Y/N, duration)
7.1	Root CA HSM (offline root device, held by SBS) with dual control backup token set (SAM-INF-040)	HSM	1 device + 1 backup token set	Y, maintenance 2 years

7.2	Operational HSM resilient pair (issuing CA and all issuance, card and credential signing; consolidated footprint per SAM-INF-040, serving Table 5 signing needs)	HSM	2 (resilient pair)	Y, maintenance 2 years
7.3	PKI software, CP/CPS drafting support, key ceremony execution (scripted, filmed, witnessed) and ceremony training	service	1	Y, support 2 years

Table 8. Implementation and recurrent services

Item	Description	Unit	Quantity (Supply & Install)	Recurrent (Y/N, duration)
8.1	Design workshops, detailed specifications, integration and configuration services	lump sum	1	N
8.2	CRVS data preloading and stock load services (Version 1, base scope). Full legacy migration and reconciliation are priced within the CRVS option (Table 4, line 4.3 scope)	lump sum	1	N
8.3	Training and capacity building programme per the Capacity Building Annex (plan within 4 weeks, paired working, immersion, knowledge base, code in the Purchaser repository, acceptance by Purchaser performed deployment)	programme	1	N (retention terms in SCC)
8.4	Supplier support during the mass registration campaign (field support, hot line, spare logistics)	months	8	N
8.5	Card production operation support, first year (train and supervise before handover to local teams)	months	12	N
8.6	Warranty and post acceptance support, all subsystems	years	n/a	Y, 2 years proposed
8.7	Relying party pilot support (3 to 5 relying parties, at least 5 co developed use cases, about 6 months)	programme	1	N

8.8	Cyber security management services: ISMS operation, risk assessments, hardening verification, participation in national cyber crisis exercises, security documentation (SAM-CYB-001 to 024)	lump sum	1	N

VII.4 Background and Informational Materials

The material in this part is provided for information only. Nothing in this part creates a requirement on the Supplier or modifies the requirements stated elsewhere in Section VII. Where a statement here appears to conflict with a requirement, the requirement prevails.

The country and the project

Samoa is implementing a National Digital Identification System (NDIDS) under the World Bank financed project P181456. The implementing agency and Purchaser is the Samoa Bureau of Statistics (SBS), whose Chief Executive Officer also holds the office of Registrar General under the national identification law. The project objective for the first phase is a foundational identity registry with 60,000 persons enrolled and processed by 31 December 2027, followed by progressive coverage of the full eligible population (of the order of 99,000 identities by the end of 2029 and about 250,000 in the long run, figures under confirmation by SBS against the October 2026 census). The system is planned in two releases: Version 1 covers enrolment, deduplication, SDIN generation, the first authentication capability, digital credential issuance and the National ID Card chain; Version 2 covers the opening of the identity verification services to relying parties, the relying party pilot and, if the option is exercised, the civil registration flow with legacy migration. The Government has designated the NDIDS a national critical infrastructure (see VII.1.6 for the resulting requirements). During the inception phase, two scope gaps were identified and added to the programme scope: the public key infrastructure serving the signature and encryption needs of the system, and the completion of the hosting facilities (uninterruptible power, generator interface and central supervision), now carried by the ICT Infrastructure component of VII.1 and part D.

A. Background

0.1 The Purchaser

- **SBS and the Registrar General.** SBS implements the project, hosts the National ID Division and operates the national census. The Registrar General function is legally distinct from the Government Statistician function.
- **NDID Advisory Board.** Established by the NDID Act to advise on the operation of the system.
- **Office of the Attorney General (OAG).** Involved in the regulations and in the legal instruments around credentials and relying parties.
- **DCRS project (Digitally Connected and Resilient Samoa, P180807).** A parallel World Bank project covering wider digital infrastructure, standards and the national data centre programme, under separate governance. NDIDS rolls out first, so infrastructure dependencies are mitigated on the NDIDS side; a coordination channel between the two project teams manages standards, hosting rules and security baselines. Choices made for NDIDS may act as pioneer implementations for the wider programme.

0.2 The Purchaser's business objectives for the Information System

SBS pursues five objectives with the National Digital Identification System. First, to give every resident of Samoa a single trusted identity that can be proven in person and online, held in one authoritative register under SBS control. Second, to make registration inclusive and reachable, through a mass enrolment wave followed by continuous registration, covering the outer islands and persons with limited mobility. Third, to let public bodies and licensed private relying parties verify an identity without copying and storing personal data,

through a verification service kept separate from the identity register. Fourth, to modernise civil registration so that the record of vital events is digital, authoritative and usable online. Fifth, to build the capacity of SBS staff so that the System is operated by Samoa, and not by the Supplier, at the end of the contract. The Supplier is expected to design and implement the System so that these objectives can be measured after go live.

B. Informational Materials

0.3 The legal, regulatory and normative context for the Information System

- **National Digital Identification Act 2024 (NDID Act).** The framework law. Several Parts, notably Part 3 (registration) and Part 6 (SDIN, credentials, authentication), commence on dates to be fixed by the Minister (s.1(2)). Operational steps such as the mass registration period, continuous registration, feeding of the Identity Database from civil registration and passports, and the relying party list are triggered by publications in the Savali. These commencement steps are the Purchaser's responsibility and are reflected as Purchaser prerequisites in the Implementation Schedule (VII.2).
- **Regulations in preparation.** A number of technical parameters are delegated to regulations, among them the length of the SDIN and token and the checksum formula (s.31(3)), the machine readability of credentials including the QR code (s.34(5)), the protection of the digital credential (s.35(2)), authentication procedures, protocols and standards (s.37(2), s.39), the cybersecurity of the Biometric Database (s.38(3)), relying party eligibility and access procedures (s.40), general security measures (s.46(3)), the complaint procedure (s.53(2)) and fees (s.59(a)). The functional requirements in VII.1 ask for configurability on these points so the system can absorb the regulations when made.
- **National Digital ID Policy v20.0.** The endorsed policy instrument carrying, among others, the coverage and inclusion targets, the service integration target (5 services integrated in year 2), key performance indicators reflected in the service levels (VII.1, SLA block), and the data localisation measure (national hosting with a possible cloud extension).
- **Births, Deaths and Marriages Registration Act 2002 (BDM Act).** Governs civil registration, which remains the primary source of identity evidence for most Samoans.

0.4 Existing information systems and technologies relevant to the Information System

- **SBS main server room (Apia).** Exists: secured, access controlled, air conditioned, running SBS production systems and a replica environment, with space for one additional rack. Planned reinforcement covers uninterruptible power (20 to 30 kVA with generator autostart), supervision and monitoring, additional firewall capacity and additional storage. The identity platform will be logically isolated from existing SBS systems.
- **Vodafone data centre.** Exists as the disaster recovery site, remotely operated by the SBS ICT team which retains control of the systems. It already hosts the civil registration replica environment and project backups (virtual machine replication to a dedicated 20 TB server, with offsite copies).
- **Connectivity.** Mobile network coverage supports kit synchronisation over 4G with fallback; inter island bandwidth between Upolu and Savai'i shapes the synchronisation and DR design. Equipment procurement through approved suppliers in Samoa typically takes 12 to 14 weeks, about one week by air freight where justified.
- The SBS ICT team is lean but capable, with basic development skills, and has a stated working preference for established server platforms (a preference, not a restriction).

0.4 (continued) Civil registration today

- The Births, Deaths and Marriages Register runs on a digital system in service since 2003, covering births, deaths, marriages, divorces and adoptions. Originally supplied and managed from Australia, the system is **no longer maintained by its vendor**; it currently runs in a virtual machine on SBS servers (BDM visit of 31 Jul 2026). BDM staff produce CSV extracts from it routinely: bidders shall assume **file based (CSV) extraction as the only interface to the legacy system**; no vendor support and no API are available. The system was sized for about 570,000 records and that capacity has been exceeded, so older records are extracted and stored separately. Because this unmaintained system remains the system of record for new vital events until the CRVS cutover, the early commissioning of the stock database and a frequent extraction discipline are part of the continuity approach of the Requirements.
- Registration is delivered from two offices, Apia and Salelologa. Officers hold role based licences and registration uses double key verification, giving real segregation of duties.
- About 80 percent of births occur in hospitals and are notified directly by the hospital; the remaining 20 percent are home births declared by the parents, with village representatives authorised to complete the notification, and these are less likely to be registered.
- Paper records reach back to about 1961 and are well organised through a card index by year of birth and village. Digitisation is incomplete and there is no intention to digitise every historical record; the strategy is demand driven digitisation of the most requested record years.
- Senior officers can perform data extractions and the SBS ICT team has direct access to the database, which is favourable for the migration of the existing stock.
- SBS has confirmed that the civil registration system will be replaced rather than upgraded; the replacement is part of the CRVS scope described in VII.1 (V1 stock, V2 flow and migration).
- There is no existing national identity card in Samoa. The passport is the main government issued photo credential; birth certificate and passport are the two primary identity proofing documents.
- The national census of October 2026 carries NDID questions and a household listing (about 34,808 households counted recently), which seeds the registration campaign planning and identifies households needing assisted enrolment.

0.5 Available training facilities to support the implementation of the Information System

The Purchaser makes its own premises available for training, in Apia and at the Salelologa office, and expects the Supplier to deliver training on those premises. The Purchaser may also rent dedicated facilities if on premises facilities cannot accommodate training capacity. The rooms available, their capacity, the workstations and the network available to trainees are to be confirmed by the Purchaser before the proposal submission deadline. The Purchaser premises facilities available for training comprise the Conference Rooms 1, 2, 3 (recommended maximum 20 participants; restricted free-space capacity of 25) and the National ID Room. For a targeted audience of more than 20 participants, an alternative venue can be arranged, with network connectivity supplied. Equipment, such as laptops and tablets (excluding procured enrolment kits) are to be provided by participants.

0.6 Site drawings and site survey information relevant to the Information System

The sites concerned by the System are listed in the site table of VII.2. They are the SBS premises and server room in Apia, the secondary data centre at the Vodafone site, the Salelologa office, and the itinerant enrolment sites used during the mass enrolment wave. Drawings and survey information for the two data centre sites, covering floor plans, rack elevations, power and cooling, are held by the Purchaser and are made available to

proposers on request during the clarification period. Whether a further survey is required before the design phase is to be confirmed by the Purchaser.

0.7 Geography and logistics

Samoa comprises two main inhabited islands, Upolu (with the capital Apia) and Savai'i, linked by ferry. The country is divided into 4 regions (Apia Urban Area, North West Upolu, Rest of Upolu, Savai'i), 51 districts and 339 villages, with 695 census enumeration areas. The census field model (about 24 teams working one area at a time, district by district) is the operational backbone for mass registration. Communities are expected to travel about 5 to 10 km to an enrolment point; churches and community halls are the natural enrolment venues. The climate is humid tropical maritime; equipment travels by road and ferry.

0.8 Responsibilities of the Purchaser and of the Supplier

For information, the split of responsibilities is broadly as follows; the binding statements are in VII.1 to VII.3 and in the Contract:

- **The Purchaser provides:** the sites listed in the Site Table (VII.2(b)) including the accommodations to be identified; the legal framework steps (commencement orders, Savali publications, regulations) listed as Purchaser prerequisites in the Implementation Schedule; the extraction of the existing civil registration data for preloading and migration; the field operations of the registration campaign (staffing, mobilisation, community engagement, logistics of the field teams); and the governance bodies.
- **The Supplier is expected to deliver:** the full system scope described in VII.1 (enrolment fleet and capture application, IDMS/ABIS, IDVS and relying party services, CRVS platform, credentials and card chain, PKI, infrastructure reinforcement within the scope settled in the inventory tables), the implementation services (design, integration, migration, testing), and the training and capacity building programme, whose acceptance model rests on deployments performed by SBS staff.

PART 3 – CONDITIONS OF CONTRACT AND CONTRACT FORMS

SECTION VIII - GENERAL CONDITIONS OF CONTRACT

Table of Clauses

A. Contract and Interpretation 297

1. Definitions 297
2. Contract Documents 304
3. Interpretation 304
4. Notices 307
5. Governing Law 308
6. Fraud and Corruption 308

B. Subject Matter of Contract 308

7. Scope of the System 308
8. Time for Commencement and Operational Acceptance 309
9. Supplier's Responsibilities 310
10. Purchaser's Responsibilities 316

C. Payment 318

11. Contract Price 318
12. Terms of Payment 318
13. Securities 319
14. Taxes and Duties 320

D. Intellectual Property 321

15. Copyright 321
16. Software License Agreements 322
17. Confidential Information 323

E. Supply, Installation, Testing, Commissioning, and Acceptance of the System 325

18. Representatives 325
19. Project Plan 327
20. Subcontracting 329
21. Design and Engineering 330
22. Procurement, Delivery, and Transport 333
23. Product Upgrades 335
24. Implementation, Installation, and Other Services 336
25. Inspections and Tests 336
26. Installation of the System 337
27. Commissioning and Operational Acceptance 338

F. Guarantees and Liabilities 341

28. Operational Acceptance Time Guarantee 341
29. Defect Liability 342
30. Functional Guarantees 345
31. Intellectual Property Rights Warranty 346
32. Intellectual Property Rights Indemnity 346
33. Limitation of Liability 349

G. Risk Distribution 349

34. Transfer of Ownership 349
35. Care of the System 349

36. Loss of or Damage to Property; Accident or Injury to Workers; Indemnification 351
37. Insurances 352
38. Force Majeure 354

H. Change in Contract Elements 356

39. Changes to the System 356
40. Extension of Time for Achieving Operational Acceptance 360
41. Termination 360
42. Assignment 367

I. Settlement of Disputes 367

43. Settlement of Disputes 367

J. Cyber Security 369

44. Cyber Security 369

General Conditions of Contract

A. CONTRACT AND INTERPRETATION

1. Definitions

1.1 In this Contract, the following terms shall be interpreted as indicated below.

(a) contract elements

(i) **"Contract"** means the Contract Agreement entered into between the Purchaser and the Supplier, together with the Contract Documents referred to therein. The Contract Agreement and the Contract Documents shall constitute the Contract, and the term "the Contract" shall in all such documents be construed accordingly.

(ii) **"Contract Documents"** means the documents specified in Article 1.1 (Contract Documents) of the Contract Agreement (including any amendments to these Documents).

(iii) **"Contract Agreement"** means the agreement entered into between the Purchaser and the Supplier using the form of Contract Agreement contained in the Sample Contractual Forms Section of the request for proposals documents and any modifications to this form agreed to by the Purchaser and the Supplier. The date of the Contract Agreement shall be recorded in the signed form.

(iv) **"GCC"** means the General Conditions of Contract.

(v) **"SCC"** means the Special Conditions of Contract.

(vi) **"Technical Requirements"** means the Technical Requirements in Section VII of the request for proposals documents.

(vii) **"Implementation Schedule"** means the Implementation Schedule in Section VII of the request for proposals documents.

(viii) **"Contract Price"** means the price or prices defined in Article 2 (Contract Price and Terms of Payment) of the Contract Agreement.

(ix) **"Procurement Regulations"** refers to the edition **specified in the SCC** of the World Bank "Procurement Regulations for IPF Borrowers".

(x) **"**request for proposals **document"** refers to the document issued by the Purchaser on the subject procurement process.

(xi) "**Sexual Exploitation and Abuse" "(SEA)"** means the following:

Sexual Exploitation is defined as any actual or attempted abuse of position of vulnerability, differential power or trust, for sexual purposes, including, but not limited to, profiting monetarily, socially or politically from the sexual exploitation of another.

Sexual Abuse is defined as the actual or threatened physical intrusion of a sexual nature, whether by force or under unequal or coercive conditions.

(xii) **"Sexual Harassment" "(SH)"** is defined as unwelcome sexual advances, requests for sexual favors, and other verbal or physical conduct of a sexual nature by the Supplier's Personnel with other Supplier's or Purchaser's personnel.

(b) entities

(i) **"Purchaser"** means the entity purchasing the Information System, as **specified in the SCC.**

(ii) **"Purchaser's Personnel"** means all staff, labor and other employees of the Project Manager and of the Purchaser engaged in fulfilling the Purchaser's obligations under the Contract; and any other personnel identified as Purchaser's Personnel, by a notice from the Purchaser to the Supplier;

(iii) **"Project Manager"** means the person **named as such in the SCC** or otherwise appointed by the Purchaser in the manner provided in GCC Clause 18.1 (Project Manager) to perform the duties delegated by the Purchaser.

(iv) **"Supplier"** means the firm or Joint Venture whose proposal to **perform** the **Contract** has been accepted by the Purchaser and is named as such in the Contract Agreement.

(v) **"Supplier's Representative"** means any person **nominated** by the Supplier and named as such in the Contract Agreement or otherwise approved by the Purchaser in the manner provided in GCC Clause 18.2 (Supplier's

Representative) to perform the duties delegated by the Supplier.

(vi) **"Supplier's Personnel"** means all personnel whom the Supplier utilizes in the execution of the Contract, including the staff, labor and other employees of the Supplier and each Subcontractor; and any other personnel assisting the Supplier in the execution of the Contract;

(vii) **"Subcontractor"** means any firm to whom any of the obligations of the Supplier, including preparation of any design or supply of any Information Technologies or other Goods or Services, is subcontracted directly or indirectly by the Supplier.

(viii) **"Adjudicator"** means the person named in Appendix 2 of the Contract Agreement, **appointed** by agreement between the Purchaser and the Supplier to make a decision on or to settle any dispute between the Purchaser and the Supplier referred to him or her by the parties, pursuant to GCC Clause 43.1 (Adjudication).

(ix) **"The World Bank"** (also called "The Bank") means the International Bank for Reconstruction and Development (IBRD) or the International Development Association (IDA).

(c) scope

(i) "Information System," also called "the System," means all the Information Technologies, Materials, and other Goods to be supplied, installed, integrated, and made operational (exclusive of the Supplier's Equipment), together with the Services to be carried out by the Supplier under the Contract.

(ii) "Subsystem" means any subset of the System identified as such in the Contract that may be supplied, installed, tested, and commissioned individually before Commissioning of the entire System.

(iii) "Information Technologies" means all information processing and communications-related hardware, Software, supplies, and consumable items that the Supplier is required to supply and install under the Contract.

(iv) "Goods" means all equipment, machinery, furnishings, Materials, and other tangible items that the Supplier is required to supply or supply and install under the Contract, including, without limitation, the Information Technologies and Materials, but excluding the Supplier's Equipment.

(v) "Services" means all technical, logistical, management, and any other Services to be provided by the Supplier under the Contract to supply, install, customize, integrate, and make operational the System. Such Services may include, but are not restricted to, activity management and quality assurance, design, development, customization, documentation, transportation, insurance, inspection, expediting, site preparation, installation, integration, training, data migration, Pre-commissioning, Commissioning, maintenance, and technical support.

(vi) "The Project Plan" means the document to be developed by the Supplier and approved by the Purchaser, pursuant to GCC Clause 19, based on the requirements of the Contract and the Preliminary Project Plan included in the Supplier's proposal. The "Agreed Project Plan" is the version of the Project Plan approved by the Purchaser, in accordance with GCC Clause 19.2. Should the Project Plan conflict with the Contract in any way, the relevant provisions of the Contract, including any amendments, shall prevail.

(vii) "Software" means that part of the System which are instructions that cause information processing Subsystems to perform in a specific manner or execute specific operations.

(viii) "System Software" means Software that provides the operating and management instructions for the underlying hardware and other components, and is identified as such in Appendix 4 of the Contract Agreement and such other Software as the parties may agree in writing to be Systems Software. Such System Software includes, but is not restricted to, micro-code embedded in hardware (i.e., "firmware"), operating systems, communications, system and network management, and utility software.

(ix) "General-Purpose Software" means Software that supports general-purpose office and software development activities and is identified as such in Appendix 4 of the Contract Agreement and such other Software as the parties may agree in writing to be General-Purpose Software. Such General-Purpose Software may include, but is not restricted to, word processing, spreadsheet, generic database management, and application development software.

(x) "Application Software" means Software formulated to perform specific business or technical functions and interface with the business or technical users of the System and is identified as such in Appendix 4 of the Contract Agreement and such other Software as the parties may agree in writing to be Application Software.

(xi) "Standard Software" means Software identified as such in Appendix 4 of the Contract Agreement and such other Software as the parties may agree in writing to be Standard Software.

(xii) "Custom Software" means Software identified as such in Appendix 4 of the Contract Agreement and such other Software as the parties may agree in writing to be Custom Software.

(xiii) "Source Code" means the database structures, dictionaries, definitions, program source files, and any other symbolic representations necessary for the compilation, execution, and subsequent maintenance of the Software (typically, but not exclusively, required for Custom Software).

(xiv) "Materials" means all documentation in printed or printable form and all instructional and informational aides in any form (including audio, video, and text) and on any medium, provided to the Purchaser under the Contract.

(xv) "Standard Materials" means all Materials not specified as Custom Materials.

(xvi) "Custom Materials" means Materials developed by the Supplier at the Purchaser's expense under the Contract and identified as such in Appendix 5 of the Contract Agreement

and such other Materials as the parties may agree in writing to be Custom Materials. Custom Materials includes Materials created from Standard Materials.

(xvii) "Intellectual Property Rights" means any and all copyright, moral rights, trademark, patent, and other intellectual and proprietary rights, title and interests worldwide, whether vested, contingent, or future, including without limitation all economic rights and all exclusive rights to reproduce, fix, adapt, modify, translate, create derivative works from, extract or re-utilize data from, manufacture, introduce into circulation, publish, distribute, sell, license, sublicense, transfer, rent, lease, transmit or provide access electronically, broadcast, display, enter into computer memory, or otherwise use any portion or copy, in whole or in part, in any form, directly or indirectly, or to authorize or assign others to do so.

(xviii) "Supplier's Equipment" means all equipment, tools, apparatus, or things of every kind required in or for installation, completion and maintenance of the System that are to be provided by the Supplier, but excluding the Information Technologies, or other items forming part of the System.

(d) activities

(i) "Delivery" means the transfer of the Goods from the Supplier to the Purchaser in accordance with the current edition Incoterms specified in the Contract.

(ii) "Installation" means that the System or a Subsystem as specified in the Contract is ready for Commissioning as provided in GCC Clause 26 (Installation).

(iii) "Pre-commissioning" means the testing, checking, and any other required activity that may be specified in the Technical Requirements that are to be carried out by the Supplier in preparation for Commissioning of the System as provided in GCC Clause 26 (Installation).

(iv) "Commissioning" means operation of the System or any Subsystem by the Supplier following Installation, which operation is to be

carried out by the Supplier as provided in GCC Clause 27.1 (Commissioning), for the purpose of carrying out Operational Acceptance Test(s).

(v) "Operational Acceptance Tests" means the tests specified in the Technical Requirements and Agreed Project Plan to be carried out to ascertain whether the System, or a specified Subsystem, is able to attain the functional and performance requirements specified in the Technical Requirements and Agreed Project Plan, in accordance with the provisions of GCC Clause 27.2 (Operational Acceptance Test).

(vi) "Operational Acceptance" means the acceptance by the Purchaser of the System (or any Subsystem(s) where the Contract provides for acceptance of the System in parts), in accordance with GCC Clause 27.3 (Operational Acceptance).

(e) place and time

(i) "Purchaser's Country" is the **country named in the SCC.**

(ii) "Supplier's Country" is the country in which the Supplier is legally organized, as named in the Contract Agreement.

(iii) **Unless otherwise specified in the SCC** "Project Site(s)" means the place(s) in the Site Table in the Technical Requirements Section for the supply and installation of the System.

(iv) "Eligible Country" means the countries and territories eligible for participation in procurements financed by the World Bank as defined in the Procurement Regulations.

(v) "Day" means calendar day of the Gregorian Calendar.

(vi) "Week" means seven (7) consecutive Days, beginning the day of the week as is customary in the Purchaser's Country.

(vii) "Month" means calendar month of the Gregorian Calendar.

(viii) "Year" means twelve (12) consecutive Months.

(ix) "Effective Date" means the date of fulfillment of all conditions specified in Article 3 (Effective Date for Determining Time for Achieving Operational Acceptance) of the Contract

Agreement, for the purpose of determining the Delivery, Installation, and Operational Acceptance dates for the System or Subsystem(s).

(x) "Contract Period" is the time period during which this Contract governs the relations and obligations of the Purchaser and Supplier in relation to the System, as **unless otherwise specified in the SCC,** the Contract shall continue in force until the Information System and all the Services have been provided, unless the Contract is terminated earlier in accordance with the terms set out in the Contract**.**

(xi) "Defect Liability Period" (also referred to as the "Warranty Period") means the period of validity of the warranties given by the Supplier commencing at date of the Operational Acceptance Certificate of the System or Subsystem(s), during which the Supplier is responsible for defects with respect to the System (or the relevant Subsystem[s]) as provided in GCC Clause 29 (Defect Liability).

(xii) "The Coverage Period" means the Days of the Week and the hours of those Days during which maintenance, operational, and/or technical support services (if any) must be available.

(xiii) The Post-Warranty Services Period" means the number of years **defined in the SCC** (if any), following the expiration of the Warranty Period during which the Supplier may be obligated to provide Software licenses, maintenance, and/or technical support services for the System, either under this Contract or under separate contract(s).

2. Contract Documents

2.1 Subject to Article 1.2 (Order of Precedence) of the Contract Agreement, all documents forming part of the Contract (and all parts of these documents) are intended to be correlative, complementary, and mutually explanatory. The Contract shall be read as a whole.

3. Interpretation

3.1 Governing Language

3.1.1 **Unless otherwise specified in the SCC**, all Contract Documents and related correspondence exchanged between Purchaser and Supplier shall be written in the language of the request for proposals document (English)**,** and the Contract shall be construed and interpreted in accordance with that language.

3.1.2 If any of the Contract Documents or related correspondence are prepared in a language other than the governing language under GCC Clause 3.1.1 above, the translation of such documents into the governing language shall prevail in matters of interpretation. The originating party, with respect to such documents shall bear the costs and risks of such translation.

3.2 Singular and Plural

The singular shall include the plural and the plural the singular, except where the context otherwise requires.

3.3 Headings

The headings and marginal notes in the GCC are included for ease of reference and shall neither constitute a part of the Contract nor affect its interpretation.

3.4 Persons

Words importing persons or parties shall include firms, corporations, and government entities.

3.5 Incoterms

Unless inconsistent with any provision of the Contract, the meaning of any trade term and the rights and obligations of parties thereunder shall be as prescribed by the Incoterms

Incoterms means international rules for interpreting trade terms published by the International Chamber of Commerce (latest edition), 38 Cours Albert 1er, 75008 Paris, France.

3.6 Entire Agreement

The Contract constitutes the entire agreement between the Purchaser and Supplier with respect to the subject matter of Contract and supersedes all communications, negotiations, and agreements (whether written or oral) of parties with respect to the subject matter of the Contract made prior to the date of Contract.

3.7 Amendment

No amendment or other variation of the Contract shall be effective unless it is in writing, is dated, expressly refers to the Contract, and is signed by a duly authorized representative of each party to the Contract.

3.8 Independent Supplier

The Supplier shall be an independent contractor performing the Contract. The Contract does not create any agency, partnership, joint venture, or other joint relationship between the parties to the Contract.

Subject to the provisions of the Contract, the Supplier shall be solely responsible for the manner in which the Contract is performed. All employees, representatives, or Subcontractors engaged by the Supplier in connection with the performance of the Contract shall be under the complete control of the Supplier and shall not be deemed to be employees of the Purchaser, and nothing contained in the Contract or in any subcontract awarded by the Supplier shall be construed to create any contractual relationship between any such employees, representatives, or Subcontractors and the Purchaser.

3.9 Joint Venture

If the Supplier is a Joint Venture of two or more firms, all such firms shall be jointly and severally bound to the Purchaser for the fulfillment of the provisions of the Contract and shall designate one of such firms to act as a leader with authority to bind the Joint Venture. The composition or constitution of the Joint Venture shall not be altered without the prior consent of the Purchaser.

3.10 Nonwaiver

3.10.1 Subject to GCC Clause 3.10.2 below, no relaxation, forbearance, delay, or indulgence by either party in enforcing any of the terms and conditions of the Contract or the granting of time by either party to the other shall prejudice, affect, or restrict the rights of that party under the Contract, nor shall any waiver by either party of any breach of Contract operate as waiver of any subsequent or continuing breach of Contract.

3.10.2 Any waiver of a party's rights, powers, or remedies under the Contract must be in writing, must be dated and signed by an authorized representative of the party granting such waiver, and must specify the right and the extent to which it is being waived.

3.11 Severability

If any provision or condition of the Contract is prohibited or rendered invalid or unenforceable, such prohibition, invalidity, or unenforceability shall not affect the validity or enforceability of any other provisions and conditions of the Contract.

3.12 Country of Origin

"Origin" means the place where the Information Technologies, Materials, and other Goods for the System were produced or from which the Services are supplied. Goods are produced when, through manufacturing, processing, Software development, or substantial and major

assembly or integration of components, a commercially recognized product results that is substantially different in basic characteristics or in purpose or utility from its components. The Origin of Goods and Services is distinct from the nationality of the Supplier and may be different.

4. Notices

4.1 Unless otherwise stated in the Contract, all notices to be given under the Contract shall be in writing and shall be sent, pursuant to GCC Clause 4.3 below, by personal delivery, airmail post, special courier, facsimile, electronic mail, or other electronic means, with the following provisions.

4.1.1 Any notice sent by facsimile, electronic mail, or EDI shall be confirmed within two (2) days after dispatch by notice sent by airmail post or special courier, except as otherwise specified in the Contract.

4.1.2 Any notice sent by airmail post or special courier shall be deemed (in the absence of evidence of earlier receipt) to have been delivered ten (10) days after dispatch. In proving the fact of dispatch, it shall be sufficient to show that the envelope containing such notice was properly addressed, stamped, and conveyed to the postal authorities or courier service for transmission by airmail or special courier.

4.1.3 Any notice delivered personally or sent by facsimile, electronic mail, or EDI shall be deemed to have been delivered on the date of its dispatch.

4.1.4 Either party may change its postal, facsimile, electronic mail, or EDI addresses for receipt of such notices by ten (10) days' notice to the other party in writing.

4.2 Notices shall be deemed to include any approvals, consents, instructions, orders, certificates, information and other communication to be given under the Contract.

4.3 Pursuant to GCC Clause 18, notices from/to the Purchaser are normally given by, or addressed to, the Project Manager, while notices from/to the Supplier are normally given by, or addressed to, the Supplier's Representative, or in its absence its deputy if any. If there is no appointed Project Manager or Supplier's Representative (or deputy), or if their related authority is limited by the SCC for GCC Clauses 18.1 or 18.2.2, or for any other reason, the Purchaser or Supplier may give and receive notices at their fallback addresses. The address of the Project Manager and the fallback address of the Purchaser are as **specified in the SCC** or as subsequently established/amended. The address of the Supplier's Representative and the fallback address of the

Supplier are as specified in Appendix 1 of the Contract Agreement or as subsequently established/amended.

5. Governing Law

5.1 The Contract shall be governed by and interpreted in accordance with the laws of the country **specified in the SCC**.

5.2 Throughout the execution of the Contract, the Supplier shall comply with the import of goods and services prohibitions in the Purchaser's Country when

(a) as a matter of law or official regulations, the Borrower's country prohibits commercial relations with that country; or

(b) by an act of compliance with a decision of the United Nations Security Council taken under Chapter VII of the Charter of the United Nations, the Borrower's Country prohibits any import of goods from that country or any payments to any country, person, or entity in that country.

6. Fraud and Corruption

6.1 The Bank requires compliance with the Bank's Anti-Corruption Guidelines and its prevailing sanctions policies and procedures as set forth in the WBG's Sanctions Framework, as set forth in the Appendix 1 to the GCC.

6.2 The Purchaser requires the Suppliers to disclose any commissions or fees that may have been paid or are to be paid to agents or any other party with respect to the procurement process or execution of the Contract. The information disclosed must include at least the name and address of the agent or other party, the amount and currency, and the purpose of the commission, gratuity or fee.

B. SUBJECT MATTER OF CONTRACT

7. Scope of the System

7.1 Unless otherwise expressly **limited in the SCC** or Technical Requirements, the Supplier's obligations cover the provision of all Information Technologies, Materials and other Goods as well as the performance of all Services required for the design, development, and implementation (including procurement, quality assurance, assembly, associated site preparation, Delivery, Pre-commissioning, Installation, Testing, and Commissioning) of the System, in accordance with the plans, procedures, specifications, drawings, codes, and any other documents specified in the Contract and the Agreed Project Plan.

7.2 The Supplier shall, unless specifically excluded in the Contract, perform all such work and / or supply all such items and Materials not specifically mentioned in the Contract but

that can be reasonably inferred from the Contract as being required for attaining Operational Acceptance of the System as if such work and / or items and Materials were expressly mentioned in the Contract.

7.3 The Supplier's obligations (if any) to provide Goods and Services as implied by the Recurrent Cost tables of the Supplier's proposal, such as consumables, spare parts, and technical services (e.g., maintenance, technical assistance, and operational support), are as **specified in the SCC,** including the relevant terms, characteristics, and timings.

8. Time for Commencement and Operational Acceptance

8.1 The Supplier shall commence work on the System within the period **specified in the SCC,** and without prejudice to GCC Clause 28.2, the Supplier shall thereafter proceed with the System in accordance with the time schedule specified in the Implementation Schedule and any refinements made in the Agreed Project Plan.

8.2 The Supplier shall achieve Operational Acceptance of the System (or Subsystem(s) where a separate time for Operational Acceptance of such Subsystem(s) is specified in the Contract) in accordance with the time schedule specified in the Implementation Schedule and any refinements made in the Agreed Project Plan, or within such extended time to which the Supplier shall be entitled under GCC Clause 40 (Extension of Time for Achieving Operational Acceptance).

9. Supplier's Responsibilities

9.1 The Supplier shall conduct all activities with due care and diligence, in accordance with the Contract and with the skill and care expected of a competent provider of information technologies, information systems, support, maintenance, training, and other related services, or in accordance with best industry practices. In particular, the Supplier shall provide and employ only technical personnel who are skilled and experienced in their respective callings and supervisory staff who are competent to adequately supervise the work at hand. The Supplier shall ensure that its Subcontractors carryout the work on the Information System in accordance with the Contract, including complying with relevant environmental and social requirements and the obligations set out in GCC Clause 9.9.

The Supplier shall at all times take all reasonable precautions to maintain the health and safety of the Supplier's Personnel employed for the execution of the Contract at the Project Site/s in the Purchaser's country where the Contract is executed.

If **required in the SCC**, the Supplier shall submit to the Purchaser for its approval a health and safety manual which has been specifically prepared for the Contract.

The health and safety manual shall be in addition to any other similar document required under applicable health and safety regulations and laws.

The health and safety manual shall set out any applicable health and safety requirement under the Contract,

(a) which may include:

(i) the procedures to establish and maintain a safe working environment;

(ii) the procedures for prevention, preparedness and response activities to be implemented in the case of an emergency event (i.e. an unanticipated incident, arising from natural or man-made hazards);

(iii) the measures to be taken to avoid or minimize the potential for community exposure to water-borne, water-based, water-related, and vector-borne diseases,

(iv) the measures to be implemented to avoid or minimize the spread of communicable diseases; and

(b) any other requirements stated in the Purchaser's Requirements.

9.2 The Supplier confirms that it has entered into this Contract on the basis of a proper examination of the data relating to the System provided by the Purchaser and on the basis of information that the Supplier could have obtained from a visual inspection of the site (if access to the site was available) and of other data readily available to the Supplier relating to the System as at the date twenty-eight (28) days prior to proposal submission. The Supplier acknowledges that any failure to acquaint itself with all such data and information shall not relieve its responsibility for properly estimating the difficulty or cost of successfully performing the Contract.

9.3 The Supplier shall be responsible for timely provision of all resources, information, and decision making under its control that are necessary to reach a mutually Agreed Project Plan (pursuant to GCC Clause 19.2) within the time schedule specified in the Implementation Schedule. Failure to provide such resources, information, and decision-making may constitute grounds for termination pursuant to GCC Clause 41.2.

9.4 The Supplier shall acquire in its name all permits, approvals, and/or licenses from all local, state, or national government authorities or public service undertakings in the Purchaser's Country that are necessary for the performance of the Contract, including, without limitation, visas for the Supplier's Personnel and entry permits for all imported Supplier's Equipment. The Supplier shall acquire all other permits, approvals, and/or licenses that are not the responsibility of the Purchaser under GCC Clause 10.4 and that are necessary for the performance of the Contract.

9.5 The Supplier shall comply with all laws in force in the Purchaser's Country. The laws will include all national, provincial, municipal, or other laws that affect the performance of the Contract and are binding upon the Supplier. The Supplier shall indemnify and hold harmless the Purchaser from and against any and all liabilities, damages, claims, fines, penalties, and expenses of whatever nature arising or resulting from the violation of such laws by the Supplier or its personnel, including the Subcontractors and their personnel, but without prejudice to GCC Clause 10.1. The Supplier shall not indemnify the Purchaser to the extent that such liability, damage, claims, fines, penalties, and expenses were caused or contributed to by a fault of the Purchaser.

9.6 Any Information Technologies or other Goods and Services that will be incorporated in or be required for the System and other supplies shall have their Origin, as defined in GCC

Clause 3.12, in a country that shall be an Eligible Country, as defined in GCC Clause 1.1 (e) (iv).

9.7 Pursuant to paragraph 2.2 e. of the Appendix 1 to the General Conditions of Contract, the Supplier shall permit and shall cause its agents (where declared or not), subcontractors, subconsultants, service providers, suppliers, and personnel, to permit, the Bank and/or persons appointed by the Bank to inspect the site and/or the accounts, records and other documents relating to the procurement process, selection and/or contract execution, and to have such accounts, records and other documents audited by auditors appointed by the Bank. The Supplier's and its Subcontractors' and subconsultants' attention is drawn to GCC Clause 6.1 (Fraud and Corruption) which provides, inter alia, that acts intended to materially impede the exercise of the Bank's inspection and audit rights constitute a prohibited practice subject to contract termination (as well as to a determination of ineligibility pursuant to the Bank's prevailing sanctions procedures).

9.8 The Supplier shall conform to the sustainable procurement contractual provisions, if and as **specified in the SCC.**

9.9 **Code of Conduct**

The Supplier shall have a Code of Conduct for the Supplier's Personnel employed for the execution of the Contract at the Project Site/s.

The Supplier shall take all necessary measures to ensure that each such personnel is made aware of the Code of Conduct including specific behaviors that are prohibited, and understands the consequences of engaging in such prohibited behaviors.

These measures include providing instructions and documentation that can be understood by such personnel, and seeking to obtain that person's signature acknowledging receipt of such instructions and/or documentation, as appropriate.

The Supplier shall also ensure that the Code of Conduct is visibly displayed in the Project Site/s as well as, as applicable, in areas outside the Project Site/s accessible to the local community and any project affected people. The posted Code of Conduct shall be provided in languages comprehensible to the Supplier's Personnel, Purchaser's Personnel and the local community.

The Supplier's Management Strategy and Implementation Plans, if applicable, shall include appropriate processes for the Supplier to verify compliance with these obligations.

9.10 The Supplier shall, in all dealings with its labor and the labor of its Subcontractors currently employed on or connected with

the Contract, pay due regard to all recognized festivals, official holidays, religious or other customs, and all local laws and regulations pertaining to the employment of labor.

9.11 The Supplier, including its Subcontractors, shall comply with all applicable safety obligations. The Supplier shall at all times take all reasonable precautions to maintain the health and safety of the Supplier's Personnel employed for the execution of Contract at the Project Site/s.

9.12 Training of Supplier's Personnel

The Supplier shall provide appropriate training to relevant Supplier's Personnel on any applicable environmental and social aspect of the Contract, including appropriate sensitization on prohibition of SEA, health and safety.

As stated in the Purchaser's Requirements or as instructed by the Project Manager, the Supplier shall also allow appropriate opportunities for the relevant personnel to be trained on any applicable environmental and social aspects of the Contract by the Purchaser's Personnel and/or other personnel assigned by the Purchaser.

The Supplier shall provide training on SEA and SH, including its prevention, to any of its personnel who has a role to supervise other Supplier's Personnel.

9.13 Stakeholder engagements

The Supplier shall provide relevant contract- related information, as the Purchaser and/or Project Manager may reasonably request to conduct contract stakeholder engagement. "Stakeholder" refers to individuals or groups who:

(a) are affected or likely to be affected by the Contract; and

(b) may have an interest in the Contract.

The Supplier may also directly participate in contract stakeholder engagements, as the Purchaser and/or Project Manager may reasonably request.

9.14 Forced Labor

The Supplier, including its Subcontractors, shall not employ or engage forced labour. Forced labour consists of any work or service, not voluntarily performed, that is exacted from an individual under threat of force or penalty, and includes any kind of involuntary or compulsory labour, such as indentured labour, bonded labour or similar labour-contracting arrangements.

No persons shall be employed or engaged who have been subject to trafficking. Trafficking in persons is defined as the

recruitment, transportation, transfer, harbouring or receipt of persons by means of the threat or use of force or other forms of coercion, abduction, fraud, deception, abuse of power, or of a position of vulnerability, or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purposes of exploitation.

9.15 Child Labor

The Supplier, including its Subcontractors, shall not employ or engage a child under the age of 14 unless the national law specifies a higher age (the minimum age).

The Supplier, including its Subcontractors, shall not employ or engage a child between the minimum age and the age of 18 in a manner that is likely to be hazardous, or to interfere with, the child's education, or to be harmful to the child's health or physical, mental, spiritual, moral, or social development.

The Supplier, including its Subcontractors, shall only employ or engage children between the minimum age and the age of 18 after an appropriate risk assessment has been conducted by the Supplier with the Project Manager's consent. The Supplier shall be subject to regular monitoring by the Project Manager that includes monitoring of health, working conditions and hours of work.

Work considered hazardous for children is work that, by its nature or the circumstances in which it is carried out, is likely to jeopardize the health, safety, or morals of children. Such work activities prohibited for children include work:

(a) with exposure to physical, psychological or sexual abuse;

(b) underground, underwater, working at heights or in confined spaces;

(c) with dangerous machinery, equipment or tools, or involving handling or transport of heavy loads;

(d) in unhealthy environments exposing children to hazardous substances, agents, or processes, or to temperatures, noise or vibration damaging to health; or

(e) under difficult conditions such as work for long hours, during the night or in confinement on the premises of the employer.

9.16 Non-Discrimination and Equal Opportunity

The Supplier shall not make decisions relating to the employment or treatment of personnel for the execution of the Contract on the basis of personal characteristics unrelated to inherent job requirements. The Supplier shall base the

employment of personnel for the execution of the Contract on the principle of equal opportunity and fair treatment, and shall not discriminate with respect to any aspects of the employment relationship, including recruitment and hiring, compensation (including wages and benefits), working conditions and terms of employment, access to training, job assignment, promotion, termination of employment or retirement, and disciplinary practices.

Special measures of protection or assistance to remedy past discrimination or selection for a particular job based on the inherent requirements of the job shall not be deemed discrimination. The Supplier shall provide protection and assistance as necessary to ensure non-discrimination and equal opportunity, including for specific groups such as women, people with disabilities, migrant workers and children (of working age in accordance with GCC Clause 9.15).

9.17 Personnel Grievance Mechanism

The Supplier shall have a grievance mechanism for personnel employed in the execution of the Contract to raise workplace concerns. The grievance mechanism shall be proportionate to the nature, scale, risks and impacts of the Contract. The grievance mechanism may utilize existing grievance mechanisms, provided that they are properly designed and implemented, address concerns promptly, and are readily accessible to such personnel.

9.18 Security of the Project Site

If stated in the SCC, the Supplier shall be responsible for the security at the Project Site/s including providing and maintaining at its own expense all lighting, fencing, and watching when and where necessary for the proper execution and the protection of the locations, or for the safety of the owners and occupiers of adjacent property and for the safety of the public.

In making security arrangements, the Supplier shall be guided by applicable laws and any other requirements that may be stated in the Purchaser's Requirements.

The Supplier shall (i) conduct appropriate background checks on any personnel retained to provide security; (ii) train the security personnel adequately (or determine that they are properly trained) in the use of force (and where applicable, firearms), and appropriate conduct towards the Supplier's Personnel, Purchaser's Personnel and affected communities; and (iii) require the security personnel to act within the applicable Laws and any requirements set out in the Purchaser's Requirements.

The Supplier shall not permit any use of force by security personnel in providing security except when used for preventive and defensive purposes in proportion to the nature and extent of the threat.

9.19 Recruitment of Persons

The Supplier shall not recruit, or attempt to recruit, either on limited time or `permanent basis or through any other contractual agreement, staff and labor from amongst the Purchaser's Personnel.

9.20 **Unless otherwise specified in the SCC** the Supplier shall have no other Supplier responsibilities.

10. Purchaser's Responsibilities

10.1 The Purchaser shall ensure the accuracy of all information and/or data to be supplied by the Purchaser to the Supplier, except when otherwise expressly stated in the Contract.

10.2 The Purchaser shall be responsible for timely provision of all resources, information, and decision making under its control that are necessary to reach an Agreed Project Plan (pursuant to GCC Clause 19.2) within the time schedule specified in the Implementation Schedule. Failure to provide such resources, information, and decision making may constitute grounds for Termination pursuant to GCC Clause 41.3.1 (b).

10.3 The Purchaser shall be responsible for acquiring and providing legal and physical possession of the site and access to it, and for providing possession of and access to all other areas reasonably required for the proper execution of the Contract.

10.4 If requested by the Supplier, the Purchaser shall use its best endeavors to assist the Supplier in obtaining in a timely and expeditious manner all permits, approvals, and/or licenses necessary for the execution of the Contract from all local, state, or national government authorities or public service undertakings that such authorities or undertakings require the Supplier or Subcontractors or the Supplier's Personnel, as the case may be, to obtain.

10.5 In such cases where the responsibilities of specifying and acquiring or upgrading telecommunications and/or electric power services falls to the Supplier, as specified in the Technical Requirements, SCC, Agreed Project Plan, or other parts of the Contract, the Purchaser shall use its best endeavors to assist the Supplier in obtaining such services in a timely and expeditious manner.

10.6 The Purchaser shall be responsible for timely provision of all resources, access, and information necessary for the Installation and Operational Acceptance of the System

(including, but not limited to, any required telecommunications or electric power services), as identified in the Agreed Project Plan, except where provision of such items is explicitly identified in the Contract as being the responsibility of the Supplier. Delay by the Purchaser may result in an appropriate extension of the Time for Operational Acceptance, at the Supplier's discretion.

10.7 Unless otherwise specified in the Contract or agreed upon by the Purchaser and the Supplier, the Purchaser shall provide sufficient, properly qualified operating and technical personnel, as required by the Supplier to properly carry out Delivery, Pre-commissioning, Installation, Commissioning, and Operational Acceptance, at or before the time specified in the Implementation Schedule and the Agreed Project Plan.

10.8 The Purchaser will designate appropriate staff for the training courses to be given by the Supplier and shall make all appropriate logistical arrangements for such training as specified in the Technical Requirements, SCC, the Agreed Project Plan, or other parts of the Contract.

10.9 The Purchaser assumes primary responsibility for the Operational Acceptance Test(s) for the System, in accordance with GCC Clause 27.2, and shall be responsible for the continued operation of the System after Operational Acceptance. However, this shall not limit in any way the Supplier's responsibilities after the date of Operational Acceptance otherwise specified in the Contract.

10.10 The Purchaser is responsible for performing and safely storing timely and regular backups of its data and Software in accordance with accepted data management principles, except where such responsibility is clearly assigned to the Supplier elsewhere in the Contract.

10.11 All costs and expenses involved in the performance of the obligations under this GCC Clause 10 shall be the responsibility of the Purchaser, save those to be incurred by the Supplier with respect to the performance of the Operational Acceptance Test(s), in accordance with GCC Clause 27.2.

10.12 **Unless otherwise specified in the SCC** the Purchaser shall have no other Purchaser responsibilities.

C. PAYMENT

11. Contract Price

11.1 The Contract Price shall be as specified in Article 2 (Contract Price and Terms of Payment) of the Contract Agreement.

11.2 Unless an adjustment clause is **provided for in the SCC,** the Contract Price shall be a firm lump sum not subject to any alteration, except in the event of a Change in the System pursuant to GCC Clause 39 or to other clauses in the Contract;

11.3 The Supplier shall be deemed to have satisfied itself as to the correctness and sufficiency of the Contract Price, which shall, except as otherwise provided for in the Contract, cover all its obligations under the Contract.

12. Terms of Payment

12.1 The Supplier's request for payment shall be made to the Purchaser in writing, accompanied by an invoice describing, as appropriate, the System or Subsystem(s), Delivered, Pre-commissioned, Installed, and Operationally Accepted, and by documents submitted pursuant to GCC Clause 22.5 and upon fulfillment of other obligations stipulated in the Contract.

The Contract Price shall be paid as **specified in the SCC.**

12.2 No payment made by the Purchaser herein shall be deemed to constitute acceptance by the Purchaser of the System or any Subsystem(s).

12.3 Payments shall be made promptly by the Purchaser, but in no case later than forty five (45) days after submission of a valid invoice by the Supplier. In the event that the Purchaser fails to make any payment by its respective due date or within the period set forth in the Contract, the Purchaser shall pay to the Supplier interest on the amount of such delayed payment at the rate(s) **specified in the SCC** for the period of delay until payment has been made in full, whether before or after judgment or arbitration award.

12.4 Payments shall be made in the currency(ies) specified in the Contract Agreement, pursuant to GCC Clause 11. For Goods and Services supplied locally, payments shall be made **as specified in the SCC.**

12.5 **Unless otherwise specified in the SCC,** payment of the foreign currency portion of the Contract Price for Goods supplied from outside the Purchaser's Country shall be made to the Supplier through an irrevocable letter of credit opened by an authorized bank in the Supplier's Country and will be payable on presentation of the appropriate

documents. It is agreed that the letter of credit will be subject to Article 10 of the latest revision of *Uniform Customs and Practice for Documentary Credits*, published by the International Chamber of Commerce, Paris.

12.6 **As specified in the SCC**, if the Supplier fails to perform its cyber security obligations under the Contract, an assessed amount, as determined by the Project Manager, may be withheld until the obligation has been performed.

13. Securities

13.1 Issuance of Securities

The Supplier shall provide the securities specified below in favor of the Purchaser at the times and in the amount, manner, and form specified below.

13.2 Advance Payment Security

13.2.1 The Supplier shall provide within twenty-eight (28) days of the notification of Contract award an Advance Payment Security in the amount and currency of the Advance Payment specified in SCC for GCC Clause 12.1 above and valid until the System is Operationally Accepted.

13.2.2 The security shall be in the form provided in the request for proposal document or in another form acceptable to the Purchaser. The amount of the security shall be reduced in proportion to the value of the System executed by and paid to the Supplier from time to time and shall automatically become null and void when the full amount of the advance payment has been recovered by the Purchaser. **Unless otherwise specified in the SCC,** the reduction in value and expiration of the Advance Payment Security are calculated as follows:

P*a/(100-a), where "P" is the sum of all payments effected so far to the Supplier (excluding the Advance Payment), and "a" is the Advance Payment expressed as a percentage of the Contract Price pursuant to the SCC for GCC Clause 12.1.

The security shall be returned to the Supplier immediately after its expiration.

13.3 Performance Security

13.3.1 The Supplier shall, within twenty-eight (28) days of the notification of Contract award, provide a security for the due performance of the Contract in the amount and currency **specified in the SCC.**

13.3.2 The security shall be a bank guarantee in the form provided in the Sample Contractual Forms Section of

the request for proposal document, or it shall be in another form acceptable to the Purchaser.

13.3.3 The security shall automatically become null and void once all the obligations of the Supplier under the Contract have been fulfilled, including, but not limited to, any obligations during the Warranty Period and any extensions to the period. The security shall be returned to the Supplier no later than twenty-eight (28) days after its expiration.

13.3.4 Upon Operational Acceptance of the entire System, the security shall be reduced to the amount **specified in the SCC,** on the date of the Operational Acceptance, so that the reduced security would only cover the remaining warranty obligations of the Supplier.

14. Taxes and Duties

14.1 For Goods or Services supplied from outside the Purchaser's country, the Supplier shall be entirely responsible for all taxes, stamp duties, license fees, and other such levies imposed outside the Purchaser's country. Any duties, such as importation or customs duties, and taxes and other levies, payable in the Purchaser's country for the supply of Goods and Services from outside the Purchaser's country are the responsibility of the Purchaser unless these duties or taxes have been made part of the Contract Price in Article 2 of the Contract Agreement and the Price Schedule it refers to, in which case the duties and taxes will be the Supplier's responsibility.

14.2 For Goods or Services supplied locally, the Supplier shall be entirely responsible for all taxes, duties, license fees, etc., incurred until delivery of the contracted Goods or Services to the Purchaser. The only exception are taxes or duties, such as value-added or sales tax or stamp duty as apply to, or are clearly identifiable, on the invoices and provided they apply in the Purchaser's country, and only if these taxes, levies and/or duties are also excluded from the Contract Price in Article 2 of the Contract Agreement and the Price Schedule it refers to.

14.3 If any tax exemptions, reductions, allowances, or privileges may be available to the Supplier in the Purchaser's Country, the Purchaser shall use its best efforts to enable the Supplier to benefit from any such tax savings to the maximum allowable extent.

14.4 For the purpose of the Contract, it is agreed that the Contract Price specified in Article 2 (Contract Price and Terms of Payment) of the Contract Agreement is based on the taxes, duties, levies, and charges prevailing at the date twenty-eight (28) days prior to the date of proposal

submission in the Purchaser's Country (also called "Tax" in this GCC Clause 14.4). If any Tax rates are increased or decreased, a new Tax is introduced, an existing Tax is abolished, or any change in interpretation or application of any Tax occurs in the course of the performance of the Contract, which was or will be assessed on the Supplier, its Subcontractors, or their employees in connection with performance of the Contract, an equitable adjustment to the Contract Price shall be made to fully take into account any such change by addition to or reduction from the Contract Price, as the case may be.

D. INTELLECTUAL PROPERTY

15. Copyright

15.1 The Intellectual Property Rights in all Standard Software and Standard Materials shall remain vested in the owner of such rights.

15.2 The Purchaser agrees to restrict use, copying, or duplication of the Standard Software and Standard Materials in accordance with GCC Clause 16, except that additional copies of Standard Materials may be made by the Purchaser for use within the scope of the project of which the System is a part, in the event that the Supplier does not deliver copies within thirty (30) days from receipt of a request for such Standard Materials.

15.3 The Purchaser's contractual rights to use the Standard Software or elements of the Standard Software may not be assigned, licensed, or otherwise transferred voluntarily except in accordance with the relevant license agreement or **unless otherwise specified in the SCC** to a legally constituted successor organization (e.g., a reorganization of a public entity formally authorized by the government or through a merger or acquisition of a private entity)**.**

15.4 **Unless otherwise specified in the SCC,** the Intellectual Property Rights in all Custom Software and Custom Materials specified in Appendices 4 and 5 of the Contract Agreement (if any) shall, at the date of this Contract or on creation of the rights (if later than the date of this Contract), vest in the Purchaser. The Supplier shall do and execute or arrange for the doing and executing of each necessary act, document, and thing (as legally sufficient) that the Purchaser may consider necessary or desirable to perfect the right, title, and interest of the Purchaser in and to those rights. In respect of such Custom Software and Custom Materials, the Supplier shall ensure that the holder of a moral right in such an item does not assert it, and the Supplier shall, if requested to do so by the Purchaser and

where permitted by applicable law, ensure that the holder of such a moral right waives it.

15.5 **Unless otherwise specified in the SCC**, escrow arrangements shall NOT be required.

16. Software License Agreements

16.1 Except to the extent that the Intellectual Property Rights in the Software vest in the Purchaser, the Supplier hereby grants to the Purchaser license to access and use the Software, including all inventions, designs, and marks embodied in the Software.

Such license to access and use the Software shall:

(a) be:

(i) nonexclusive;

(ii) fully paid up and irrevocable (except that it shall terminate if the Contract terminates under GCC Clauses 41.1 or 41.3);

(iii) **unless otherwise specified in the SCC** valid throughout the territory of the Purchaser's Country;

(iv) **unless otherwise specified in the SCC** subject to NO additional restrictions.

(b) permit the Software to be:

(i) used or copied for use on or with the computer(s) for which it was acquired (if specified in the Technical Requirements and/or the Supplier's proposal), plus a backup computer(s) of the same or similar capacity, if the primary is(are) inoperative, and during a reasonable transitional period when use is being transferred between primary and backup;

(ii) used or copied for use on or transferred to a replacement computer(s), (and use on the original and replacement computer(s) may be simultaneous during a reasonable transitional period) provided that, if the Technical Requirements and/or the Supplier's proposal specifies a class of computer to which the license is restricted, the replacement computer(s) is(are) within that class;

(iii) if the nature of the System is such as to permit such access, accessed from other computers connected to the primary and/or backup computer(s) by means of a local or wide-area network or similar arrangement, and used on or copied for use on

those other computers to the extent necessary to that access;

(iv) reproduced for safekeeping or backup purposes;

(v) customized, adapted, or combined with other computer software for use by the Purchaser, provided that derivative software incorporating any substantial part of the delivered, restricted Software shall be subject to same restrictions as are set forth in this Contract;

(vi) **unless otherwise specified in the SCC,** disclosed to, and reproduced for use by, support service suppliers and their subcontractors, to the extent reasonably necessary to the performance of their support service contracts, subject to the same restrictions as are set forth in this Contract; and

(vii) **unless otherwise specified in the SCC** disclosed to, and reproduced for use by, NO other parties.

16.2 The Supplier has the right to audit the Standard Software to verify compliance with the above license agreements. **Unless otherwise specified in the SCC**, the Purchaser will make available to the Supplier, within seven (7) days of a written request, accurate and up-to-date records of the number and location of copies, the number of authorized users, or any other relevant data required to demonstrate use of the Standard Software as per the license agreement. If and only if, expressly agreed in writing between the Purchaser and the Supplier, Purchaser will allow, under a pre-specified agreed procedure, the execution of embedded software functions under Supplier's control, and unencumbered transmission of resulting information on software usage.

17. Confidential Information

17.1 **Unless otherwise specified in the SCC,** the "Receiving Party" (either the Purchaser or the Supplier) shall keep confidential and shall not, without the written consent of the other party to this Contract ("the Disclosing Party"), divulge to any third party any documents, data, or other information of a confidential nature ("Confidential Information") connected with this Contract, and furnished directly or indirectly by the Disclosing Party prior to or during performance, or following termination, of this Contract.

17.2 For the purposes of GCC Clause 17.1, the Supplier is also deemed to be the Receiving Party of Confidential Information generated by the Supplier itself in the course of the performance of its obligations under the Contract and

relating to the businesses, finances, suppliers, employees, or other contacts of the Purchaser or the Purchaser's use of the System.

17.3 Notwithstanding GCC Clauses 17.1 and 17.2:

(a) the Supplier may furnish to its Subcontractor Confidential Information of the Purchaser to the extent reasonably required for the Subcontractor to perform its work under the Contract; and

(b) the Purchaser may furnish Confidential Information of the Supplier: (i) to its support service suppliers and their subcontractors to the extent reasonably required for them to perform their work under their support service contracts; and (ii) to its affiliates and subsidiaries,

in which event the Receiving Party shall ensure that the person to whom it furnishes Confidential Information of the Disclosing Party is aware of and abides by the Receiving Party's obligations under this GCC Clause 17 as if that person were party to the Contract in place of the Receiving Party.

17.4 The Purchaser shall not, without the Supplier's prior written consent, use any Confidential Information received from the Supplier for any purpose other than the operation, maintenance and further development of the System. Similarly, the Supplier shall not, without the Purchaser's prior written consent, use any Confidential Information received from the Purchaser for any purpose other than those that are required for the performance of the Contract.

17.5 The obligation of a party under GCC Clauses 17.1 through 17.4 above, however, shall not apply to that information which:

(a) now or hereafter enters the public domain through no fault of the Receiving Party;

(b) can be proven to have been possessed by the Receiving Party at the time of disclosure and that was not previously obtained, directly or indirectly, from the Disclosing Party;

(c) otherwise lawfully becomes available to the Receiving Party from a third party that has no obligation of confidentiality;

(d) is being provided to the Bank.

17.6 The above provisions of this GCC Clause 17 shall not in any way modify any undertaking of confidentiality given

by either of the parties to this Contract prior to the date of the Contract in respect of the System or any part thereof.

17.7 **Unless otherwise specified in the SCC**, the provisions of this GCC Clause 17 shall survive the termination, for whatever reason, of the Contract for three (3) years.

E. SUPPLY, INSTALLATION, TESTING, COMMISSIONING, AND ACCEPTANCE OF THE SYSTEM

18. Representatives

18.1 Project Manager

If the Project Manager is not named in the Contract, then within fourteen (14) days of the Effective Date, the Purchaser shall appoint and notify the Supplier in writing of the name of the Project Manager. The Purchaser may from time to time appoint some other person as the Project Manager in place of the person previously so appointed and shall give a notice of the name of such other person to the Supplier without delay. No such appointment shall be made at such a time or in such a manner as to impede the progress of work on the System. Such appointment shall take effect only upon receipt of such notice by the Supplier. **Unless otherwise specified in the SCC** (if any), the Project Manager shall have the authority to represent the Purchaser on all day-to-day matters relating to the System or arising from the Contract, and shall normally be the person giving or receiving notices on behalf of the Purchaser pursuant to GCC Clause 4.

18.2 Supplier's Representative

18.2.1 If the Supplier's Representative is not named in the Contract, then within fourteen (14) days of the Effective Date, the Supplier shall appoint the Supplier's Representative and shall request the Purchaser in writing to approve the person so appointed. The request must be accompanied by a detailed curriculum vitae for the nominee, as well as a description of any other System or non-System responsibilities the nominee would retain while performing the duties of the Supplier's Representative. If the Purchaser does not object to the appointment within fourteen (14) days, the Supplier's Representative shall be deemed to have been approved. If the Purchaser objects to the appointment within fourteen (14) days giving the reason therefor, then the Supplier shall appoint a replacement within fourteen (14) days of such objection in accordance with this GCC Clause 18.2.1.

18.2.2 **Unless otherwise specified in the SCC** (if any), the Supplier's Representative shall have the authority to represent the Supplier on all day-to-day matters relating to the System or arising from the Contract, and shall normally be the person giving or receiving notices on behalf of the Supplier pursuant to GCC Clause 4.

18.2.3 The Supplier shall not revoke the appointment of the Supplier's Representative without the Purchaser's prior written consent, which shall not be unreasonably withheld. If the Purchaser consents to such an action, the Supplier shall appoint another person of equal or superior qualifications as the Supplier's Representative, pursuant to the procedure set out in GCC Clause 18.2.1.

18.2.4 The Supplier's Representative and staff are obliged to work closely with the Purchaser's Project Manager and staff, act within their own authority, and abide by directives issued by the Purchaser that are consistent with the terms of the Contract. The Supplier's Representative is responsible for managing the activities of the Supplier's Personnel.

18.2.5 The Supplier's Representative may, subject to the approval of the Purchaser (which shall not be unreasonably withheld), at any time delegate to any person any of the powers, functions, and authorities vested in him or her. Any such delegation may be revoked at any time. Any such delegation or revocation shall be subject to a prior notice signed by the Supplier's Representative and shall specify the powers, functions, and authorities thereby delegated or revoked. No such delegation or revocation shall take effect unless and until the notice of it has been delivered.

18.2.6 Any act or exercise by any person of powers, functions and authorities so delegated to him or her in accordance with GCC Clause 18.2.5 shall be deemed to be an act or exercise by the Supplier's Representative.

18.3 Removal of Supplier's Personnel

18.3.1 The Project Manager may require the Supplier to remove (or cause to be removed) the Supplier's Representative or any other person employed by the Supplier in the execution of the Contract, who:

(a) persists in any misconduct or lack of care;

(b) carries out duties incompetently or negligently;

(c) fails to comply with any provision of the Contract;

(d) persists in any conduct which is prejudicial to safety, health, or the protection of the environment;

(e) based on reasonable evidence, is determined to have engaged in Fraud and Corruption during the execution of the Contract;

(f) has been recruited from the Purchaser's Personnel;

(g) engages in any other behaviour which breaches the Code of Conduct, as applicable;

If appropriate, the Supplier shall then promptly appoint (or cause to be appointed) a suitable replacement with equivalent skills and experience.

Notwithstanding any requirement from the Project Manager to remove or cause to remove any person, the Supplier shall take immediate action as appropriate in response to any violation of (a) through (g) above. Such immediate action shall include removing (or causing to be removed) from work on the System, any person Employed by the Supplier in the execution of the Contract who engages in (a), (b), (c), (d), (e) or (g) above or has been recruited as stated in (f) above.

18.3.2 If any representative or person employed by the Supplier is removed in accordance with GCC Clause 18.3.1, the Supplier shall, where required, promptly appoint a suitable replacement with equivalent skills and experience.

19. Project Plan

19.1 In close cooperation with the Purchaser and based on the Preliminary Project Plan included in the Supplier's proposal, the Supplier shall develop a Project Plan encompassing the activities specified in the Contract. The contents of the Project Plan shall be as **specified in the SCC** and/or Technical Requirements.

19.2 **Unless otherwise specified in the SCC**, within thirty (30) days from the Effective Date of the Contract, the Supplier shall present a Project Plan to the Purchaser. Such submission to the Purchaser shall include any applicable environmental and social management plan to manage environmental and social risks and impacts. The Purchaser shall, within fourteen (14) days of receipt of the Project Plan, notify the Supplier of any respects in which it considers that the Project Plan does not adequately ensure that the proposed program of work, proposed methods, and/or proposed Information Technologies will satisfy the Technical Requirements and/or the SCC (in this Clause

19.2 called "non-conformities" below). The Supplier shall, within five (5) days of receipt of such notification, correct the Project Plan and resubmit to the Purchaser. The Purchaser shall, within five (5) days of resubmission of the Project Plan, notify the Supplier of any remaining non-conformities. This procedure shall be repeated as necessary until the Project Plan is free from non-conformities. When the Project Plan is free from non-conformities, the Purchaser shall provide confirmation in writing to the Supplier. This approved Project Plan ("the Agreed Project Plan") shall be contractually binding on the Purchaser and the Supplier.

19.3 If required, the impact on the Implementation Schedule of modifications agreed during finalization of the Agreed Project Plan shall be incorporated in the Contract by amendment, in accordance with GCC Clauses 39 and 40.

19.4 The Supplier shall undertake to supply, install, test, and commission the System in accordance with the Agreed Project Plan and the Contract.

19.5 **Unless otherwise specified in the SCC**, the Supplier shall submit to the Purchaser Monthly Progress Reports summarizing:

(i) results accomplished during the prior period;

(ii) cumulative deviations to date from schedule of progress milestones as specified in the Agreed Project Plan;

(iii) corrective actions to be taken to return to planned schedule of progress; proposed revisions to planned schedule;

(iv) other issues and outstanding problems; proposed actions to be taken;

(v) resources that the Supplier expects to be provided by the Purchaser and/or actions to be taken by the Purchaser in the next reporting period;

(vi) status of compliance to environmental and social requirements, as applicable;

(vii) other issues or potential problems the Supplier foresees that could impact on project progress and/or effectiveness.

19.6 The Supplier shall submit to the Purchaser other (periodic) reports as specified in the SCC.

19.7 Immediate Reporting requirement

The Supplier shall inform the Project Manager immediately of any allegation, incident or accident in

Project Site/s, which has or is likely to have a significant adverse effect on the environment, the affected communities, the public, Purchaser's Personnel or Supplier's Personnel. This includes, but is not limited to, any incident or accident causing fatality or serious injury; significant adverse effects or damage to private property; any cyber security incidents as **specified in the SCC**; or any allegation of SEA and/or SH. In case of SEA and/or SH, while maintaining confidentiality as appropriate, the type of allegation (sexual exploitation, sexual abuse or sexual harassment), gender and age of the person who experienced the alleged incident should be included in the information.

The Supplier, upon becoming aware of the allegation, incident or accident, shall also immediately inform the Purchaser of any such incident or accident on the Subcontractors' or suppliers' premises relating to the Contract which has or is likely to have a significant adverse effect on the environment, the affected communities, the public, Purchaser's Personnel or Supplier's Personnel. The notification shall provide sufficient detail regarding such incidents or accidents.

The Supplier shall provide full details of such incidents or accidents to the Project Manager within the timeframe agreed with the Purchaser.

The Purchaser shall require its Subcontractors to immediately notify it of any incidents or accidents referred to in this Sub- Clause.

20. Subcontracting 20.1 Appendix 3 (List of Approved Subcontractors) to the Contract Agreement specifies critical items of supply or services and a list of Subcontractors for each item that are considered acceptable by the Purchaser. If no Subcontractors are listed for an item, the Supplier shall prepare a list of Subcontractors it considers qualified and wishes to be added to the list for such items. The Supplier may from time to time propose additions to or deletions from any such list. The Supplier shall submit any such list or any modification to the list to the Purchaser for its approval in sufficient time so as not to impede the progress of work on the System. Submision by the Supplier, for addition of any Subcontractor not named in the Contract, shall also include the Subcontractor's declaration in accordance with Appendix 2 to the GCC- Sexual exploitation and Abuse (SEA) and/or Sexual Harassment (SH) Performance Declaration. Approval by the Purchaser of a Subcontractor(s) shall not relieve the Supplier from

any of its obligations, duties, or responsibilities under the Contract.

20.2 The Supplier may, at its discretion, select and employ Subcontractors for such critical items from those Subcontractors listed pursuant to GCC Clause 20.1. If the Supplier wishes to employ a Subcontractor not so listed, or subcontract an item not so listed, it must seek the Purchaser's prior approval under GCC Clause 20.3.

20.3 For items for which pre-approved Subcontractor lists have not been specified in Appendix 3 to the Contract Agreement, the Supplier may employ such Subcontractors as it may select, provided: (i) the Supplier notifies the Purchaser in writing at least twenty-eight (28) days prior to the proposed mobilization date for such Subcontractor, including by providing the Subcontractor's declaration in accordance with Appendix 2 to the GCC- Sexual exploitation and Abuse (SEA) and/or Sexual Harassment (SH) Performance Declaration; and (ii) by the end of this period either the Purchaser has granted its approval in writing or fails to respond. The Supplier shall not engage any Subcontractor to which the Purchaser has objected in writing prior to the end of the notice period. The absence of a written objection by the Purchaser during the above specified period shall constitute formal acceptance of the proposed Subcontractor. Except to the extent that it permits the deemed approval of the Purchaser of Subcontractors not listed in the Contract Agreement, nothing in this Clause, however, shall limit the rights and obligations of either the Purchaser or Supplier as they are specified in GCC Clauses 20.1 and 20.2, or in Appendix 3 of the Contract Agreement.

20.4 The Supplier shall ensure that its Subcontractors comply with the relevant ES requirements and the obligations set out in GCC Clause 9.9.

21. Design and Engineering

21.1 Technical Specifications and Drawings

21.1.1 The Supplier shall execute the basic and detailed design and the implementation activities necessary for successful installation of the System in compliance with the provisions of the Contract or, where not so specified, in accordance with good industry practice.

The Supplier shall be responsible for any discrepancies, errors or omissions in the specifications, drawings, and other technical documents that it has prepared, whether such specifications, drawings, and other documents have been approved by the Project Manager or not, provided that such discrepancies, errors, or omissions

are not because of inaccurate information furnished in writing to the Supplier by or on behalf of the Purchaser.

21.1.2 The Supplier shall be entitled to disclaim responsibility for any design, data, drawing, specification, or other document, or any modification of such design, drawings, specification, or other documents provided or designated by or on behalf of the Purchaser, by giving a notice of such disclaimer to the Project Manager.

21.2 Codes and Standards

Wherever references are made in the Contract to codes and standards in accordance with which the Contract shall be executed, the edition or the revised version of such codes and standards current at the date twenty-eight (28) days prior to date of proposal submission shall apply. During Contract execution, any changes in such codes and standards shall be applied after approval by the Purchaser and shall be treated in accordance with GCC Clause 39.3.

21.3 Approval/Review of Controlling Technical Documents by the Project Manager

21.3.1 **Unless otherwise specified in the SCC**, there will NO Controlling Technical Documents required. However, **if the SCC specifies** Controlling Technical Documents, the Supplier shall prepare and furnish such documents for the Project Manager's approval or review.

Any part of the System covered by or related to the documents to be approved by the Project Manager shall be executed only after the Project Manager's approval of these documents.

GCC Clauses 21.3.2 through 21.3.7 shall apply to those documents requiring the Project Manager's approval, but not to those furnished to the Project Manager for its review only.

21.3.2 Within fourteen (14) days after receipt by the Project Manager of any document requiring the Project Manager's approval in accordance with GCC Clause 21.3.1, the Project Manager shall either return one copy of the document to the Supplier with its approval endorsed on the document or shall notify the Supplier in writing of its disapproval of the document and the reasons for disapproval and the modifications that the Project Manager proposes. If the Project Manager fails to take such action within the fourteen (14) days, then the document shall be deemed to have been approved by the Project Manager.

21.3.3 The Project Manager shall not disapprove any document except on the grounds that the document does not comply with some specified provision of the Contract or that it is contrary to good industry practice.

21.3.4 If the Project Manager disapproves the document, the Supplier shall modify the document and resubmit it for the Project Manager's approval in accordance with GCC Clause 21.3.2. If the Project Manager approves the document subject to modification(s), the Supplier shall make the required modification(s), and the document shall then be deemed to have been approved, subject to GCC Clause 21.3.5. The procedure set out in GCC Clauses 21.3.2 through 21.3.4 shall be repeated, as appropriate, until the Project Manager approves such documents.

21.3.5 If any dispute occurs between the Purchaser and the Supplier in connection with or arising out of the disapproval by the Project Manager of any document and/or any modification(s) to a document that cannot be settled between the parties within a reasonable period, then, in case the Contract Agreement includes and names an Adjudicator, such dispute may be referred to the Adjudicator for determination in accordance with GCC Clause 43.1 (Adjudication). If such dispute is referred to an Adjudicator, the Project Manager shall give instructions as to whether and if so, how, performance of the Contract is to proceed. The Supplier shall proceed with the Contract in accordance with the Project Manager's instructions, provided that if the Adjudicator upholds the Supplier's view on the dispute and if the Purchaser has not given notice under GCC Clause 43.1.2, then the Supplier shall be reimbursed by the Purchaser for any additional costs incurred by reason of such instructions and shall be relieved of such responsibility or liability in connection with the dispute and the execution of the instructions as the Adjudicator shall decide, and the Time for Achieving Operational Acceptance shall be extended accordingly.

21.3.6 The Project Manager's approval, with or without modification of the document furnished by the Supplier, shall not relieve the Supplier of any responsibility or liability imposed upon it by any provisions of the Contract except to the extent that any subsequent failure results from modifications required by the Project Manager or inaccurate information furnished in writing to the Supplier by or on behalf of the Purchaser.

21.3.7 The Supplier shall not depart from any approved document unless the Supplier has first submitted to the Project Manager an amended document and obtained the Project Manager's approval of the document, pursuant to the provisions of this GCC Clause 21.3. If the Project Manager requests any change in any already approved document and/or in any document based on such an approved document, the provisions of GCC Clause 39 (Changes to the System) shall apply to such request.

22. Procurement, Delivery, and Transport

22.1 Subject to related Purchaser's responsibilities pursuant to GCC Clauses 10 and 14, the Supplier shall manufacture or procure and transport all the Information Technologies, Materials, and other Goods in an expeditious and orderly manner to the Project Site.

22.2 Delivery of the Information Technologies, Materials, and other Goods shall be made by the Supplier in accordance with the Technical Requirements.

22.3 Early or partial deliveries require the explicit written consent of the Purchaser, which consent shall not be unreasonably withheld.

22.4 Transportation

22.4.1 The Supplier shall provide such packing of the Goods as is required to prevent their damage or deterioration during shipment. The packing, marking, and documentation within and outside the packages shall comply strictly with the Purchaser's instructions to the Supplier.

22.4.2 The Supplier will bear responsibility for and cost of transport to the Project Sites in accordance with the terms and conditions used in the specification of prices in the Price Schedules, including the terms and conditions of the associated Incoterms.

22.4.3 **Unless otherwise specified in the SCC,** the Supplier shall be free to use transportation through carriers registered in any eligible country and to obtain insurance from any eligible source country.

22.5 **Unless otherwise specified in the SCC,** the Supplier will provide the Purchaser with shipping and other documents, as specified below:

22.5.1 For Goods supplied from outside the Purchaser's Country:

Upon shipment, the Supplier shall notify the Purchaser and the insurance company contracted by the Supplier to provide cargo insurance by cable, facsimile,

electronic mail, or EDI with the full details of the shipment. The Supplier shall promptly send the following documents to the Purchaser by mail or courier, as appropriate, with a copy to the cargo insurance company:

(a) two copies of the Supplier's invoice showing the description of the Goods, quantity, unit price, and total amount;

(b) usual transportation documents;

(c) insurance certificate;

(d) certificate(s) of origin; and

(e) estimated time and point of arrival in the Purchaser's Country and at the site.

22.5.2 For Goods supplied locally (i.e., from within the Purchaser's country):

Upon shipment, the Supplier shall notify the Purchaser by cable, facsimile, electronic mail, or EDI with the full details of the shipment. The Supplier shall promptly send the following documents to the Purchaser by mail or courier, as appropriate:

(a) two copies of the Supplier's invoice showing the Goods' description, quantity, unit price, and total amount;

(b) delivery note, railway receipt, or truck receipt;

(c) certificate of insurance;

(d) certificate(s) of origin; and

(e) estimated time of arrival at the site.

22.6 Customs Clearance

(a) The Purchaser will bear responsibility for, and cost of, customs clearance into the Purchaser's country in accordance the particular Incoterm(s) used for Goods supplied from outside the Purchaser's country in the Price Schedules referred to by Article 2 of the Contract Agreement.

(b) At the request of the Purchaser, the Supplier will make available a representative or agent during the process of customs clearance in the Purchaser's country for goods supplied from outside the Purchaser's country. In the event of delays in customs clearance that are not the fault of the Supplier:

(i) the Supplier shall be entitled to an extension in the Time for Achieving Operational Acceptance, pursuant to GCC Clause 40;

(ii) the Contract Price shall be adjusted to compensate the Supplier for any additional storage charges that the Supplier may incur as a result of the delay.

23. Product Upgrades

23.1 At any point during performance of the Contract, should technological advances be introduced by the Supplier for Information Technologies originally offered by the Supplier in its proposal and still to be delivered, the Supplier shall be obligated to offer to the Purchaser the latest versions of the available Information Technologies having equal or better performance or functionality at the same or lesser unit prices, pursuant to GCC Clause 39 (Changes to the System).

23.2 At any point during performance of the Contract, for Information Technologies still to be delivered, the Supplier will also pass on to the Purchaser any cost reductions and additional and/or improved support and facilities that it offers to other clients of the Supplier in the Purchaser's Country, pursuant to GCC Clause 39 (Changes to the System).

23.3 During performance of the Contract, the Supplier shall offer to the Purchaser all new versions, releases, and updates of Standard Software, as well as related documentation and technical support services, within thirty (30) days of their availability from the Supplier to other clients of the Supplier in the Purchaser's Country, and no later than twelve (12) months after they are released in the country of origin. In no case will the prices for these Software exceed those quoted by the Supplier in the Recurrent Costs tables in its proposal.

23.4 **Unless otherwise specified in the SCC,** during the Warranty Period, the Supplier will provide at no additional cost to the Purchaser all new versions, releases, and updates for all Standard Software that are used in the System, within thirty (30) days of their availability from the Supplier to other clients of the Supplier in the Purchaser's country, and no later than twelve (12) months after they are released in the country of origin of the Software.

23.5 The Purchaser shall introduce all new versions, releases or updates of the Software within eighteen (18) months of receipt of a production-ready copy of the new version, release, or update, provided that the new version, release, or update does not adversely affect System operation or

performance or require extensive reworking of the System. In cases where the new version, release, or update adversely affects System operation or performance, or requires extensive reworking of the System, the Supplier shall continue to support and maintain the version or release previously in operation for as long as necessary to allow introduction of the new version, release, or update. In no case shall the Supplier stop supporting or maintaining a version or release of the Software less than twenty four (24) months after the Purchaser receives a production-ready copy of a subsequent version, release, or update. The Purchaser shall use all reasonable endeavors to implement any new version, release, or update as soon as practicable, subject to the twenty-four-month-long stop date.

24. Implementation, Installation, and Other Services

24.1 The Supplier shall provide all Services specified in the Contract and Agreed Project Plan in accordance with the highest standards of professional competence and integrity.

24.2 Prices charged by the Supplier for Services, if not included in the Contract, shall be agreed upon in advance by the parties (including, but not restricted to, any prices submitted by the Supplier in the Recurrent Cost Schedules of its proposal) and shall not exceed the prevailing rates charged by the Supplier to other purchasers in the Purchaser's Country for similar services.

25. Inspections and Tests

25.1 The Purchaser or its representative shall have the right to inspect and/or test any components of the System, as specified in the Technical Requirements, to confirm their good working order and/or conformity to the Contract at the point of delivery and/or at the Project Site.

25.2 The Purchaser or its representative shall be entitled to attend any such inspections and/or tests of the components, provided that the Purchaser shall bear all costs and expenses incurred in connection with such attendance, including but not limited to all inspection agent fees, travel, and related expenses.

25.3 Should the inspected or tested components fail to conform to the Contract, the Purchaser may reject the component(s), and the Supplier shall either replace the rejected component(s), or make alterations as necessary so that it meets the Contract requirements free of cost to the Purchaser.

25.4 The Project Manager may require the Supplier to carry out any inspection and/or test not specified in the Contract, provided that the Supplier's reasonable costs and expenses incurred in the carrying out of such inspection and/or test

shall be added to the Contract Price. Further, if such inspection and/or test impedes the progress of work on the System and/or the Supplier's performance of its other obligations under the Contract, due allowance will be made in respect of the Time for Achieving Operational Acceptance and the other obligations so affected.

25.5 If any dispute shall arise between the parties in connection with or caused by an inspection and/or with regard to any component to be incorporated in the System that cannot be settled amicably between the parties within a reasonable period of time, either party may invoke the process pursuant to GCC Clause 43 (Settlement of Disputes), starting with referral of the matter to the Adjudicator in case an Adjudicator is included and named in the Contract Agreement.

26. Installation of the System

26.1 As soon as the System, or any Subsystem, has, in the opinion of the Supplier, been delivered, Pre-commissioned, and made ready for Commissioning and Operational Acceptance Testing in accordance with the Technical Requirements, the SCC and the Agreed Project Plan, the Supplier shall so notify the Purchaser in writing.

26.2 The Project Manager shall, within fourteen (14) days after receipt of the Supplier's notice under GCC Clause 26.1, either issue an Installation Certificate in the form specified in the Sample Contractual Forms Section in the request for proposals document, stating that the System, or major component or Subsystem (if Acceptance by major component or Subsystem is specified pursuant to the SCC for GCC Clause 27.2.1), has achieved Installation by the date of the Supplier's notice under GCC Clause 26.1, or notify the Supplier in writing of any defects and/or deficiencies, including, but not limited to, defects or deficiencies in the interoperability or integration of the various components and/or Subsystems making up the System. The Supplier shall use all reasonable endeavors to promptly remedy any defect and/or deficiencies that the Project Manager has notified the Supplier of. The Supplier shall then promptly carry out retesting of the System or Subsystem and, when in the Supplier's opinion the System or Subsystem is ready for Commissioning and Operational Acceptance Testing, notify the Purchaser in writing, in accordance with GCC Clause 26.1. The procedure set out in this GCC Clause 26.2 shall be repeated, as necessary, until an Installation Certificate is issued.

26.3 If the Project Manager fails to issue the Installation Certificate and fails to inform the Supplier of any defects and/or deficiencies within fourteen (14) days after receipt

of the Supplier's notice under GCC Clause 26.1, or if the Purchaser puts the System or a Subsystem into production operation, then the System (or Subsystem) shall be deemed to have achieved successful Installation as of the date of the Supplier's notice or repeated notice, or when the Purchaser put the System into production operation, as the case may be.

27. Commissioning and Operational Acceptance

27.1 Commissioning

27.1.1 Commissioning of the System (or Subsystem if specified pursuant to the SCC for GCC Clause 27.2.1) shall be commenced by the Supplier:

(a) immediately after the Installation Certificate is issued by the Project Manager, pursuant to GCC Clause 26.2; or

(b) as otherwise specified in the Technical Requirement or the Agreed Project Plan; or

(c) immediately after Installation is deemed to have occurred, under GCC Clause 26.3.

27.1.2 The Purchaser shall supply the operating and technical personnel and all materials and information reasonably required to enable the Supplier to carry out its obligations with respect to Commissioning.

Production use of the System or Subsystem(s) shall not commence prior to the start of formal Operational Acceptance Testing.

27.2 Operational Acceptance Tests

27.2.1 The Operational Acceptance Tests (and repeats of such tests) shall be the primary responsibility of the Purchaser (in accordance with GCC Clause 10.9), but shall be conducted with the full cooperation of the Supplier during Commissioning of the System (or major components or Subsystem[s]), to ascertain whether the System (or major component or Subsystem[s]) conforms to the Technical Requirements and meets the standard of performance quoted in the Supplier's proposal, including, but not restricted to, the functional and technical performance requirements. **Unless otherwise specified in the SCC**, the Operational Acceptance Tests during Commissioning will be conducted as specified in the Technical Requirements and/or the Agreed Project Plan.

At the Purchaser's discretion, Operational Acceptance Tests may also be performed on replacement Goods, upgrades and new version releases, and Goods that are

added or field-modified after Operational Acceptance of the System.

27.2.2 If for reasons attributable to the Purchaser, the Operational Acceptance Test of the System (or Subsystem[s] or major components, pursuant to the SCC for GCC Clause 27.2.1) cannot be successfully completed within ninety (90) days from the date of Installation or any other period agreed upon in writing by the Purchaser and the Supplier, the Supplier shall be deemed to have fulfilled its obligations with respect to the technical and functional aspects of the Technical Specifications, SCC and/or the Agreed Project Plan, and GCC Clause 28.2 and 28.3 shall not apply.

27.3 Operational Acceptance

27.3.1 Subject to GCC Clause 27.4 (Partial Acceptance) below, Operational Acceptance shall occur in respect of the System, when

(a) the Operational Acceptance Tests, as specified in the Technical Requirements, and/or SCC and/or the Agreed Project Plan have been successfully completed; or

(b) the Operational Acceptance Tests have not been successfully completed or have not been carried out for reasons that are attributable to the Purchaser within the period from the date of Installation or any other agreed-upon period as specified in GCC Clause 27.2.2 above; or

(c) the Purchaser has put the System into production or use for sixty (60) consecutive days. If the System is put into production or use in this manner, the Supplier shall notify the Purchaser and document such use.

27.3.2 At any time after any of the events set out in GCC Clause 27.3.1 have occurred, the Supplier may give a notice to the Project Manager requesting the issue of an Operational Acceptance Certificate.

27.3.3 After consultation with the Purchaser, and within fourteen (14) days after receipt of the Supplier's notice, the Project Manager shall:

(a) issue an Operational Acceptance Certificate; or

(b) notify the Supplier in writing of any defect or deficiencies or other reason for the failure of the Operational Acceptance Tests; or

(c) issue the Operational Acceptance Certificate, if the situation covered by GCC Clause 27.3.1 (b) arises.

27.3.4 The Supplier shall use all reasonable endeavors to promptly remedy any defect and/or deficiencies and/or other reasons for the failure of the Operational Acceptance Test that the Project Manager has notified the Supplier of. Once such remedies have been made by the Supplier, the Supplier shall notify the Purchaser, and the Purchaser, with the full cooperation of the Supplier, shall use all reasonable endeavors to promptly carry out retesting of the System or Subsystem. Upon the successful conclusion of the Operational Acceptance Tests, the Supplier shall notify the Purchaser of its request for Operational Acceptance Certification, in accordance with GCC Clause 27.3.3. The Purchaser shall then issue to the Supplier the Operational Acceptance Certification in accordance with GCC Clause 27.3.3 (a), or shall notify the Supplier of further defects, deficiencies, or other reasons for the failure of the Operational Acceptance Test. The procedure set out in this GCC Clause 27.3.4 shall be repeated, as necessary, until an Operational Acceptance Certificate is issued.

27.3.5 If the System or Subsystem fails to pass the Operational Acceptance Test(s) in accordance with GCC Clause 27.2, then either:

(a) the Purchaser may consider terminating the Contract, pursuant to GCC Clause 41.2.2;

or

(b) if the failure to achieve Operational Acceptance within the specified time period is a result of the failure of the Purchaser to fulfill its obligations under the Contract, then the Supplier shall be deemed to have fulfilled its obligations with respect to the relevant technical and functional aspects of the Contract, and GCC Clauses 30.3 and 30.4 shall not apply.

27.3.6 If within fourteen (14) days after receipt of the Supplier's notice the Project Manager fails to issue the Operational Acceptance Certificate or fails to inform the Supplier in writing of the justifiable reasons why the Project Manager has not issued the Operational Acceptance Certificate, the System or Subsystem shall be deemed to have been accepted as of the date of the Supplier's said notice.

27.4 Partial Acceptance

27.4.1 If so specified in the SCC for GCC Clause 27.2.1, Installation and Commissioning shall be carried out individually for each identified major component or Subsystem(s) of the System. In this event, the provisions in the Contract relating to Installation and Commissioning, including the Operational Acceptance Test, shall apply to each such major component or Subsystem individually, and Operational Acceptance Certificate(s) shall be issued accordingly for each such major component or Subsystem of the System, subject to the limitations contained in GCC Clause 27.4.2.

27.4.2 The issuance of Operational Acceptance Certificates for individual major components or Subsystems pursuant to GCC Clause 27.4.1 shall not relieve the Supplier of its obligation to obtain an Operational Acceptance Certificate for the System as an integrated whole (if so specified in the SCC for GCC Clauses 12.1 and 27.2.1) once all major components and Subsystems have been supplied, installed, tested, and commissioned.

27.4.3 In the case of minor components for the System that by their nature do not require Commissioning or an Operational Acceptance Test (e.g., minor fittings, furnishings or site works, etc.), the Project Manager shall issue an Operational Acceptance Certificate within fourteen (14) days after the fittings and/or furnishings have been delivered and/or installed or the site works have been completed. The Supplier shall, however, use all reasonable endeavors to promptly remedy any defects or deficiencies in such minor components detected by the Purchaser or Supplier.

F. GUARANTEES AND LIABILITIES

28. Operational Acceptance Time Guarantee

28.1 The Supplier guarantees that it shall complete the supply, Installation, Commissioning, and achieve Operational Acceptance of the System (or Subsystems, pursuant to the SCC for GCC Clause 27.2.1) within the time periods specified in the Implementation Schedule and/or the Agreed Project Plan pursuant to GCC Clause 8.2, or within such extended time to which the Supplier shall be entitled under GCC Clause 40 (Extension of Time for Achieving Operational Acceptance).

28.2 **Unless otherwise specified in the SCC**, if the Supplier fails to supply, install, commission, and achieve Operational Acceptance of the System (or Subsystems

pursuant to the SCC for GCC Clause 27.2.1) within the time for achieving Operational Acceptance specified in the Implementation Schedule or the Agreed Project Plan, or any extension of the time for achieving Operational Acceptance previously granted under GCC Clause 40 (Extension of Time for Achieving Operational Acceptance), the Supplier shall pay to the Purchaser liquidated damages at the rate of one half of one percent per week as a percentage of the Contract Price (exclusive of Recurrent Costs if any), or the relevant part of the Contract Price if a Subsystem has not achieved Operational Acceptance. The aggregate amount of such liquidated damages shall in no event exceed the amount of ten (10) percent of the Contract Price (exclusive of Recurrent Costs if any). Once the Maximum is reached, the Purchaser may consider termination of the Contract, pursuant to GCC Clause 41.2.2.

28.3 **Unless otherwise specified in the SCC,** liquidated damages payable under GCC Clause 28.2 shall apply only to the failure to achieve Operational Acceptance of the System (and Subsystems) as specified in the Implementation Schedule and/or Agreed Project Plan. This Clause 28.3 shall not limit, however, any other rights or remedies the Purchaser may have under the Contract for other delays.

28.4 If liquidated damages are claimed by the Purchaser for the System (or Subsystem), the Supplier shall have no further liability whatsoever to the Purchaser in respect to the Operational Acceptance time guarantee for the System (or Subsystem). However, the payment of liquidated damages shall not in any way relieve the Supplier from any of its obligations to complete the System or from any other of its obligations and liabilities under the Contract.

29. Defect Liability

29.1 The Supplier warrants that the System, including all Information Technologies, Materials, and other Goods supplied and Services provided, shall be free from defects in the design, engineering, Materials, and workmanship that prevent the System and/or any of its components from fulfilling the Technical Requirements or that limit in a material fashion the performance, reliability, or extensibility of the System and/or Subsystems. **Unless otherwise specified in the SCC**, there will be NO exceptions and/or limitations to this warranty with respect to Software (or categories of Software). Commercial warranty provisions of products supplied under the Contract shall apply to the extent that they do not conflict with the provisions of this Contract.

29.2 The Supplier also warrants that the Information Technologies, Materials, and other Goods supplied under the Contract are new, unused, and incorporate all recent improvements in design that materially affect the System's or Subsystem's ability to fulfill the Technical Requirements.

29.3 **Unless otherwise specified in the SCC,** the Supplier warrants that: (i) all Goods components to be incorporated into the System form part of the Supplier's and/or Subcontractor's current product lines, and (ii) they have been previously released to the market.

29.4 **Unless otherwise specified in the SCC**, the Warranty Period shall commence from the date of Operational Acceptance of the System (or of any major component or Subsystem for which separate Operational Acceptance is provided for in the Contract) and shall extend for thirty-six (36) months.

29.5 If during the Warranty Period any defect as described in GCC Clause 29.1 should be found in the design, engineering, Materials, and workmanship of the Information Technologies and other Goods supplied or of the Services provided by the Supplier, the Supplier shall promptly, in consultation and agreement with the Purchaser regarding appropriate remedying of the defects, and at its sole cost, repair, replace, or otherwise make good (as the Supplier shall, at its discretion, determine) such defect as well as any damage to the System caused by such defect. Any defective Information Technologies or other Goods that have been replaced by the Supplier shall remain the property of the Supplier.

29.6 The Supplier shall not be responsible for the repair, replacement, or making good of any defect, or of any damage to the System arising out of or resulting from any of the following causes:

(a) improper operation or maintenance of the System by the Purchaser;

(b) normal wear and tear;

(c) use of the System with items not supplied by the Supplier, unless otherwise identified in the Technical Requirements, or approved by the Supplier; or

(d) modifications made to the System by the Purchaser, or a third party, not approved by the Supplier.

29.7 The Supplier's obligations under this GCC Clause 29 shall not apply to:

(a) any materials that are normally consumed in operation or have a normal life shorter than the Warranty Period; or

(b) any designs, specifications, or other data designed, supplied, or specified by or on behalf of the Purchaser or any matters for which the Supplier has disclaimed responsibility, in accordance with GCC Clause 21.1.2.

29.8 The Purchaser shall give the Supplier a notice promptly following the discovery of such defect, stating the nature of any such defect together with all available evidence. The Purchaser shall afford all reasonable opportunity for the Supplier to inspect any such defect. The Purchaser shall afford the Supplier all necessary access to the System and the site to enable the Supplier to perform its obligations under this GCC Clause 29.

29.9 The Supplier may, with the consent of the Purchaser, remove from the site any Information Technologies and other Goods that are defective, if the nature of the defect, and/or any damage to the System caused by the defect, is such that repairs cannot be expeditiously carried out at the site. If the repair, replacement, or making good is of such a character that it may affect the efficiency of the System, the Purchaser may give the Supplier notice requiring that tests of the defective part be made by the Supplier immediately upon completion of such remedial work, whereupon the Supplier shall carry out such tests.

If such part fails the tests, the Supplier shall carry out further repair, replacement, or making good (as the case may be) until that part of the System passes such tests. The tests shall be agreed upon by the Purchaser and the Supplier.

29.10 **Unless otherwise specified in the SCC**, the response times and repair/replacement times for Warranty Defect Repair are specified in the Technical Requirements. Nevertheless, if the Supplier fails to commence the work necessary to remedy such defect or any damage to the System caused by such defect within two weeks the Purchaser may, following notice to the Supplier, proceed to do such work or contract a third party (or parties) to do such work, and the reasonable costs incurred by the Purchaser in connection with such work shall be paid to the Purchaser by the Supplier or may be deducted by the Purchaser from any monies due the Supplier or claimed under the Performance Security.

29.11 If the System or Subsystem cannot be used by reason of such defect and/or making good of such defect, the

Warranty Period for the System shall be extended by a period equal to the period during which the System or Subsystem could not be used by the Purchaser because of such defect and/or making good of such defect.

29.12 Items substituted for defective parts of the System during the Warranty Period shall be covered by the Defect Liability Warranty for the remainder of the Warranty Period applicable for the part replaced or three (3) months, whichever is greater. For reasons of information security, the Purchaser may choose to retain physical possession of any replaced defective information storage devices.

29.13 At the request of the Purchaser and without prejudice to any other rights and remedies that the Purchaser may have against the Supplier under the Contract, the Supplier will offer all possible assistance to the Purchaser to seek warranty services or remedial action from any subcontracted third-party producers or licensor of Goods included in the System, including without limitation assignment or transfer in favor of the Purchaser of the benefit of any warranties given by such producers or licensors to the Supplier.

30. Functional Guarantees

30.1 The Supplier guarantees that, once the Operational Acceptance Certificate(s) has been issued, the System represents a complete, integrated solution to the Purchaser's requirements set forth in the Technical Requirements and it conforms to all other aspects of the Contract. The Supplier acknowledges that GCC Clause 27 regarding Commissioning and Operational Acceptance governs how technical conformance of the System to the Contract requirements will be determined.

30.2 If, for reasons attributable to the Supplier, the System does not conform to the Technical Requirements or does not conform to all other aspects of the Contract, the Supplier shall at its cost and expense make such changes, modifications, and/or additions to the System as may be necessary to conform to the Technical Requirements and meet all functional and performance standards. The Supplier shall notify the Purchaser upon completion of the necessary changes, modifications, and/or additions and shall request the Purchaser to repeat the Operational Acceptance Tests until the System achieves Operational Acceptance.

30.3 If the System (or Subsystem[s]) fails to achieve Operational Acceptance, the Purchaser may consider termination of the Contract, pursuant to GCC Clause 41.2.2, and forfeiture of the Supplier's Performance Security in accordance with GCC Clause 13.3 in

compensation for the extra costs and delays likely to result from this failure.

31. Intellectual Property Rights Warranty

31.1 The Supplier hereby represents and warrants that:

(a) the System as supplied, installed, tested, and accepted;

(b) use of the System in accordance with the Contract; and

(c) copying of the Software and Materials provided to the Purchaser in accordance with the Contract

do not and will not infringe any Intellectual Property Rights held by any third party and that it has all necessary rights or at its sole expense shall have secured in writing all transfers of rights and other consents necessary to make the assignments, licenses, and other transfers of Intellectual Property Rights and the warranties set forth in the Contract, and for the Purchaser to own or exercise all Intellectual Property Rights as provided in the Contract. Without limitation, the Supplier shall secure all necessary written agreements, consents, and transfers of rights from its employees and other persons or entities whose services are used for development of the System.

32. Intellectual Property Rights Indemnity

32.1 The Supplier shall indemnify and hold harmless the Purchaser and its employees and officers from and against any and all losses, liabilities, and costs (including losses, liabilities, and costs incurred in defending a claim alleging such a liability), that the Purchaser or its employees or officers may suffer as a result of any infringement or alleged infringement of any Intellectual Property Rights by reason of:

(a) installation of the System by the Supplier or the use of the System, including the Materials, in the country where the site is located;

(b) copying of the Software and Materials provided the Supplier in accordance with the Agreement; and

(c) sale of the products produced by the System in any country, except to the extent that such losses, liabilities, and costs arise as a result of the Purchaser's breach of GCC Clause 32.2.

32.2 Such indemnity shall not cover any use of the System, including the Materials, other than for the purpose indicated by or to be reasonably inferred from the Contract, any infringement resulting from the use of the System, or any products of the System produced thereby in association or combination with any other goods or services not

supplied by the Supplier, where the infringement arises because of such association or combination and not because of use of the System in its own right.

32.3 Such indemnities shall also not apply if any claim of infringement:

(a) is asserted by a parent, subsidiary, or affiliate of the Purchaser's organization;

(b) is a direct result of a design mandated by the Purchaser's Technical Requirements and the possibility of such infringement was duly noted in the Supplier's Proposal; or

(c) results from the alteration of the System, including the Materials, by the Purchaser or any persons other than the Supplier or a person authorized by the Supplier.

32.4 If any proceedings are brought or any claim is made against the Purchaser arising out of the matters referred to in GCC Clause 32.1, the Purchaser shall promptly give the Supplier notice of such proceedings or claims, and the Supplier may at its own expense and in the Purchaser's name conduct such proceedings or claim and any negotiations for the settlement of any such proceedings or claim.

If the Supplier fails to notify the Purchaser within twenty-eight (28) days after receipt of such notice that it intends to conduct any such proceedings or claim, then the Purchaser shall be free to conduct the same on its own behalf. Unless the Supplier has so failed to notify the Purchaser within the twenty-eight (28) days, the Purchaser shall make no admission that may be prejudicial to the defense of any such proceedings or claim. The Purchaser shall, at the Supplier's request, afford all available assistance to the Supplier in conducting such proceedings or claim and shall be reimbursed by the Supplier for all reasonable expenses incurred in so doing.

32.5 The Purchaser shall indemnify and hold harmless the Supplier and its employees, officers, and Subcontractors from and against any and all losses, liabilities, and costs (including losses, liabilities, and costs incurred in defending a claim alleging such a liability) that the Supplier or its employees, officers, or Subcontractors may suffer as a result of any infringement or alleged infringement of any Intellectual Property Rights arising out of or in connection with any design, data, drawing, specification, or other documents or materials provided to the Supplier in connection with this Contract by the Purchaser or any persons (other than the Supplier) contracted by the

Purchaser, except to the extent that such losses, liabilities, and costs arise as a result of the Supplier's breach of GCC Clause 32.8.

32.6 Such indemnity shall not cover

(a) any use of the design, data, drawing, specification, or other documents or materials, other than for the purpose indicated by or to be reasonably inferred from the Contract;

(b) any infringement resulting from the use of the design, data, drawing, specification, or other documents or materials, or any products produced thereby, in association or combination with any other Goods or Services not provided by the Purchaser or any other person contracted by the Purchaser, where the infringement arises because of such association or combination and not because of the use of the design, data, drawing, specification, or other documents or materials in its own right.

32.7 Such indemnities shall also not apply:

(a) if any claim of infringement is asserted by a parent, subsidiary, or affiliate of the Supplier's organization;

(b) to the extent that any claim of infringement is caused by the alteration, by the Supplier, or any persons contracted by the Supplier, of the design, data, drawing, specification, or other documents or materials provided to the Supplier by the Purchaser or any persons contracted by the Purchaser.

32.8 If any proceedings are brought or any claim is made against the Supplier arising out of the matters referred to in GCC Clause 32.5, the Supplier shall promptly give the Purchaser notice of such proceedings or claims, and the Purchaser may at its own expense and in the Supplier's name conduct such proceedings or claim and any negotiations for the settlement of any such proceedings or claim. If the Purchaser fails to notify the Supplier within twenty-eight (28) days after receipt of such notice that it intends to conduct any such proceedings or claim, then the Supplier shall be free to conduct the same on its own behalf. Unless the Purchaser has so failed to notify the Supplier within the twenty-eight (28) days, the Supplier shall make no admission that may be prejudicial to the defense of any such proceedings or claim. The Supplier shall, at the Purchaser's request, afford all available assistance to the Purchaser in conducting such proceedings or claim and shall be reimbursed by the Purchaser for all reasonable expenses incurred in so doing.

33. Limitation of Liability

33.1 Provided the following does not exclude or limit any liabilities of either party in ways not permitted by applicable law:

(a) the Supplier shall not be liable to the Purchaser, whether in contract, tort, or otherwise, for any indirect or consequential loss or damage, loss of use, loss of production, or loss of profits or interest costs, provided that this exclusion shall not apply to any obligation of the Supplier to pay liquidated damages to the Purchaser; and

(b) the aggregate liability of the Supplier to the Purchaser, whether under the Contract, in tort or otherwise, shall not exceed the total Contract Price, provided that this limitation shall not apply to any obligation of the Supplier to indemnify the Purchaser with respect to intellectual property rights infringement.

G. RISK DISTRIBUTION

34. Transfer of Ownership

34.1 With the exception of Software and Materials, the ownership of the Information Technologies and other Goods shall be transferred to the Purchaser at the time of Delivery or otherwise under terms that may be agreed upon and specified in the Contract Agreement.

34.2 Ownership and the terms of usage of the Software and Materials supplied under the Contract shall be governed by GCC Clause 15 (Copyright) Clause 16 (Software License Agreements), and any elaboration in the Technical Requirements.

34.3 Ownership of the Supplier's Equipment used by the Supplier and its Subcontractors in connection with the Contract shall remain with the Supplier or its Subcontractors.

35. Care of the System

35.1 The Purchaser shall become responsible for the care and custody of the System or Subsystems upon their Delivery. The Purchaser shall make good at its own cost any loss or damage that may occur to the System or Subsystems from any cause from the date of Delivery until the date of Operational Acceptance of the System or Subsystems, pursuant to GCC Clause 27 (Commissioning and Operational Acceptance), excepting such loss or damage arising from acts or omissions of the Supplier, its employees, or subcontractors.

35.2 If any loss or damage occurs to the System or any part of the System by reason of:

(a) (insofar as they relate to the country where the Project Site is located) nuclear reaction, nuclear radiation, radioactive contamination, a pressure wave caused by aircraft or other aerial objects, or any other occurrences that an experienced Supplier could not reasonably foresee, or if reasonably foreseeable could not reasonably make provision for or insure against, insofar as such risks are not normally insurable on the insurance market and are mentioned in the general exclusions of the policy of insurance taken out under GCC Clause 37;

(b) any use not in accordance with the Contract, by the Purchaser or any third party;

(c) any use of or reliance upon any design, data, or specification provided or designated by or on behalf of the Purchaser, or any such matter for which the Supplier has disclaimed responsibility in accordance with GCC Clause 21.1.2,

the Purchaser shall pay to the Supplier all sums payable in respect of the System or Subsystems that have achieved Operational Acceptance, notwithstanding that the same be lost, destroyed, or damaged. If the Purchaser requests the Supplier in writing to make good any loss or damage to the System thereby occasioned, the Supplier shall make good the same at the cost of the Purchaser in accordance with GCC Clause 39. If the Purchaser does not request the Supplier in writing to make good any loss or damage to the System thereby occasioned, the Purchaser shall either request a change in accordance with GCC Clause 39, excluding the performance of that part of the System thereby lost, destroyed, or damaged, or, where the loss or damage affects a substantial part of the System, the Purchaser shall terminate the Contract pursuant to GCC Clause 41.1.

35.3 The Purchaser shall be liable for any loss of or damage to any Supplier’s Equipment which the Purchaser has authorized to locate within the Purchaser's premises for use in fulfillment of Supplier's obligations under the Contract, except where such loss or damage arises from acts or omissions of the Supplier, its employees, or subcontractors.

36. Loss of or Damage to Property; Accident or Injury to Workers; Indemnification

36.1 The Supplier and each and every Subcontractor shall abide by the job safety, insurance, customs, and immigration measures prevalent and laws in force in the Purchaser's Country.

36.2 Subject to GCC Clause 36.3, the Supplier shall indemnify and hold harmless the Purchaser and its employees and officers from and against any and all losses, liabilities and costs (including losses, liabilities, and costs incurred in defending a claim alleging such a liability) that the Purchaser or its employees or officers may suffer as a result of the death or injury of any person or loss of or damage to any property (other than the System, whether accepted or not) arising in connection with the supply, installation, testing, and Commissioning of the System and by reason of the negligence of the Supplier or its Subcontractors, or their employees, officers or agents, except any injury, death, or property damage caused by the negligence of the Purchaser, its contractors, employees, officers, or agents.

36.3 If any proceedings are brought or any claim is made against the Purchaser that might subject the Supplier to liability under GCC Clause 36.2, the Purchaser shall promptly give the Supplier notice of such proceedings or claims, and the Supplier may at its own expense and in the Purchaser's name conduct such proceedings or claim and any negotiations for the settlement of any such proceedings or claim. If the Supplier fails to notify the Purchaser within twenty-eight (28) days after receipt of such notice that it intends to conduct any such proceedings or claim, then the Purchaser shall be free to conduct the same on its own behalf. Unless the Supplier has so failed to notify the Purchaser within the twenty-eight (28) day period, the Purchaser shall make no admission that may be prejudicial to the defense of any such proceedings or claim. The Purchaser shall, at the Supplier's request, afford all available assistance to the Supplier in conducting such proceedings or claim and shall be reimbursed by the Supplier for all reasonable expenses incurred in so doing.

36.4 The Purchaser shall indemnify and hold harmless the Supplier and its employees, officers, and Subcontractors from any and all losses, liabilities, and costs (including losses, liabilities, and costs incurred in defending a claim alleging such a liability) that the Supplier or its employees, officers, or Subcontractors may suffer as a result of the death or personal injury of any person or loss of or damage to property of the Purchaser, other than the System not yet achieving Operational Acceptance, that is caused by fire, explosion, or any other perils, in excess of the amount recoverable from insurances procured under GCC Clause

37 (Insurances), provided that such fire, explosion, or other perils were not caused by any act or failure of the Supplier.

36.5 If any proceedings are brought or any claim is made against the Supplier that might subject the Purchaser to liability under GCC Clause 36.4, the Supplier shall promptly give the Purchaser notice of such proceedings or claims, and the Purchaser may at its own expense and in the Supplier's name conduct such proceedings or claim and any negotiations for the settlement of any such proceedings or claim. If the Purchaser fails to notify the Supplier within twenty-eight (28) days after receipt of such notice that it intends to conduct any such proceedings or claim, then the Supplier shall be free to conduct the same on its own behalf. Unless the Purchaser has so failed to notify the Supplier within the twenty-eight (28) days, the Supplier shall make no admission that may be prejudicial to the defense of any such proceedings or claim. The Supplier shall, at the Purchaser's request, afford all available assistance to the Purchaser in conducting such proceedings or claim and shall be reimbursed by the Purchaser for all reasonable expenses incurred in so doing.

36.6 The party entitled to the benefit of an indemnity under this GCC Clause 36 shall take all reasonable measures to mitigate any loss or damage that has occurred. If the party fails to take such measures, the other party's liabilities shall be correspondingly reduced.

37. Insurances

37.1 The Supplier shall at its expense take out and maintain in effect, or cause to be taken out and maintained in effect, during the performance of the Contract, the insurance set forth below. The identity of the insurers and the form of the policies shall be subject to the approval of the Purchaser, who should not unreasonably withhold such approval.

(a) Cargo Insurance During Transport

as applicable, 110 percent of the price of the Information Technologies and other Goods in a freely convertible currency, covering the Goods from physical loss or damage during shipment through receipt at the Project Site.

(b) Installation "All Risks" Insurance

as applicable, 110 percent of the price of the Information Technologies and other Goods covering the Goods at the site from all risks of physical loss or damage (excluding only perils commonly excluded under "all risks" insurance policies of this type by

reputable insurers) occurring prior to Operational Acceptance of the System.

(c) Third-Party Liability Insurance

On terms as **specified in the SCC,** covering bodily injury or death suffered by third parties (including the Purchaser's personnel) and loss of or damage to property (including the Purchaser's property and any Subsystems that have been accepted by the Purchaser) occurring in connection with the supply and installation of the Information System.

(d) Automobile Liability Insurance

In accordance with the statutory requirements prevailing in the Purchaser's Country, covering use of all vehicles used by the Supplier or its Subcontractors (whether or not owned by them) in connection with the execution of the Contract.

(e) Other Insurance (if any), as **specified in the SCC.**

37.2 The Purchaser shall be named as co-insured under all insurance policies taken out by the Supplier pursuant to GCC Clause 37.1, except for the Third-Party Liability, and the Supplier's Subcontractors shall be named as co-insured under all insurance policies taken out by the Supplier pursuant to GCC Clause 37.1 except for Cargo Insurance During Transport. All insurer's rights of subrogation against such co-insured for losses or claims arising out of the performance of the Contract shall be waived under such policies.

37.3 The Supplier shall deliver to the Purchaser certificates of insurance (or copies of the insurance policies) as evidence that the required policies are in full force and effect.

37.4 The Supplier shall ensure that, where applicable, its Subcontractor(s) shall take out and maintain in effect adequate insurance policies for their personnel and vehicles and for work executed by them under the Contract, unless such Subcontractors are covered by the policies taken out by the Supplier.

37.5 If the Supplier fails to take out and/or maintain in effect the insurance referred to in GCC Clause 37.1, the Purchaser may take out and maintain in effect any such insurance and may from time to time deduct from any amount due the Supplier under the Contract any premium that the Purchaser shall have paid to the insurer or may otherwise recover such amount as a debt due from the Supplier.

37.6 Unless otherwise provided in the Contract, the Supplier shall prepare and conduct all and any claims made under

the policies affected by it pursuant to this GCC Clause 37, and all monies payable by any insurers shall be paid to the Supplier. The Purchaser shall give to the Supplier all such reasonable assistance as may be required by the Supplier in connection with any claim under the relevant insurance policies. With respect to insurance claims in which the Purchaser's interest is involved, the Supplier shall not give any release or make any compromise with the insurer without the prior written consent of the Purchaser. With respect to insurance claims in which the Supplier's interest is involved, the Purchaser shall not give any release or make any compromise with the insurer without the prior written consent of the Supplier.

38. Force Majeure

38.1 "Force Majeure" shall mean any event beyond the reasonable control of the Purchaser or of the Supplier, as the case may be, and which is unavoidable notwithstanding the reasonable care of the party affected and shall include, without limitation, the following:

(a) war, hostilities, or warlike operations (whether a state of war be declared or not), invasion, act of foreign enemy, and civil war;

(b) rebellion, revolution, insurrection, mutiny, usurpation of civil or military government, conspiracy, riot, civil commotion, and terrorist acts;

(c) confiscation, nationalization, mobilization, commandeering or requisition by or under the order of any government or de jure or de facto authority or ruler, or any other act or failure to act of any local state or national government authority;

(d) strike, sabotage, lockout, embargo, import restriction, port congestion, lack of usual means of public transportation and communication, industrial dispute, shipwreck, shortage or restriction of power supply, epidemics, quarantine, and plague;

(e) earthquake, landslide, volcanic activity, fire, flood or inundation, tidal wave, typhoon or cyclone, hurricane, storm, lightning, or other inclement weather condition, nuclear and pressure waves, or other natural or physical disaster;

(f) failure, by the Supplier, to obtain the necessary export permit(s) from the governments of the Country(s) of Origin of the Information Technologies or other Goods, or Supplier's Equipment provided that the Supplier has made all reasonable efforts to obtain the required export permit(s), including the exercise of due diligence in determining the eligibility of the

System and all of its components for receipt of the necessary export permits.

38.2 If either party is prevented, hindered, or delayed from or in performing any of its obligations under the Contract by an event of Force Majeure, then it shall notify the other in writing of the occurrence of such event and the circumstances of the event of Force Majeure within fourteen (14) days after the occurrence of such event.

38.3 The party who has given such notice shall be excused from the performance or punctual performance of its obligations under the Contract for so long as the relevant event of Force Majeure continues and to the extent that such party's performance is prevented, hindered, or delayed. The Time for Achieving Operational Acceptance shall be extended in accordance with GCC Clause 40 (Extension of Time for Achieving Operational Acceptance).

38.4 The party or parties affected by the event of Force Majeure shall use reasonable efforts to mitigate the effect of the event of Force Majeure upon its or their performance of the Contract and to fulfill its or their obligations under the Contract, but without prejudice to either party's right to terminate the Contract under GCC Clause 38.6.

38.5 No delay or nonperformance by either party to this Contract caused by the occurrence of any event of Force Majeure shall:

(a) constitute a default or breach of the Contract;

(b) (subject to GCC Clauses 35.2, 38.3, and 38.4) give rise to any claim for damages or additional cost or expense occasioned by the delay or nonperformance,

if, and to the extent that, such delay or nonperformance is caused by the occurrence of an event of Force Majeure.

38.6 If the performance of the Contract is substantially prevented, hindered, or delayed for a single period of more than sixty (60) days or an aggregate period of more than one hundred and twenty (120) days on account of one or more events of Force Majeure during the time period covered by the Contract, the parties will attempt to develop a mutually satisfactory solution, failing which, either party may terminate the Contract by giving a notice to the other.

38.7 In the event of termination pursuant to GCC Clause 38.6, the rights and obligations of the Purchaser and the Supplier shall be as specified in GCC Clauses 41.1.2 and 41.1.3.

38.8 Notwithstanding GCC Clause 38.5, Force Majeure shall not apply to any obligation of the Purchaser to make payments to the Supplier under this Contract.

H. CHANGE IN CONTRACT ELEMENTS

39. Changes to the System

39.1 Introducing a Change

39.1.1 Subject to GCC Clauses 39.2.5 and 39.2.7, the Purchaser shall have the right to propose, and subsequently require, the Project Manager to order the Supplier from time to time during the performance of the Contract to make any change, modification, addition, or deletion to, in, or from the System (interchangeably called "Change"), provided that such Change falls within the general scope of the System, does not constitute unrelated work, and is technically practicable, taking into account both the state of advancement of the System and the technical compatibility of the Change envisaged with the nature of the System as originally specified in the Contract.

A Change may involve, but is not restricted to, the substitution of updated Information Technologies and related Services in accordance with GCC Clause 23 (Product Upgrades).

39.1.2 The Supplier may from time to time during its performance of the Contract propose to the Purchaser (with a copy to the Project Manager) any Change that the Supplier considers necessary or desirable to improve the quality or efficiency of the System. The Purchaser may at its discretion approve or reject any Change proposed by the Supplier.

39.1.3 Notwithstanding GCC Clauses 39.1.1 and 39.1.2, no change made necessary because of any default of the Supplier in the performance of its obligations under the Contract shall be deemed to be a Change, and such change shall not result in any adjustment of the Contract Price or the Time for Achieving Operational Acceptance.

39.1.4 The procedure on how to proceed with and execute Changes is specified in GCC Clauses 39.2 and 39.3, and further details and sample forms are provided in the Sample Contractual Forms Section in the request for proposals document.

39.1.5 Moreover, the Purchaser and Supplier will agree, during development of the Project Plan, to a date prior to the scheduled date for Operational Acceptance, after which the Technical Requirements for the System shall be "frozen." Any Change initiated after this time will be dealt with after Operational Acceptance.

39.2 Changes Originating from Purchaser

39.2.1 If the Purchaser proposes a Change pursuant to GCC Clauses 39.1.1, it shall send to the Supplier a "Request for Change Proposal," requiring the Supplier to prepare and furnish to the Project Manager as soon as reasonably practicable a "Change Proposal," which shall include the following:

(a) brief description of the Change;

(b) impact on the Time for Achieving Operational Acceptance;

(c) detailed estimated cost of the Change;

(d) effect on Functional Guarantees (if any);

(e) effect on any other provisions of the Contract; and

(f) any additional documents as **specified in the SCC**.

39.2.2 Prior to preparing and submitting the "Change Proposal," the Supplier shall submit to the Project Manager a "Change Estimate Proposal," which shall be an estimate of the cost of preparing the Change Proposal, plus a first approximation of the suggested approach and cost for implementing the changes. Upon receipt of the Supplier's Change Estimate Proposal, the Purchaser shall do one of the following:

(a) accept the Supplier's estimate with instructions to the Supplier to proceed with the preparation of the Change Proposal;

(b) advise the Supplier of any part of its Change Estimate Proposal that is unacceptable and request the Supplier to review its estimate;

(c) advise the Supplier that the Purchaser does not intend to proceed with the Change.

39.2.3 Upon receipt of the Purchaser's instruction to proceed under GCC Clause 39.2.2 (a), the Supplier shall, with proper expedition, proceed with the preparation of the Change Proposal, in accordance with GCC Clause 39.2.1. The Supplier, at its discretion, may specify a validity period for the Change Proposal, after which if the Purchaser and Supplier has not reached agreement in accordance with GCC Clause 39.2.6, then GCC Clause 39.2.7 shall apply.

39.2.4 The pricing of any Change shall, as far as practicable, be calculated in accordance with the rates and prices included in the Contract. If the nature of the Change is such that the Contract rates and prices are

inequitable, the parties to the Contract shall agree on other specific rates to be used for valuing the Change.

39.2.5 If before or during the preparation of the Change Proposal it becomes apparent that the aggregate impact of compliance with the Request for Change Proposal and with all other Change Orders that have already become binding upon the Supplier under this GCC Clause 39 would be to increase or decrease the Contract Price as originally set forth in Article 2 (Contract Price) of the Contract Agreement by more than fifteen (15) percent, the Supplier may give a written notice of objection to this Request for Change Proposal prior to furnishing the Change Proposal. If the Purchaser accepts the Supplier's objection, the Purchaser shall withdraw the proposed Change and shall notify the Supplier in writing of its acceptance.

The Supplier's failure to so object to a Request for Change Proposal shall neither affect its right to object to any subsequent requested Changes or Change Orders, nor affect its right to take into account, when making such subsequent objection, the percentage increase or decrease in the Contract Price that any Change not objected to by the Supplier represents.

39.2.6 Upon receipt of the Change Proposal, the Purchaser and the Supplier shall mutually agree upon all matters contained in the Change Proposal. Within fourteen (14) days after such agreement, the Purchaser shall, if it intends to proceed with the Change, issue the Supplier a Change Order. If the Purchaser is unable to reach a decision within fourteen (14) days, it shall notify the Supplier with details of when the Supplier can expect a decision. If the Purchaser decides not to proceed with the Change for whatever reason, it shall, within the said period of fourteen (14) days, notify the Supplier accordingly. Under such circumstances, the Supplier shall be entitled to reimbursement of all costs reasonably incurred by it in the preparation of the Change Proposal, provided that these do not exceed the amount given by the Supplier in its Change Estimate Proposal submitted in accordance with GCC Clause 39.2.2.

39.2.7 If the Purchaser and the Supplier cannot reach agreement on the price for the Change, an equitable adjustment to the Time for Achieving Operational Acceptance, or any other matters identified in the Change Proposal, the Change will not be implemented. However, this provision does not limit the rights of

either party under GCC Clause 6 (Settlement of Disputes).

39.3 Changes Originating from Supplier

If the Supplier proposes a Change pursuant to GCC Clause 39.1.2, the Supplier shall submit to the Project Manager a written "Application for Change Proposal," giving reasons for the proposed Change and including the information specified in GCC Clause 39.2.1. Upon receipt of the Application for Change Proposal, the parties shall follow the procedures outlined in GCC Clauses 39.2.6 and 39.2.7. However, should the Purchaser choose not to proceed or the Purchaser and the Supplier cannot come to agreement on the change during any validity period that the Supplier may specify in its Application for Change Proposal, the Supplier shall not be entitled to recover the costs of preparing the Application for Change Proposal, unless subject to an agreement between the Purchaser and the Supplier to the contrary.

39.4 Value engineering. The Supplier may prepare, at its own cost, a value engineering proposal at any time during the performance of the Contract. The value engineering proposal shall, at a minimum, include the following;

(a) the proposed change(s), and a description of the difference to the existing Contract requirements;

(b) a full cost/benefit analysis of the proposed change(s) including a description and estimate of costs (including life cycle costs) the Purchaser may incur in implementing the value engineering proposal; and

(c) a description of any effect(s) of the change on performance/functionality.

The Purchaser may accept the value engineering proposal if the proposal demonstrates benefits that:

(a) accelerates the delivery period; or

(b) reduces the Contract Price or the life cycle costs to the Purchaser; or

(c) improves the quality, efficiency, safety or sustainability of the systems; or

(d) yields any other benefits to the Purchaser,

without compromising the necessary functions of the systems.

If the value engineering proposal is approved by the Purchaser and results in:

(a) a reduction of the Contract Price; the amount to be paid to the Supplier shall be the percentage specified in the SCC of the reduction in the Contract Price; or

(b) an increase in the Contract Price; but results in a reduction in life cycle costs due to any benefit described in (a) to (d) above,

the amount to be paid to the Supplier shall be the full increase in the Contract Price.

40. Extension of Time for Achieving Operational Acceptance

40.1 The time(s) for achieving Operational Acceptance specified in the Schedule of Implementation shall be extended if the Supplier is delayed or impeded in the performance of any of its obligations under the Contract by reason of any of the following:

(a) any Change in the System as provided in GCC Clause 39 (Change in the Information System);

(b) any occurrence of Force Majeure as provided in GCC Clause 38 (Force Majeure);

(c) default of the Purchaser; or

(d) any other matter specifically mentioned in the Contract;

by such period as shall be fair and reasonable in all the circumstances and as shall fairly reflect the delay or impediment sustained by the Supplier.

40.2 Except where otherwise specifically provided in the Contract, the Supplier shall submit to the Project Manager a notice of a claim for an extension of the time for achieving Operational Acceptance, together with particulars of the event or circumstance justifying such extension as soon as reasonably practicable after the commencement of such event or circumstance. As soon as reasonably practicable after receipt of such notice and supporting particulars of the claim, the Purchaser and the Supplier shall agree upon the period of such extension. In the event that the Supplier does not accept the Purchaser's estimate of a fair and reasonable time extension, the Supplier shall be entitled to refer the matter to the provisions for the Settlement of Disputes pursuant to GCC Clause 43.

40.3 The Supplier shall at all times use its reasonable efforts to minimize any delay in the performance of its obligations under the Contract.

41. Termination

41.1 Termination for Purchaser's Convenience

41.1.1 The Purchaser may at any time terminate the Contract for any reason by giving the Supplier a notice of termination that refers to this GCC Clause 41.1.

41.1.2 Upon receipt of the notice of termination under GCC Clause 41.1.1, the Supplier shall either as soon as reasonably practical or upon the date specified in the notice of termination

(a) cease all further work, except for such work as the Purchaser may specify in the notice of termination for the sole purpose of protecting that part of the System already executed, or any work required to leave the site in a clean and safe condition;

(b) terminate all subcontracts, except those to be assigned to the Purchaser pursuant to GCC Clause 41.1.2 (d) (ii) below;

(c) remove all Supplier's Equipment from the site, repatriate the Supplier's Personnel from the site, remove from the site any wreckage, rubbish, and debris of any kind;

(d) in addition, the Supplier, subject to the payment specified in GCC Clause 41.1.3, shall

(i) deliver to the Purchaser the parts of the System executed by the Supplier up to the date of termination;

(ii) to the extent legally possible, assign to the Purchaser all right, title, and benefit of the Supplier to the System, or Subsystem, as at the date of termination, and, as may be required by the Purchaser, in any subcontracts concluded between the Supplier and its Subcontractors;

(iii) deliver to the Purchaser all nonproprietary drawings, specifications, and other documents prepared by the Supplier or its Subcontractors as of the date of termination in connection with the System.

41.1.3 In the event of termination of the Contract under GCC Clause 41.1.1, the Purchaser shall pay to the Supplier the following amounts:

(a) the Contract Price, properly attributable to the parts of the System executed by the Supplier as of the date of termination;

(b) the costs reasonably incurred by the Supplier in the removal of the Supplier's Equipment from

the site and in the repatriation of the Supplier's Personnel;

(c) any amount to be paid by the Supplier to its Subcontractors in connection with the termination of any subcontracts, including any cancellation charges;

(d) costs incurred by the Supplier in protecting the System and leaving the site in a clean and safe condition pursuant to GCC Clause 41.1.2 (a); and

(e) the cost of satisfying all other obligations, commitments, and claims that the Supplier may in good faith have undertaken with third parties in connection with the Contract and that are not covered by GCC Clauses 41.1.3 (a) through (d) above.

41.2 Termination for Supplier's Default

41.2.1 The Purchaser, without prejudice to any other rights or remedies it may possess, may terminate the Contract forthwith in the following circumstances by giving a notice of termination and its reasons therefore to the Supplier, referring to this GCC Clause 41.2:

(a) if the Supplier becomes bankrupt or insolvent, has a receiving order issued against it, compounds with its creditors, or, if the Supplier is a corporation, a resolution is passed or order is made for its winding up (other than a voluntary liquidation for the purposes of amalgamation or reconstruction), a receiver is appointed over any part of its undertaking or assets, or if the Supplier takes or suffers any other analogous action in consequence of debt;

(b) if the Supplier assigns or transfers the Contract or any right or interest therein in violation of the provision of GCC Clause 42 (Assignment); or

(c) if the Supplier, in the judgment of the Purchaser has engaged in Fraud and Corruption, as defined in paragraph 2.2 a. of the Appendix 1 to the GCC, in competing for or in executing the Contract, including but not limited to willful misrepresentation of facts concerning ownership of Intellectual Property Rights in, or proper authorization and/or licenses from the owner to offer, the hardware, software, or materials provided under this Contract.

41.2.2 If the Supplier:

(a) has abandoned or repudiated the Contract;

(b) has without valid reason failed to commence work on the System promptly;

(c) persistently fails to execute the Contract in accordance with the Contract or persistently neglects to carry out its obligations under the Contract without just cause;

(d) refuses or is unable to provide sufficient Materials, Services, or labor to execute and complete the System in the manner specified in the Agreed Project Plan furnished under GCC Clause 19 at rates of progress that give reasonable assurance to the Purchaser that the Supplier can attain Operational Acceptance of the System by the Time for Achieving Operational Acceptance as extended;

then the Purchaser may, without prejudice to any other rights it may possess under the Contract, give a notice to the Supplier stating the nature of the default and requiring the Supplier to remedy the same. If the Supplier fails to remedy or to take steps to remedy the same within thirty (30) days of its receipt of such notice, then the Purchaser may terminate the Contract forthwith by giving a notice of termination to the Supplier that refers to this GCC Clause 41.2.

41.2.3 Upon receipt of the notice of termination under GCC Clauses 41.2.1 or 41.2.2, the Supplier shall, either immediately or upon such date as is specified in the notice of termination:

(a) cease all further work, except for such work as the Purchaser may specify in the notice of termination for the sole purpose of protecting that part of the System already executed or any work required to leave the site in a clean and safe condition;

(b) terminate all subcontracts, except those to be assigned to the Purchaser pursuant to GCC Clause 41.2.3 (d) below;

(c) deliver to the Purchaser the parts of the System executed by the Supplier up to the date of termination;

(d) to the extent legally possible, assign to the Purchaser all right, title and benefit of the Supplier to the System or Subsystems as at the

date of termination, and, as may be required by the Purchaser, in any subcontracts concluded between the Supplier and its Subcontractors;

(e) deliver to the Purchaser all drawings, specifications, and other documents prepared by the Supplier or its Subcontractors as at the date of termination in connection with the System.

41.2.4 The Purchaser may enter upon the site, expel the Supplier, and complete the System itself or by employing any third party. Upon completion of the System or at such earlier date as the Purchaser thinks appropriate, the Purchaser shall give notice to the Supplier that such Supplier's Equipment will be returned to the Supplier at or near the site and shall return such Supplier's Equipment to the Supplier in accordance with such notice. The Supplier shall thereafter without delay and at its cost remove or arrange removal of the same from the site.

41.2.5 Subject to GCC Clause 41.2.6, the Supplier shall be entitled to be paid the Contract Price attributable to the portion of the System executed as at the date of termination and the costs, if any, incurred in protecting the System and in leaving the site in a clean and safe condition pursuant to GCC Clause 41.2.3 (a). Any sums due the Purchaser from the Supplier accruing prior to the date of termination shall be deducted from the amount to be paid to the Supplier under this Contract.

41.2.6 If the Purchaser completes the System, the cost of completing the System by the Purchaser shall be determined. If the sum that the Supplier is entitled to be paid, pursuant to GCC Clause 41.2.5, plus the reasonable costs incurred by the Purchaser in completing the System, exceeds the Contract Price, the Supplier shall be liable for such excess. If such excess is greater than the sums due the Supplier under GCC Clause 41.2.5, the Supplier shall pay the balance to the Purchaser, and if such excess is less than the sums due the Supplier under GCC Clause 41.2.5, the Purchaser shall pay the balance to the Supplier. The Purchaser and the Supplier shall agree, in writing, on the computation described above and the manner in which any sums shall be paid.

41.3 Termination by Supplier

41.3.1 If:

(a) the Purchaser has failed to pay the Supplier any sum due under the Contract within the specified

period, has failed to approve any invoice or supporting documents without just cause **pursuant to the SCC,** or commits a substantial breach of the Contract, the Supplier may give a notice to the Purchaser that requires payment of such sum, with interest on this sum as stipulated in GCC Clause 12.3, requires approval of such invoice or supporting documents, or specifies the breach and requires the Purchaser to remedy the same, as the case may be. If the Purchaser fails to pay such sum together with such interest, fails to approve such invoice or supporting documents or give its reasons for withholding such approval, fails to remedy the breach or take steps to remedy the breach within fourteen (14) days after receipt of the Supplier's notice; or

(b) the Supplier is unable to carry out any of its obligations under the Contract for any reason attributable to the Purchaser, including but not limited to the Purchaser's failure to provide possession of or access to the site or other areas or failure to obtain any governmental permit necessary for the execution and/or completion of the System;

then the Supplier may give a notice to the Purchaser of such events, and if the Purchaser has failed to pay the outstanding sum, to approve the invoice or supporting documents, to give its reasons for withholding such approval, or to remedy the breach within twenty-eight (28) days of such notice, or if the Supplier is still unable to carry out any of its obligations under the Contract for any reason attributable to the Purchaser within twenty-eight (28) days of the said notice, the Supplier may by a further notice to the Purchaser referring to this GCC Clause 41.3.1, forthwith terminate the Contract.

41.3.2 The Supplier may terminate the Contract immediately by giving a notice to the Purchaser to that effect, referring to this GCC Clause 41.3.2, if the Purchaser becomes bankrupt or insolvent, has a receiving order issued against it, compounds with its creditors, or, being a corporation, if a resolution is passed or order is made for its winding up (other than a voluntary liquidation for the purposes of amalgamation or reconstruction), a receiver is appointed over any part of its undertaking or assets, or if the Purchaser takes or suffers any other analogous action in consequence of debt.

41.3.3 If the Contract is terminated under GCC Clauses 41.3.1 or 41.3.2, then the Supplier shall immediately:

(a) cease all further work, except for such work as may be necessary for the purpose of protecting that part of the System already executed, or any work required to leave the site in a clean and safe condition;

(b) terminate all subcontracts, except those to be assigned to the Purchaser pursuant to Clause 41.3.3 (d) (ii);

(c) remove all Supplier's Equipment from the site and repatriate the Supplier's Personnel from the site.

(d) In addition, the Supplier, subject to the payment specified in GCC Clause 41.3.4, shall:

(i) deliver to the Purchaser the parts of the System executed by the Supplier up to the date of termination;

(ii) to the extent legally possible, assign to the Purchaser all right, title, and benefit of the Supplier to the System, or Subsystems, as of the date of termination, and, as may be required by the Purchaser, in any subcontracts concluded between the Supplier and its Subcontractors;

(iii) to the extent legally possible, deliver to the Purchaser all drawings, specifications, and other documents prepared by the Supplier or its Subcontractors as of the date of termination in connection with the System.

41.3.4 If the Contract is terminated under GCC Clauses 41.3.1 or 41.3.2, the Purchaser shall pay to the Supplier all payments specified in GCC Clause 41.1.3 and reasonable compensation for all loss, except for loss of profit, or damage sustained by the Supplier arising out of, in connection with, or in consequence of such termination.

41.3.5 Termination by the Supplier pursuant to this GCC Clause 41.3 is without prejudice to any other rights or remedies of the Supplier that may be exercised in lieu of or in addition to rights conferred by GCC Clause 41.3.

41.4 In this GCC Clause 41, the expression "portion of the System executed" shall include all work executed, Services

provided, and all Information Technologies, or other Goods acquired (or subject to a legally binding obligation to purchase) by the Supplier and used or intended to be used for the purpose of the System, up to and including the date of termination.

41.5 In this GCC Clause 41, in calculating any monies due from the Purchaser to the Supplier, account shall be taken of any sum previously paid by the Purchaser to the Supplier under the Contract, including any advance payment paid **pursuant to the SCC.**

42. Assignment

42.l Neither the Purchaser nor the Supplier shall, without the express prior written consent of the other, assign to any third party the Contract or any part thereof, or any right, benefit, obligation, or interest therein or thereunder, except that the Supplier shall be entitled to assign either absolutely or by way of charge any monies due and payable to it or that may become due and payable to it under the Contract.

I. SETTLEMENT OF DISPUTES

43. Settlement of Disputes

43.1 Adjudication

43.1.1 If any dispute of any kind whatsoever shall arise between the Purchaser and the Supplier in connection with or arising out of the Contract, including without prejudice to the generality of the foregoing, any question regarding its existence, validity, or termination, or the operation of the System (whether during the progress of implementation or after its achieving Operational Acceptance and whether before or after the termination, abandonment, or breach of the Contract), the parties shall seek to resolve any such dispute by mutual consultation. If the parties fail to resolve such a dispute by mutual consultation within fourteen (14) days after one party has notified the other in writing of the dispute, then, if the Contract Agreement in Appendix 2 includes and names an Adjudicator, the dispute shall, within another fourteen (14) days, be referred in writing by either party to the Adjudicator, with a copy to the other party. If there is no Adjudicator specified in the Contract Agreement, the mutual consultation period stated above shall last twenty-eight (28) days (instead of fourteen), upon expiry of which either party may move to the notification of arbitration pursuant to GCC Clause 43.2.1.

43.1.2 The Adjudicator shall give his or her decision in writing to both parties within twenty-eight (28) days of the dispute being referred to the Adjudicator. If the Adjudicator has done so, and no notice of intention to commence arbitration has been given by either the Purchaser or the Supplier within fifty-six (56) days of such reference, the decision shall become final and binding upon the Purchaser and the Supplier. Any decision that has become final and binding shall be implemented by the parties forthwith.

43.1.3 The Adjudicator shall be paid an hourly fee at the rate specified in the Contract Agreement plus reasonable expenditures incurred in the execution of duties as Adjudicator, and these costs shall be divided equally between the Purchaser and the Supplier.

43.1.4 Should the Adjudicator resign or die, or should the Purchaser and the Supplier agree that the Adjudicator is not fulfilling his or her functions in accordance with the provisions of the Contract, a new Adjudicator shall be jointly appointed by the Purchaser and the Supplier. Failing agreement between the two within twenty-eight (28) days, the new Adjudicator shall be appointed at the request of either party by the Appointing Authority **specified in the SCC,** or, if no Appointing Authority is **specified in SCC,** the Contract shall, from this point onward and until the parties may otherwise agree on an Adjudicator or an Appointing Authority, be implemented as if there is no Adjudicator.

43.2 Arbitration

43.2.1 If

(a) the Purchaser or the Supplier is dissatisfied with the Adjudicator's decision and acts before this decision has become final and binding pursuant to GCC Clause 43.1.2, or

(b) the Adjudicator fails to give a decision within the allotted time from referral of the dispute pursuant to GCC Clause 43.1.2, and the Purchaser or the Supplier acts within the following fourteen (14) days, or

(c) in the absence of an Adjudicator from the Contract Agreement, the mutual consultation pursuant to GCC Clause 43.1.1 expires without resolution of the dispute and the Purchaser or the Supplier acts within the following fourteen (14) days,

then either the Purchaser or the Supplier may act to give notice to the other party, with a copy for information to the Adjudicator in case an Adjudicator had been involved, of its intention to commence arbitration, as provided below, as to the matter in dispute, and no arbitration in respect of this matter may be commenced unless such notice is given.

43.2.2 Any dispute in respect of which a notice of intention to commence arbitration has been given, in accordance with GCC Clause 43.2.1, shall be finally settled by arbitration. Arbitration may be commenced prior to or after Installation of the Information System.

43.2.3 Arbitration proceedings shall be conducted in accordance with the rules of procedure **specified in the SCC.**

43.3 Notwithstanding any reference to the Adjudicator or arbitration in this clause,

(a) the parties shall continue to perform their respective obligations under the Contract unless they otherwise agree;

(b) the Purchaser shall pay the Supplier any monies due the Supplier.

J. CYBER SECURITY

44. Cyber Security

44.1 **Pursuant to the SCC**, the Supplier, including its Subcontractors/ suppliers/ manufacturers shall take all technical and organizational measures necessary to protect the information technology systems and data used in connection with the Contract. Without limiting the foregoing, the Supplier, including its Subcontractors/ suppliers/ manufacturers, shall use all reasonable efforts to establish, maintain, implement and comply with, reasonable information technology, information security, cyber security and data protection controls, policies and procedures, including oversight, access controls, encryption, technological and physical safeguards and business continuity/disaster recovery and security plans that are designed to protect against and prevent breach, destruction, loss, unauthorized distribution, use, access, disablement, misappropriation or modification, or other compromise or misuse of or relating to any information technology system or data used in connection with the Contract.

APPENDIX 1

Fraud and Corruption

(Text in this Appendix shall not be modified)

1. Purpose

1.1 The Bank's Anti-Corruption Guidelines and this annex apply with respect to procurement under Bank Investment Project Financing operations.

2. Requirements

2.1 The Bank requires that Borrowers (including beneficiaries of Bank financing); bidders (applicants/proposers), consultants, contractors and suppliers; any sub-contractors, sub-consultants, service providers or suppliers; any agents (whether declared or not); and any of their personnel, observe the highest standard of ethics during the procurement process, selection and contract execution of Bank-financed contracts, and refrain from Fraud and Corruption.

2.2 To this end, the Bank:

a. Defines, for the purposes of this provision, the terms set forth below as follows:

i. "corrupt practice" is the offering, giving, receiving, or soliciting, directly or indirectly, of anything of value to influence improperly the actions of another party;

ii. "fraudulent practice" is any act or omission, including misrepresentation, that knowingly or recklessly misleads, or attempts to mislead, a party to obtain financial or other benefit or to avoid an obligation;

iii. "collusive practice" is an arrangement between two or more parties designed to achieve an improper purpose, including to influence improperly the actions of another party;

iv. "coercive practice" is impairing or harming, or threatening to impair or harm, directly or indirectly, any party or the property of the party to influence improperly the actions of a party;

v. "obstructive practice" is:

(a) deliberately destroying, falsifying, altering, or concealing of evidence material to the investigation or making false statements to investigators in order to materially impede a Bank investigation into allegations of a corrupt, fraudulent, coercive, or collusive practice; and/or threatening, harassing, or intimidating any party to prevent it from disclosing its knowledge of matters relevant to the investigation or from pursuing the investigation; or

(b) acts intended to materially impede the exercise of the Bank's inspection and audit rights provided for under paragraph 2.2 e. below.

b. Rejects a proposal for award if the Bank determines that the firm or individual recommended for award, any of its personnel, or its agents, or its sub-consultants, sub-contractors, service providers, suppliers and/ or their employees, has, directly

or indirectly, engaged in corrupt, fraudulent, collusive, coercive, or obstructive practices in competing for the contract in question;

c. In addition to the legal remedies set out in the relevant Legal Agreement, may take other appropriate actions, including declaring misprocurement, if the Bank determines at any time that representatives of the Borrower or of a recipient of any part of the proceeds of the loan engaged in corrupt, fraudulent, collusive, coercive, or obstructive practices during the procurement process, selection and/or execution of the contract in question, without the Borrower having taken timely and appropriate action satisfactory to the Bank to address such practices when they occur, including by failing to inform the Bank in a timely manner at the time they knew of the practices;

d. Pursuant to the Bank's Anti-Corruption Guidelines, and in accordance with the Bank's prevailing sanctions policies and procedures, may sanction a firm or individual, either indefinitely or for a stated period of time, including by publicly declaring such firm or individual ineligible (i) to be awarded or otherwise benefit from a Bank-financed contract, financially or in any other manner;[9] (ii) to be a nominated[10] sub-contractor, consultant, manufacturer or supplier, or service provider of an otherwise eligible firm being awarded a Bank-financed contract; and (iii) to receive the proceeds of any loan made by the Bank or otherwise to participate further in the preparation or implementation of any Bank-financed project;

e. Requires that a clause be included in bidding/request for proposals documents and in contracts financed by a Bank loan, requiring (i) bidders (applicants/proposers), consultants, contractors, and suppliers, and their sub-contractors, sub-consultants, service providers, suppliers, agents, personnel, permit the Bank to inspect[11] all accounts, records and other documents relating to the procurement process, selection and/or contract execution, and to have them audited by auditors appointed by the Bank.

---

9 For the avoidance of doubt, a sanctioned party's ineligibility to be awarded a contract shall include, without limitation, (i) applying for pre-qualification, expressing interest in a consultancy, and bidding, either directly or as a nominated sub-contractor, nominated consultant, nominated manufacturer or supplier, or nominated service provider, in respect of such contract, and (ii) entering into an addendum or amendment introducing a material modification to any existing contract.

10 A nominated sub-contractor, nominated consultant, nominated manufacturer or supplier, or nominated service provider (different names are used depending on the particular bidding document) is one which has been: (i) included by the bidder in its pre-qualification application or bid because it brings specific and critical experience and know-how that allow the bidder to meet the qualification requirements for the particular bid; or (ii) appointed by the Borrower.

11 Inspections in this context usually are investigative (i.e., forensic) in nature. They involve fact-finding activities undertaken by the Bank or persons appointed by the Bank to address specific matters related to investigations/audits, such as evaluating the veracity of an allegation of possible Fraud and Corruption, through the appropriate mechanisms. Such activity includes but is not limited to: accessing and examining a firm's or individual's financial records and information, and making copies thereof as relevant; accessing and examining any other documents, data and information (whether in hard copy or electronic format) deemed relevant for the investigation/audit, and making copies thereof as relevant; interviewing staff and other relevant individuals; performing physical inspections and site visits; and obtaining third party verification of information.

APPENDIX 2

Sexual Exploitation and Abuse (SEA) and/or Sexual Harassment (SH) Performance Declaration for Subcontractors

[The following table shall be filled in by each subcontractor proposed by the Supplier, that was not named in the Contract]

Subcontractor's Name: *[insert full name]*

Date: *[insert day, month, year]*
Contract reference *[insert contract reference]*
Page *[insert page number]* of *[insert total number]* pages

SEA and/or SH Declaration
We: ☐ (a) have not been subject to disqualification by the Bank for non-compliance with SEA/ SH obligations. ☐ (b) are subject to disqualification by the Bank for non-compliance with SEA/ SH obligations. ☐ (c) had been subject to disqualification by the Bank for non-compliance with SEA/ SH obligations, and were removed from the disqualification list. An arbitral award on the disqualification case has been made in our favor.
[*If (c) above is applicable, attach evidence of an arbitral award reversing the findings on the issues underlying the disqualification.*]
Period of disqualification: From: _____ To: _____

Name of the Subcontractor_____

Name of the person duly authorized to sign on behalf of the Subcontractor_____

Title of the person signing on behalf of the Subcontractor _____

Signature of the person named above _____

Date signed _____ day of _____, _____

Countersignature of authorized representative of the Supplier:

Signature: _____

Date signed _____ day of _____, _____

SECTION IX - SPECIAL CONDITIONS OF CONTRACT

Table of Clauses

A. Contract and Interpretation **376**

Definitions (GCC Clause 1) 376
Notices (GCC Clause 4) 377

B. Subject Matter of Contract **377**

Scope of the System (GCC Clause 7) 377
Time for Commencement and Operational Acceptance (GCC Clause 8) 378
Supplier's Responsibilities (GCC Clause 9) 378

C. Payment **380**

Contract Price (GCC Clause 11) 380
Terms of Payment (GCC Clause 12) 380
Securities (GCC Clause 13) 383

D. Intellectual Property **384**

Copyright (GCC Clause 15) 384
Software License Agreements (GCC Clause 16) 385
Confidential Information (GCC Clause 17) 386

E. Supply, Installation, Testing, Commissioning, and Acceptance of the System **386**

Representatives (GCC Clause 18) 386
Project Plan (GCC Clause 19) 386
Design and Engineering (GCC Clause 21) 388
Product Upgrades (GCC Clause 23) 388
Inspections and Tests (GCC Clause 25) 388
Commissioning and Operational Acceptance (GCC Clause 27) 388

F. Guarantees and Liabilities **389**

Operational Acceptance Time Guarantee (GCC Clause 28) 389
Defect Liability (GCC Clause 29) 390
Functional Guarantees (GCC Clause 30) 390

G. Risk Distribution **391**

Insurances (GCC Clause 37) 391

H. Change in Contract Elements **391**

Changes to the System (GCC Clause 39) 391

I. Settlement of Disputes **392**

Settlement of Disputes (GCC Clause 43) 392

J. Cyber Security **393**

Cyber Security (GCC Clause 44) 393

Special Conditions of Contract

The following Special Conditions of Contract (SCC) shall supplement or amend the General Conditions of Contract (GCC). Whenever there is a conflict, the provisions of the SCC shall prevail over those in the General Conditions of Contract. For the purposes of clarity, any referenced GCC clause numbers are indicated in the left column of the SCC.

A. CONTRACT AND INTERPRETATION

Definitions (GCC Clause 1)

GCC 1.1 (a) (ix)	The applicable edition of the Procurement Regulation is dated: September 2023.
GCC 1.1 (b) (i)	The Purchaser is: the Government of Samoa, acting through the Samoa Bureau of Statistics (SBS), Independent State of Samoa. Where the Contract places an obligation or a decision on the Purchaser, it is discharged by SBS unless stated otherwise.
GCC 1.1 (b) (ii)	*The Project Manager is:* *Mama Anisi Christian Tua* *Assistant Government Statistician (AGS),* *National ID Division Head,* *Email: nid@sbs.gov.ws* *Telephone: +685 26003* .
GCC 1.1 (e) (i)	The Purchaser's Country is: *the Independent State of Samoa.*
GCC 1.1 (e) (iii)	*The Project Sites are: the sites listed in the Site Table of the Technical Requirements: the main server room and the supervision cell in the SBS building in Apia, the Apia card personalisation centre, the Apia registration, adjudication and investigation offices, the Salelologa registration and card delivery site, the Vodafone data centre used as the disaster recovery site, and the itinerant enrolment sites on Upolu and Savai'i.*
GCC 1.1 (e) (x)	**There are no Special Conditions associated with GCC 1.1 (e) (x).**
GCC 1.1 (e) (xii)	*The Coverage Period is twenty four hours a day, seven days a week for severity 1 incidents, and 08:00 to 17:00 Samoa time from Monday to Friday, excluding the public holidays listed in the Technical Requirements, for all other severities.*
GCC 1.1 (e) (xiii)	The Post-Warranty Services Period is ***zero (0) months*** starting with the completion of the Warranty Period.

	The recurrent services quoted for years one and two are performed within the Warranty Period defined in the Special Conditions for GCC 29.4.

Notices (GCC Clause 4)

GCC 4.3	*Address of the Project Manager: Samoa Bureau of Statistics, 04 Apia City Boulevard, Level 1 and 2, Government FMFMII Building, Apia, Samoa; electronic mail nid@sbs.gov.ws.* *Fallback address of the Purchaser: Leota Aliielua Salani, Government Statistician, Samoa Bureau of Statistics, 04 Apia City Boulevard, Level 1 and 2, Government FMFMII Building, Apia, Samoa; electronic mail nid@sbs.gov.ws.* For Electronic Data Interchange (EDI) the Purchaser and Supplier will use the following standards, protocols, addresses, and procedures: *not applicable.*
GCC 5.1	*The Contract is governed by and interpreted in accordance with the laws of the Independent State of Samoa.*

B. SUBJECT MATTER OF CONTRACT

Scope of the System (GCC Clause 7)

GCC 7.3	The Supplier's obligations under the Contract will include the following recurrent cost items, as identified in the Recurrent Cost tables in the Supplier's Proposal: *R1 hardware maintenance of all Goods installed at the Project Sites; R2 software support, maintenance and updates for the identity management system, the biometric identification system, the identity verification services, the civil registration system, the card chain software and the supervision platform, being a support and update service and never a licence renewal; R3 operation of the support service and of the service level regime for all subsystems, including warranty support and post acceptance support; R4 reorders of card personalisation consumables at the unit rates of the Unit Rates Schedule; R5 reorders of enrolment consumables at the same rates. The blank card stock for the initial cohort is supplied once under the base scope and is not a recurrent item. The rates quoted for years one and two are firm and are not subject to adjustment.* The Supplier agrees to supply spare parts required for the operation and maintenance of the System, as stated below, for *five (5)* years beginning with Operational Acceptance. Moreover, the price of

	such spare parts shall be those specified in the spare parts price schedule submitted by the Suppler as part of its Proposal. These prices shall include the purchase price for such spare parts and other costs and expenses (including the Supplier's fees) relating to the supply of spare parts. *The spare parts and consumables are those of the Unit Rates Schedule of the Supplier's Proposal (reorders and post contract orders), together with the local buffer stock required by the Special Conditions for GCC 9.20 (a). The Supplier shall guarantee the availability of spare parts and consumables for all delivered equipment, and in particular for the enrolment kits, the tablets and the card printers, for the Warranty Period and for a further three (3) years thereafter, at the unit rates of the Unit Rates Schedule. The Supplier shall maintain the local buffer stock required by the Special Condition to GCC 9.20 (a) throughout the Warranty Period and the recurrent services period, and shall establish the licence and support contracts for third party components in the name of the Purchaser.*

Time for Commencement and Operational Acceptance (GCC Clause 8)

GCC 8.1	The Supplier shall commence work on the System within: *fourteen (14)* days from the Effective Date of the Contract.

Supplier's Responsibilities (GCC Clause 9)

GCC 9.1	*A health and safety manual is required. The Supplier shall submit it for approval within thirty (30) days of the Effective Date and shall not begin field enrolment activities before it is approved. It shall address at least field work at itinerant enrolment sites on Upolu and Savai'i, inter island travel by ferry and the handling and lifting of enrolment kits, electrical and laser safety at the card personalisation centre, emergency preparedness and response including cyclone conditions, and the reporting of incidents and accidents.*
GCC 9.8	The following sustainable procurement contractual provisions, apply: *the Supplier shall take back and dispose of, at its own cost and in accordance with the laws of Samoa, all packaging and all equipment it replaces under warranty. No other provision applies.*
GCC 9.18	The Supplier *is not required* to make security arrangements for the Project Site/s. *The Supplier remains responsible for the physical security of the blank card stock, of the personalisation consumables and of the equipment in its custody until Operational Acceptance of the relevant Subsystem.*
GCC 9.20 (a)	*Throughout the Contract Period the Supplier shall maintain in Samoa, itself or through the local representative or local partner named in its*

	Proposal: a first level support capability with staff trained and certified by the Supplier, receiving and triaging incidents in English and Samoan; a buffer stock of spare parts and consumables in secure local storage covering at least five percent (5 %) of each deployed equipment type and not fewer than two (2) units of each type of enrolment kit, tablet and card printer, together with the consumables needed for four (4) weeks of card production at the contracted rate; not fewer than two (2) locally based technical staff able to perform first diagnosis, hardware replacement and on site intervention; and the capability to carry out import clearance and customs handling and to move equipment, spare parts and consumables between Upolu and Savai'i. The Supplier shall acknowledge a severity 1 incident within one (1) hour at any time, and shall attend on site within four (4) hours at any Project Site on Upolu and within twenty four (24) hours at any Project Site on Savai'i. The buffer stock shall be replenished within thirty (30) days of any drawdown. The Supplier shall not reduce or terminate the local arrangement without the prior written approval of the Purchaser and the prior establishment of an equivalent arrangement. The Local Entity named in the Proposal shall remain engaged for the whole Contract, including the warranty and post acceptance support periods. It may be replaced only with the Purchaser's prior written approval, by an entity of equivalent capability. The skills transfer plan shall include named staff of the Local Entity among its beneficiaries.
GCC 9.20 (b)	*The Key Personnel are the six positions named in the Contract: Project Manager; ID Solution Architect and Biometrics / ABIS Specialist; Cyber Security and Data Protection Expert; Enrolment Operations Manager; Card Personalisation Manager; Deputy Local Project Manager. The Supplier shall not replace any of them without the prior written approval of the Purchaser. A proposed replacement shall have a reference experience and qualifications equivalent to or better than those of the person replaced, as assessed against Section III 1.5, shall be provided at no additional cost, and shall work alongside the outgoing person for at least ten (10) working days. The Deputy Local Project Manager, who acts as Training and Skills Transfer Lead, shall stay mobilised for the whole duration of the Contract and shall not be replaced unless the Supplier has first submitted, and the Purchaser has approved in writing, a transfer continuity plan.*

Purchaser's Responsibilities (GCC Clause 10)

GCC 10.12	*In addition to the responsibilities set out in GCC 10, the Purchaser shall pursue the legal prerequisites P1 to P5 listed in the Special Condition to GCC 40.1; provide and fit out the accommodation for the card personalisation centre, the supervision cell, the Apia registration, adjudication and investigation offices and the Salelologa site; carry out customs clearance; plan and run the field operations of the mass registration campaign, including the enrolment teams and the site programme; provide and administer the Purchaser source code repository and the infrastructure on which the Supplier operates the build and test pipelines; and designate the staff to be trained and release them for the training and pairing activities.*

C. PAYMENT

Contract Price (GCC Clause 11)

GCC 11.2	Adjustments to the Contract Price shall be as follows: *not applicable. The Contract Price, including the recurrent prices quoted for years one and two and the unit rates of the Unit Rates Schedule, is firm and is not subject to any alteration except in the event of a Change under GCC 39..*

Terms of Payment (GCC Clause 12)

GCC 12.1	Subject to the provisions of GCC Clause 12 (Terms of Payment), the Purchaser shall pay the Contract Price to the Supplier according to the categories and in the manner specified below. (a) Advance Payment ten percent (10%) of the entire Contract Price, exclusive of all Recurrent Costs, shall be paid against receipt of a claim accompanied by the Advance Payment Security specified in GCC Clause 13.2. The advance payment is outside the milestone shares set out below and is additional to them. It is recovered pro rata by deduction from each of the milestone payments M1 to M9, including M6b and M6c, in proportion to the share of each milestone, so that the advance is fully recovered when milestone M9 is paid. No deduction is made from the release of the skills transfer retention. (b) Milestone payments The Purchaser pays the Contract Price of the base scope against the milestones of the Implementation Schedule, in the following shares of that price: M1 five percent (5 %); M2 fifteen percent (15 %); M3 five percent (5 %); M4 fifteen percent (15 %); M5 and M6 together ten percent (10 %); M6b ten percent (10 %); M6c ten percent (10 %); M7 ten percent (10 %); M8 five percent (5 %); M9 five percent (5 %); release of the skills transfer retention ten percent (10 %). These shares total one hundred percent (100 %) of the price of the base scope. The base scope does not include the civil registration platform option, and no payment of the base scope depends on the exercise of that option. Each payment falls due on the explicit written approval of the Purchaser recording that the acceptance criterion of that milestone is met, and on no other event. (c) Milestone acceptance criteria

	Payment is due only on the written instrument named. Advance: the Advance Payment Security received and verified. M1: written approval of the detailed design file, covering the system design, the card design, the enrolment workflow and the site fit out specifications. M2: a delivery certificate recording that fifty (50) enrolment kits and ten (10) tablets have been delivered in country in conformity with the Contract, inspected, and that the capture application is installed and has passed the kit configuration acceptance tests. M3: the first production enrolments recorded in the live System at an authorised site, confirmed in writing by the Project Manager. M4: the Operational Acceptance Certificate of release V1, evidencing an end to end demonstration from enrolment through deduplication, allocation of the identification number and processing in the identity management system to issuance of the credential. M5 and M6: sixty thousand (60,000) activated identities counted by the reporting function of the System and verified by the Purchaser, and continuous registration open at the permanent offices. M6b: the Operational Acceptance Certificate of the card production chain, evidencing production at the contracted rate, quality control within the contractual thresholds and the non proprietary security features demonstrated on produced cards. M6c: a delivery certificate recording that cards have been produced and delivered to the designated issuance points for the whole release V1 cohort whose legal identity has been confirmed, the register reconciled and approved in writing by the Project Manager. M7: a delivery and acceptance certificate for the civil registration base components, evidencing the registration database and the interoperable back end in operation, the stock preload executed and the write back of the identification number demonstrated. M8: the Operational Acceptance Certificate of the identity verification services issued without reservations. M9: the pilot completion reports of the relying party pilots approved by the Purchaser, with the piloted services in production without reservations. Retention: the final skills transfer assessment report scored under the Special Condition to GCC 12.1 (d) and approved by the Purchaser. (d) Skills transfer retention Ten percent (10 %) of the Contract Price, exclusive of Recurrent Costs, is retained and released only against the final skills transfer assessment. The assessment is carried out by the Purchaser, which may be assisted by its supervision consultant, at the date fixed in the Implementation Schedule and at the latest six (6) months after Operational Acceptance of release V2. The Supplier is given the draft assessment and fourteen (14) days to comment, and its comments are recorded in the final report. Each criterion is scored on the scale zero to four. The release score is computed only from the criteria evidenced by a recorded event: deployments performed by the Purchaser teams themselves, evidenced by the

	deployment log showing no Supplier intervention, weight twenty five; card production autonomy on both sites, evidenced by the production of a full batch by the Purchaser alone at a reject rate within the contractual threshold, weight fifteen; code, configurations and continuous integration operated in the Purchaser repository, evidenced by the repository history and by builds reproduced by the Purchaser, weight ten; day to day operations run by the Purchaser, evidenced by on call duty held by the Purchaser and by a failover test led by the Purchaser, weight ten. The release score is the sum over those four criteria of the score multiplied by the weight, divided by the sum over the same criteria of four multiplied by the weight, expressed as a percentage. One hundred percent (100 %) of the retention is released at a release score of seventy five or above; between fifty and seventy five it is released pro rata on a straight line; below fifty nothing is released, the Supplier shall execute a remediation plan approved by the Purchaser over six (6) months, and a single re evaluation is then carried out on the same basis. The remaining criteria of the assessment grid are assessed and reported but do not affect the release of the retention. (e) Civil registration option If the Purchaser exercises the civil registration platform option, the option price is paid in two equal instalments: fifty percent (50 %) on the acceptance certificate of milestone M10, recording the civil registration flow live for new vital events and the legacy data migration completed and reconciled, and fifty percent (50 %) on the Operational Acceptance Certificate of milestone M11, recording that the new system has become the national register of record and the legacy system archived. If the option is not exercised, no sum is due and no payment of the base scope is affected. (f) Recurrent Costs one hundred percent (100%) of the price of the services actually delivered will be paid quarterly in arrears, on submission and Purchaser’s approval of invoices. The recurrent prices are invoiced quarterly in arrears for each of the years one and two counted from Operational Acceptance of the release to which they relate. Each invoice states the service level results of the quarter and the penalties accrued under the Special Condition to GCC 30, which are deducted from that invoice.
GCC 12.3	The Purchaser shall pay to the Supplier interest on the delayed payments at a rate of: *six (6) percent* per annum.

GCC 12.4	The Supplier will invoice the Purchaser in the currency used in the Contract Agreement and the Price Schedules it refers to, for Goods and Services supplied locally, and the conversion between this currency and *the Samoan Tala (WST)* for payment purposes - in case the two currencies are different - will be made as of the actual payment date using the exchange rate found in *the selling rate published by the Central Bank of Samoa.* *The Supplier shall invoice Goods and Services supplied locally in Samoan Tala and all other Goods and Services in United States Dollars, in each case in the currency of the corresponding line of the Price Schedules.*
GCC 12.5	*Payment of the foreign currency portion shall be made by direct bank transfer to the account nominated in writing by the Supplier. The documentary credit mechanism does not apply.*
GCC 12.6	*GCC Clause 12.6 applies. If the Supplier fails to perform a cyber security obligation of the Contract, the Project Manager may assess an amount and the Purchaser may withhold it from any payment due until that obligation has been performed.*

Securities (GCC Clause 13)

GCC 13.2.1	*The Advance Payment Security is a bank guarantee in the amount and currency of the advance payment, provided within twenty eight (28) days of the notification of Contract award. It remains valid until the advance payment has been fully recovered under the Special Condition to GCC 12.1 (a), and not merely until Operational Acceptance of the System. Its amount may be progressively reduced by the amounts recovered.*
GCC 13.3.1	The Performance Security shall be denominated in *United States Dollars* for an amount equal to *ten (10)* percent of the Contract Price, excluding any Recurrent Costs. *The Performance Security shall be a bank guarantee.*
GCC 13.3.4	During the Warranty Period (i.e., after Operational Acceptance of the System), the Performance Security remains at *ten (10)* percent of the Contract Price, excluding any Recurrent Costs. *The Performance Security is not reduced on Operational Acceptance. It remains valid until twenty eight (28) days after the end of the Warranty Period of the last release accepted.*

D. INTELLECTUAL PROPERTY

Copyright (GCC Clause 15)

GCC 15.3	***There are no Special Conditions of Contract applicable to GCC Clause 15.3***
GCC 15.4	***The Intellectual Property Rights in all Custom Software and Custom Materials vest in the Purchaser. They include the custom code, all configurations and parameter sets, the business process and decision models, the card design and its artwork and personalisation layouts, the build and deployment scripts, the test assets, and all documentation produced under the Contract. The Supplier shall maintain the source code of all custom and open source components, together with the configurations and parameter sets, in the Purchaser source code repository under version control, with automated build and test pipelines operational in that repository from the start of development, and shall ensure that every release is reproducible from that repository. This material is delivered directly to the Purchaser and is not placed in escrow. The Supplier shall document all application programming interfaces without restriction and shall charge no fee or royalty for their use.***
GCC 15.5	***Escrow arrangements are required for Software written or adapted for the System, and for packaged software specific to the System, whose full source code is not delivered to the Purchaser. Standard Software that is widely available on the market under standard licence terms, such as operating systems, database management systems, office tools and security tools, is not subject to escrow. For the biometric identification system, escrow is one option: the Supplier may instead meet the outcome of SAM-IDM-137 through the exit guarantees of Section VII, namely the original biometric images kept under the control of the Purchaser (SAM-IDM-099), storage and exchange in the formats of ISO/IEC 19794 and ISO/IEC 39794 (SAM-ARC-028), and the complete export of the gallery for its rebuild by another supplier (SAM-ARC-038). The route chosen is stated in the Proposal. Where escrow applies, the Supplier shall enter into, within sixty (60) days of the Effective Date, a tripartite escrow agreement between the Supplier, the Purchaser and an independent escrow agent acceptable to the Purchaser. The deposit shall comprise the source code, the build scripts and build environment description, the design documentation, the deployment and operating documentation, and any licence keys and certificates needed to build and run the component. The deposit shall be renewed at every major version and at least once a year, and the escrow agent shall verify at each deposit that the material is complete and that the component can be built from it. The Purchaser is entitled to release of the deposit on the insolvency of the Supplier or of the owner of the component or***

	the cessation of its business; the end of support of the product by its owner; a breach by the Supplier of its maintenance obligations that remains unremedied thirty (30) days after written notice; or a refusal to renew support on reasonable commercial terms. On release, the Purchaser may use, reproduce, modify and have modified the deposited material for its own operation and maintenance of the System, in perpetuity. The Supplier bears the cost of the escrow arrangement during the Contract Period and the Warranty Period.

Software License Agreements (GCC Clause 16)

GCC 16.1 (a) (ii)	***The rights of use granted to the Purchaser over the whole delivered scope are perpetual, irrevocable and fully paid up. They do not terminate on termination of the Contract and they survive the expiry of the Contract Period, the Warranty Period and the recurrent services. No fee, subscription, licence renewal, licence key, time limit, activation mechanism or other technical measure may suspend, disable or degrade the right of the Purchaser to use the System. The Supplier shall deliver, before Operational Acceptance of each release, all licence keys and certificates required to operate that release, including perpetual keys where the component uses key based activation.***
GCC 16.1 (a) (iii)	***The rights of use are valid throughout the territory of Samoa and, for hosting, replication, backup and disaster recovery, on any site used by or on behalf of the Purchaser.***
GCC 16.1 (a) (iv)	***The rights of use are subject to no restriction as to the number of enrolled or registered persons, records, transactions, authentications, named or concurrent users, workstations, processor cores, virtual machines, sites or instances, and no additional charge arises from growth in any of those.***
GCC 16.1 (b) (vi)	***The Purchaser may disclose the Software and Materials to, and have them reproduced and used by, its support service suppliers and their subcontractors, the supervision consultant and any adviser it appoints, and any agency of the Government of Samoa acting as a relying party or as successor to the functions of the Purchaser. Any such person is bound by the same restrictions as those set out in the Contract.***
GCC 16.1 (b) (vii)	***There are no Special Conditions of Contract applicable to GCC Clause 16.1 (b) (vii)***
GCC 16.2	***There are no Special Conditions of Contract applicable to GCC Clause 16.2***

Confidential Information (GCC Clause 17)

GCC 17.1	**The obligations of GCC 17 apply to all personal data, biometric data and identity records handled under the Contract, and are read together with the National Digital Identification Act 2024 and the regulations made under it. The Supplier shall not access, use, copy, transfer outside Samoa or retain any such data except as strictly necessary to perform the Contract and as authorised in writing by the Purchaser, and shall return or destroy it on the instruction of the Purchaser. These obligations survive the termination or expiry of the Contract without limit of time.**

E. SUPPLY, INSTALLATION, TESTING, COMMISSIONING, AND ACCEPTANCE OF THE SYSTEM

Representatives (GCC Clause 18)

GCC 18.1	***There are no Special Conditions of Contract applicable to GCC Clause 18***
GCC 18.2.2	***The Supplier Representative, or a deputy approved in writing by the Purchaser with the same authority, shall be resident in Apia and available on site during the installation of the System, the mass enrolment campaign, the Operational Acceptance of release V1 and of the card production chain, and, if the civil registration platform option is exercised, the civil registration cutover.***

Project Plan (GCC Clause 19)

GCC 19.1	Chapters in the Project Plan shall address the following subject**:** ***(a) Project organisation, staffing and management, including quality assurance, configuration management and problem escalation;*** ***(b) Implementation plan for release V1 and release V2;*** ***(c) Delivery, installation and site fit out plan;*** ***(d) Training and skills transfer plan responding to the capacity building annex;*** ***(e) Testing and quality assurance plan;***

	(f) Data migration and preloading plan; ***(g) Cyber security risk management plan;*** ***(h) Risk management plan including the procurement lead time of the enrolment kits;*** ***(i) Support and service level operating plan;*** ***(j) Environmental and social management plan;*** Further details regarding the required contents of each of the above chapters are contained in the Technical Requirements, *in particular parts C and F of the Technical Requirements and the annex to 2.4 on skills transfer and capacity building*.
GCC 19.5	***The Supplier shall submit Monthly Progress Reports and shall attend a monthly joint project review at which progress, deviations, corrective actions and Purchaser dependencies are recorded in minutes signed by both parties.***
GCC 19.6	***(i) monthly inspection and quality assurance reports;*** ***(ii) monthly training results per participant against the depth targets of the skills transfer plan;*** (i) ***(iii) monthly log of service calls and problem resolutions;*** (ii) *(iv) monthly report on status of compliance to cyber security risks management, and any foreseeable cyber security risk and mitigation, covering vulnerability management, patch status and the findings of the most recent penetration test;* (iii) *(v) a monthly service report stating measured service level values, breaches, incidents, penalties accrued and corrective actions. The Supplier shall attend a quarterly service review.*
GCC 19.7	*The Supplier shall inform the Project Manager of any significant cyber incident affecting the System or the data used in connection with the Contract immediately on becoming aware of it, and in any event no later than twenty four (24) hours after detection. The initial notification shall state the nature of the incident, the systems and data affected, the containment measures taken and the assistance required. Full details shall be provided within seven (7) days and a root cause analysis with a remediation plan within thirty (30) days. This obligation applies equally to any suspected or actual compromise of personal or biometric data and to any incident affecting a Subcontractor that touches the System.*

Design and Engineering (GCC Clause 21)

GCC 21.3.1	***The following are Controlling Technical Documents requiring the approval of the Project Manager before the related downstream work is undertaken: the detailed design file, comprising the system design, the card design and the enrolment workflow design; the site fit out specifications; the security architecture and the cyber security risk management plan; the master test plan and the Operational Acceptance Test specifications of each release; the data migration and preloading plan; and, if the civil registration platform option is exercised, the civil registration cutover and rollback plan.***

Transportation (GCC Clause 22)

GCC 22.4.1	***Delivery is on CIP Apia terms. The Supplier is responsible for and bears the cost of transport of the Goods to each Project Site, including inter island transport between Upolu and Savai'i and transport to the itinerant enrolment sites, and shall pack the Goods so as to withstand maritime and road transport and open air handling in Samoa.***

Product Upgrades (GCC Clause 23)

GCC 23.4	***The Supplier shall provide at no additional cost all new versions, releases and updates of the Standard Software used in the System during the Warranty Period and during the recurrent services of years one and two, and shall install them, test them and document them under the agreed change and release procedure.***

Inspections and Tests (GCC Clause 25)

GCC 25	***There are no Special Conditions of Contract applicable to GCC Clause 25.***

Commissioning and Operational Acceptance (GCC Clause 27)

GCC 27.2.1	***Installation, Commissioning and Operational Acceptance are carried out individually for the following components, and a separate Operational Acceptance Certificate is issued for each: release V1 of the system, comprising enrolment, the identity management system, deduplication, allocation of the identification number and issuance of the digital credential, corresponding to milestone***

	M4; the card production chain, corresponding to milestone M6b, whose acceptance requires the demonstration of production at the contracted rate, of quality control within the contractual thresholds and of the non proprietary security features on cards produced during the test; release V2 of the identity verification and authentication services, corresponding to milestone M8; and, if the civil registration platform option is exercised, the civil registration system, corresponding to milestone M11. Before the Operational Acceptance of release V1, of release V2 and of the civil registration system, the Operational Acceptance Test shall include a supervised pilot period of production operation, of the duration set in the Technical Requirements, during which the measured service levels are recorded and shall be met.

F. GUARANTEES AND LIABILITIES

Operational Acceptance Time Guarantee (GCC Clause 28)

GCC 28.2	***If the Supplier fails to achieve a liquidated damages milestone by the date fixed in the Implementation Schedule or the Agreed Project Plan, or by any extension granted under GCC 40, the Supplier shall pay liquidated damages at the rate of one half of one percent (0.5 %) per week of delay, or part of a week, applied to the price of the supplies and services of the delayed milestone as shown in the Price Schedules, and not to the whole Contract Price. The aggregate of all liquidated damages shall not exceed ten percent (10 %) of the Contract Price, excluding Recurrent Costs. Once that maximum is reached the Purchaser may consider termination.***
GCC 28.3	***Liquidated damages apply to the following milestones and to no other: M2, delivery and acceptance of the enrolment kits and tablets with the capture application; M4, Operational Acceptance of release V1; M5, sixty thousand (60,000) persons enrolled and processed; M6b, Operational Acceptance of the card production chain; and, if the civil registration platform option is exercised, M11, the civil registration cutover. For milestone M5 liquidated damages are due only to the extent that the delay is attributable to the Supplier, and none is due for delay attributable to the field operations of the Purchaser. No liquidated damages are due for any period covered by an extension of time granted under GCC 40.***

Defect Liability (GCC Clause 29)

GCC 29.1	***There are no Special Conditions of Contract applicable to GCC Clause 29.1.***
GCC 29.4	***The Warranty Period is twenty four (24) months and commences, for each release and for each Subsystem separately accepted, on the date of its own Operational Acceptance. The Warranty Period of the card production chain commences at milestone M6b.***
GCC 29.10	***During the Warranty Period the Supplier shall meet the following times, measured automatically from the ticketing tool, which shall be accessible to the Purchaser at all times: severity 1, production service down or major security incident, response within one (1) hour at any time, workaround within four (4) hours, resolution within twenty four (24) hours; severity 2, significant degradation or a key function unavailable with no acceptable workaround, response within one (1) hour, workaround within eight (8) hours, resolution within seventy two (72) hours; severity 3, a degraded function with a workaround and no service interruption, response within four (4) working hours, workaround within three (3) working days, resolution in the next maintenance release; severity 4, no operational impact, response within one (1) working day, resolution in the next planned release.***

Functional Guarantees (GCC Clause 30)

GCC 30	***The service levels set out in the Technical Requirements form part of the functional guarantees of the System. They apply from the Operational Acceptance of each release and throughout the Warranty Period and the recurrent services period. Each breach is assigned the severity stated for it in the service level table. Penalties are computed quarterly by applying, to the amount invoiced for the recurrent services of the quarter in which the breach occurred, one percent (1 %) for a severity 1 breach, two percent (2 %) for severity 2, three percent (3 %) for severity 3, four percent (4 %) for severity 4 and five percent (5 %) for severity 5. This is the only service level penalty regime under the Contract. The aggregate of service level penalties in a contract year shall not exceed ten percent (10 %) of the recurrent invoice of that year. Penalties arising from the breach of a deadline fixed by the National Digital Identification Act 2024 or by a regulation made under it are capped separately at fifteen percent (15 %) of that same invoice and do not count towards the ten percent cap. No penalty is due where the breach is attributable to facilities furnished by the Purchaser, or to an act or omission of the Purchaser or of its personnel, in accordance with the attribution rule of the service level table. Service level penalties are not liquidated damages within the meaning of***

	GCC 28, are additional to any liquidated damages, and are deducted from the recurrent invoice of the quarter concerned. The service level definitions, measurement methods and targets are fixed by the Contract and may be changed only by a Change Order issued under GCC 39.
GCC 32	***There are no Special Conditions of Contract applicable to GCC Clause 32.***

G. RISK DISTRIBUTION

Insurances (GCC Clause 37)

GCC 37.1 (c)	The Supplier shall obtain Third-Party Liability Insurance in the amount of *one million United States Dollars (USD 1,000,000) per occurrence with* deductible limits of no more than *ten thousand United States Dollars (USD 10,000).* The insured Parties shall be *the Supplier, its Subcontractors and the Purchaser.* The Insurance shall cover the period from *the Effective Date of the Contract* until *the end of the Warranty Period of the last release accepted.*
GCC 37.1 (e)	***The Supplier shall also take out and maintain marine cargo insurance covering inter island maritime transport between Upolu and Savai'i, for one hundred and ten percent (110 %) of the value of the Goods carried on each voyage; property insurance covering the equipment supplied under the Contract at all Project Sites and at the itinerant enrolment sites, including equipment in transit and equipment held in the local buffer stock, for its replacement value; and workers compensation and employer liability insurance in accordance with the laws of Samoa for all its personnel and those of its Subcontractors working in Samoa. The Purchaser shall be named as co insured under each of these policies.***

H. CHANGE IN CONTRACT ELEMENTS

Changes to the System (GCC Clause 39)

GCC 39.2.1	***A Request for Change Proposal shall include, in addition to the items listed in GCC 39.2.1, sufficient information to assess the cyber security risks arising from the Change, and a statement of the effect of the Change on the service levels and on the skills transfer obligations.***

GCC 39.4	**Value Engineering** The Purchaser ***will*** consider a Value Engineering Proposal. When the Purchaser will consider a Value Engineering Proposal and if the value engineering proposal is approved by the Purchaser the amount to be paid to the Supplier shall be *fifty (50)* percent of the reduction in the Contract Price.

Extension of Time for Achieving Operational Acceptance (GCC Clause 40)

GCC 40.1	***The following legal steps are the responsibility of the Purchaser and are matters specifically mentioned in the Contract for the purposes of GCC 40.1 (d): P1, the commencement order bringing into force the part of the National Digital Identification Act 2024 on registration; P2, the regulation fixing the length of the identification number and of the token and the checksum formula; P3, the commencement order for the part of that Act on the identification number, credentials and authentication, and the publication of the list of relying parties; P4, the regulation on the machine readability of credentials, including the QR code; P5, the publications in the Savali required for continuous registration and for the feeding of the Identity Database from civil registration. If any of these steps is not completed by the date shown for it in the Implementation Schedule, the time for achieving Operational Acceptance of every milestone that depends on it is extended by the period of the delay, and no liquidated damages are due in respect of that period. The Supplier shall give the notice required by GCC 40.2 and shall use its reasonable efforts to minimise the effect of the delay.***

I. SETTLEMENT OF DISPUTES

Settlement of Disputes (GCC Clause 43)

GCC 43.1.4	The Appointing Authority for the Adjudicator is: *In the event of a failure to agree on the appointment of an adjudicator within (28) days of a request by either party, the Adjudicator shall be appointed by the****:*** **United Nations Commission on International Trade Law (UNCITRAL)** *Fee Sharing and Payment Terms:* • The Adjudicator shall be paid an hourly fee as agreed during the contract negotiations (or fixed by the Appointing Authority), plus reasonable reimbursement expenses incurred in the performance of their duties. • All fees, costs and expenses of the Adjudicator shall be divided equally. (50% by the Purchaser and 50% by the Supplier).

	• The place of arbitration shall be in: ***APIA*** Each party shall pay its share of the Adjudicator's fees directly upon receipt of the Adjudicator's itemised invoices. The purchaser's obligations hereunder shall be payable from the allocated project contingency under the project budget.
GCC 43.2.3	If the Supplier is from outside the Purchaser's Country arbitration proceedings shall be conducted in accordance with the rules of arbitration of *UNCITRAL.* These rules, in the version in force at the time of the request for arbitration, will be deemed to form part of this Contract. *The number of arbitrators is three. The seat of the arbitration is Singapore. The language of the arbitration is English. The appointing authority is the Secretary General of the Permanent Court of Arbitration at The Hague.* If the Supplier is a national of the Purchaser's Country, any dispute between the Purchaser and a Supplier arising in connection with the present Contract shall be referred to arbitration in accordance with the laws of the Purchaser's country.

J. CYBER SECURITY

Cyber Security (GCC Clause 44)

GCC 44.1	Cyber Security applies. The technical and organisational measures required of the Supplier are those set out in the cyber security chapter of the Technical Requirements. The Supplier shall obtain an independent penetration test by a third party firm, which shall not be the Supplier or one of its Subcontractors, before each Operational Acceptance and at least once a year thereafter, and shall remediate the findings within the time allowed for their severity. Cyber security incidents are reported under the Special Condition to GCC 19.7, and failure to perform a cyber security obligation carries the withholding provided by the Special Condition to GCC 12.6.

SECTION X - CONTRACT FORMS

Notes to Proposers on working with the Sample Contractual Forms

The following forms are to be completed and submitted by the successful Proposer following receipt of the Letter of Acceptance from the Purchaser: (i) Contract Agreement, with all Appendices; (ii) Performance Security; and (iii) Advance Payment Security.

- Contract Agreement: In addition to specifying the parties and the Contract Price, the Contract Agreement is where the: (i) Supplier Representative; (ii) if applicable, agreed Adjudicator and his/her compensation; and (iii) the List of Approved Subcontractors are specified. In addition, modifications to the successful Proposer's Proposal Price Schedules are attached to the Agreement. These contain corrections and adjustments to the Supplier's Proposal prices to correct errors, adjust the Contract Price to reflect – if applicable - any extensions to Proposal validity beyond the last day of original Proposal validity plus 56 days, etc.
- Performance Security: Pursuant to GCC Clause 13.3, the successful Proposer is required to provide the Performance Security in the form contained in this section of this request for proposals document and in the amount specified in accordance with the SCC.
- Advance Payment Security: Pursuant to GCC Clause 13.2, the successful Proposer is required to provide a bank guarantee for the full amount of the Advance Payment - if an Advance Payment is specified in the SCC for GCC Clause 12.1 - in the form contained in this section of this request for proposals document or another form acceptable to the Purchaser. If a Proposer wishes to propose a different Advance Payment Security form, it should submit a copy to the Purchaser promptly for review and confirmation of acceptability before the proposal submission deadline.

The Purchaser and Supplier will use the following additional forms during Contract implementation to formalize or certify important Contract events: (i) the Installation and Operational Acceptance Certificates; and (ii) the various Change Order forms. These and the procedures for their use during performance of the Contract are included in the request for proposals document for the information of Proposers.

Table of Contract Forms

Notification of Intention to Award **396**

Beneficial Ownership Disclosure Form **400**

Letter of Acceptance **402**

1. Contract Agreement **403**

Appendix 1. Supplier's Representative 406
Appendix 2. Adjudicator 407
Appendix 3. List of Approved Subcontractors 408
Appendix 4. Categories of Software 409
Appendix 5. Custom Materials 410
Appendix 6. Revised Price Schedules 411
Appendix 7. Minutes of Contract Finalization Discussions and Agreed-to Contract Amendments 412

2. Performance and Advance Payment Security Forms **414**

2.1 Performance Security Form (Bank Guarantee) 415
2.2 Advance Payment Security Bank Guarantee 416

3. Installation and Acceptance Certificates **419**

3.1 Installation Certificate 420
3.2 Operational Acceptance Certificate 420

4. Change Order Procedures and Forms **421**

4.1 Request for Change Proposal Form 422
4.2 Change Estimate Proposal Form 424
4.3 Estimate Acceptance Form 425
4.4 Change Proposal Form 426
4.5 Change Order Form 428
4.6 Application for Change Proposal Form 430

NOTIFICATION OF INTENTION TO AWARD

***[This Notification of Intention to Award shall be sent to each Proposer that submitted a Proposal, unless the Proposer has previously received notice of exclusion from the process** Proposer.]*

[Send this Notification to the Proposer's Authorized Representative named in the Proposer Information Form]

For the attention of Proposer's Authorized Representative

Name: *[insert **Authorized Representative's name**]*

Address: *[insert **Authorized Representative's Address**]*

Telephone/Fax numbers: *[insert **Authorized Representative's telephone/fax numbers**]*

Email Address: *[insert **Authorized Representative's email address**]*

[IMPORTANT: insert the date that this Notification is transmitted to all participating Proposers. The Notification must be sent to all Proposers simultaneously. This means on the same date and as close to the same time as possible.]

DATE OF TRANSMISSION: This Notification is sent by: *[specify **email / fax**]* on *[specify **date**]* (local time)

Notification of Intention to Award

Purchaser: *[insert **the name of the Purchaser**]*

Project: *[insert **name of project**]*

Contract title: *[insert the **name of the contract**]*

Country: *[insert **country where RFP is issued**]*

Loan No. /Credit No. / Grant No.: *[insert **reference number for loan/credit/grant**]*

RFP No: *[insert RFP **reference number from Procurement Plan**]*

This Notification of Intention to Award (Notification) notifies you of our decision to award the above contract. The transmission of this Notification begins the Standstill Period. During the Standstill Period you may:

a) request a debriefing in relation to the evaluation of your Proposal, and/or

b) submit a Procurement-related Complaint in relation to the decision to award the contract.

1. The successful Proposer

Name:	[*insert name of successful Proposer*]

Address:	[*insert address of the successful Proposer*]
Contract price:	[*insert contract price of the successful Proposer*]
Total combined score:	[*insert the total combined score of the successful Proposer*]

2. Other Proposers *[INSTRUCTIONS: insert names of all Proposers that submitted a Proposal, Proposal prices as read out and evaluated, technical scores and combined scores.]*

Name of Proposer	Technical Score (If applicable)	Proposal price	Evaluated Proposal Cost	Combined Score
[*insert name*]	[*insert Technical score*]	[*insert Proposal price*]	[*insert evaluated cost*]	[*insert combined score*]
[*insert name*]	[*insert Technical score*]	[*insert Proposal price*]	[*insert evaluated cost*]	[*insert combined score*]
[*insert name*]	[*insert Technical score*]	[*insert Proposal price*]	[*insert evaluated cost*]	[*insert combined score*]

3. Reason/s why your Proposal was unsuccessful *[Delete if the combined score already reveals the reason]*

[INSTRUCTIONS; State the reason/s why this Proposer's Proposal was unsuccessful. Do NOT include: (a) a point by point comparison with another Proposer's Proposal or (b) information that is marked confidential by the Proposer in its Proposal.]

4. How to request a debriefing

DEADLINE: The deadline to request a debriefing expires at midnight on *[insert date]* (local time).

You may request a debriefing in relation to the results of the evaluation of your Proposal. If you decide to request a debriefing your written request must be made within three (3) Business Days of receipt of this Notification of Intention to Award.

Provide the contract name, reference number, name of the Proposer, contact details; and address the request for debriefing as follows:

Attention: [*insert full name of person, if applicable*]

Title/position: [*insert title/position*]

Agency: [*insert name of Purchaser*]

Email address: [*insert email address*]

Fax number: [*insert fax number or state "not applicable"*]

If your request for a debriefing is received within the 3 Business Days deadline, we will provide the debriefing within five (5) Business Days of receipt of your request. If we are unable to provide the debriefing within this period, the Standstill Period shall be extended by five (5) Business Days after the date that the debriefing is provided. If this happens, we will notify you and confirm the date that the extended Standstill Period will end.

The debriefing may be in writing, by phone, video conference call or in person. We shall promptly advise you in writing how the debriefing will take place and confirm the date and time.

If the deadline to request a debriefing has expired, you may still request a debriefing. In this case, we will provide the debriefing as soon as practicable, and normally no later than fifteen (15) Business Days from the date of publication of the Contract Award Notice.

5. How to make a complaint

DEADLINE: The deadline for submitting a Procurement-related Complaint challenging the decision to award the contract expires on midnight, *[insert date]* (local time).

Provide the contract name, reference number, name of the Proposer, contact details; and address the Procurement-related Complaint as follows:

Attention: [*insert full name of person, if applicable*]

Title/position: [*insert title/position*]

Agency: [*insert name of Purchaser*]

Email address: [*insert email address*]

Fax number: [*insert fax number or state "not applicable"*]

At this point in the procurement process, you may submit a Procurement-related Complaint challenging the decision to award the contract. You do not need to have requested, or received, a debriefing before making this complaint. Your complaint must be submitted within the Standstill Period and received by us before the Standstill Period ends.

For more information see the "Procurement Regulations for IPF Borrowers (Procurement Regulations) (Annex III)." You should read these provisions before preparing and submitting your complaint. In addition, the World Bank's Guidance "How to make a Procurement-related Complaint" provides a useful explanation of the process, as well as a sample letter of complaint.

In summary, there are four essential requirements:

1. You must be an 'interested party'. In this case, that means a Proposer who submitted a Proposal in this procurement, and is the recipient of a Notification of Intention to Award.
2. The complaint can only challenge the decision to award the contract.
3. You must submit the complaint within the deadline stated above.
4. You must include, in your complaint, all of the information required by the Procurement Regulations (as described in Annex III).

6. Standstill Period

DEADLINE: The Standstill Period is due to end at midnight on *[insert date]* (local time).

The Standstill Period lasts ten (10) Business Days after the date of transmission of this Notification of Intention to Award.

The Standstill Period may be extended. This may happen where we are unable to provide a debriefing within the five (5) Business Day deadline. If this happens we will notify you of the extension.

If you have any questions regarding this Notification please do not hesitate to contact us.

On behalf of the Purchaser:

Signature: _____

Title/position: [*insert* ***title/position***]

Agency: [*insert* ***name of Purchaser***]

Email address: [*insert* ***email address***]

Telephone number: [insert ***telephone number****]*

BENEFICIAL OWNERSHIP DISCLOSURE FORM

INSTRUCTIONS TO PROPOSERS: DELETE THIS BOX ONCE YOU HAVE COMPLETED THE FORM

This Beneficial Ownership Disclosure Form ("Form") is to be completed by the successful Proposer. In case of joint venture, the Proposer must submit a separate Form for each member. The beneficial ownership information to be submitted in this Form shall be current as of the date of its submission.

For the purposes of this Form, a Beneficial Owner of a Proposer is any natural person who ultimately owns or controls the Proposer by meeting one or more of the following conditions:

directly or indirectly holding 25% or more of the shares
directly or indirectly holding 25% or more of the voting rights
directly or indirectly having the right to appoint a majority of the board of directors or equivalent governing body of the Proposer

RFP No.: *[insert number of RFP process]*
Request for Proposals No.: *[insert **identification**]*

To: **[***insert **complete name of Purchaser***]**

In response to your request in the Letter of Acceptance *dated [insert date of letter of Acceptance]* to furnish additional information on beneficial ownership: *[select one option as applicable and delete the options that are not applicable]*

(i) we hereby provide the following beneficial ownership information.

Details of beneficial ownership

Identity of Beneficial Owner	Directly or indirectly holding 25% or more of the shares (Yes / No)	Directly or indirectly holding 25 % or more of the Voting Rights (Yes / No)	Directly or indirectly having the right to appoint a majority of the board of the directors or an equivalent governing body of the Proposer (Yes / No)
[include full name (last, middle, first), nationality, country of residence]			

OR

(ii) *We declare that there is no Beneficial Owner meeting one or more of the following conditions:*

- directly or indirectly holding 25% or more of the shares
- directly or indirectly holding 25% or more of the voting rights
- directly or indirectly having the right to appoint a majority of the board of directors or equivalent governing body of the Proposer

OR

(iii) We declare that we are unable to identify any Beneficial Owner meeting one or more of the following conditions. [If this option is selected, the Proposer shall provide explanation on why it is unable to identify any Beneficial Owner]

- directly or indirectly holding 25% or more of the shares
- directly or indirectly holding 25% or more of the voting rights
- directly or indirectly having the right to appoint a majority of the board of directors or equivalent governing body of the Proposer]"

Name of the Proposer: *[*insert* ***complete name of the Proposer***]

Name of the person duly authorized to sign the Proposal on behalf of the Proposer: ***[insert* ***complete name of person duly authorized to sign the Proposal****]*

Title of the person signing the Proposal: [*insert* ***complete title of the person signing the Proposal***]

Signature of the person named above: _____

Date signed *[insert* ***ordinal number****]* day of *[insert* ***month****], [insert* ***year****]*

[*] In the case of the Proposal submitted by a Joint Venture specify the name of the Joint Venture as Proposer. In the event that the Proposer is a joint venture, each reference to "Proposer" in the Beneficial Ownership Disclosure Form (including this Introduction thereto) shall be read to refer to the joint venture member.

[**] Person signing the Proposal shall have the power of attorney given by the Proposer. The power of attorney shall be attached with the Proposal Schedules.

LETTER OF ACCEPTANCE

Purchaser: *[insert **the name of the Purchaser**]*

Project: *[insert **name of project**]*

Contract title: *[insert the **name of the contract**]*

Country: *[insert **country where RFP is issued**]*

Loan No. /Credit No. / Grant No.: *[insert **reference number for loan/credit/grant**]*

RFP No: *[insert RFP **reference number from Procurement Plan**]*

Date: *[insert **Date**]*

To: *[insert **Name of Proposer**]*

This is to notify you that your Proposal dated *[insert **Date**]* for execution of the *[insert **brief description of the Information System**]* for the Contract Price in the aggregate of *[insert **amount in figures**]* (*[insert **amount in words**]*), as corrected and modified in accordance with the Instructions to Proposers is hereby accepted by our Agency.

You are requested to furnish (i) the Performance Security within 28 days in accordance with the Conditions of Contract, using for that purpose one of the Performance Security Forms and (ii) the additional information on beneficial ownership in accordance with ITP 47.1 within eight (8) Business days using the Beneficial Ownership Disclosure Form, included in Section X, - Contract Forms, of the request for proposals document.

Authorized Signature: _____

Name and Title of Signatory: *[insert **Name and Title**]*

Name of Agency: *[insert **Purchaser Name**]*

Attachment: Contract Agreement

1. CONTRACT AGREEMENT

THIS CONTRACT AGREEMENT is made

the *[insert: **ordinal number**]* day of *[insert: **month**], [insert: **year].***

BETWEEN

(1) *[insert: **Name of Purchaser**],* a *[insert: **description of type of legal entity**, for example, an agency of the Ministry of . . . **]*** of the Government of *[insert: **country of Purchaser**],* or corporation incorporated under the laws of *[insert: **country of Purchaser**]* and having its principal place of business at *[insert**: address of Purchaser**]* (hereinafter called "the Purchaser"), and

(2) *[insert: **name of Supplier**],* a corporation incorporated under the laws of *[insert: **country of Supplier**]* and having its principal place of business at *[insert: **address of Supplier**]* (hereinafter called "the Supplier").

WHEREAS the Purchaser desires to engage the Supplier to supply, install, achieve Operational Acceptance of, and support the following Information System *[insert: **brief description of the Information System**]* ("the System"), and the Supplier has agreed to such engagement upon and subject to the terms and conditions appearing below in this Contract Agreement.

NOW IT IS HEREBY AGREED as follows:

Article 1. Contract Documents

1.1 Contract Documents (Reference GCC Clause 1.1 (a) (ii))

The following documents shall constitute the Contract between the Purchaser and the Supplier, and each shall be read and construed as an integral part of the Contract:

(a) This Contract Agreement and the Appendices attached to the Contract Agreement

(b) Special Conditions of Contract

(c) General Conditions of Contract

(d) Technical Requirements (including Implementation Schedule)

(e) The Supplier's proposal and original Price Schedules

(f) Code of Conduct for Supplier's Personnel

(g) *[Add here: **any other documents**]*

1.2 Order of Precedence (Reference GCC Clause 2)

In the event of any ambiguity or conflict between the Contract Documents listed above, the order of precedence shall be the

order in which the Contract Documents are listed in Article 1.1 (Contract Documents) above, provided that Appendix 7 shall prevail over all provisions of the Contract Agreement and the other Appendices attached to the Contract Agreement and all the other Contract Documents listed in Article 1.1 above.

1.3 Definitions (Reference GCC Clause 1)

Capitalized words and phrases used in this Contract Agreement shall have the same meanings as are ascribed to them in the General Conditions of Contract.

Article 2.

Contract Price and Terms of Payment

2.1 Contract Price (Reference GCC Clause 1.1(a)(viii) and GCC Clause 11)

The Purchaser hereby agrees to pay to the Supplier the Contract Price in consideration of the performance by the Supplier of its obligations under the Contract. The Contract Price shall be the aggregate of: *[insert:* ***amount of foreign currency A in words*** *],* *[insert:* ***amount in figures*** *],* plus *[insert:* ***amount of foreign currency B in words*** *], [insert:* ***amount in figures],*** plus *[insert:* ***amount of foreign currency C in words*** *], [insert****: amount in figures*** *], [insert:* ***amount of local currency in words*** *], [insert:* ***amount in figures],*** as specified in the Grand Summary Price Schedule.

The Contract Price shall be understood to reflect the terms and conditions used in the specification of prices in the detailed price schedules, including the terms and conditions of the associated Incoterms, and the taxes, duties and related levies if and as identified.

Article 3.

Effective Date for Determining Time for Operational Acceptance

3.1 Effective Date (Reference GCC Clause 1.1 (e) (ix))

The time allowed for supply, installation, and achieving Operational Acceptance of the System shall be determined from the date when all of the following conditions have been fulfilled:

(a) This Contract Agreement has been duly executed for and on behalf of the Purchaser and the Supplier;

(b) The Supplier has submitted to the Purchaser the performance security and the advance payment security, in accordance with GCC Clause 13.2 and GCC Clause 13.3;

(c) The Purchaser has paid the Supplier the advance payment, in accordance with GCC Clause 12;

Each party shall use its best efforts to fulfill the above conditions for which it is responsible as soon as practicable.

3.2 If the conditions listed under 3.1 are not fulfilled within two (2) months from the date of this Contract Agreement because of reasons not attributable to the Supplier, the parties shall discuss and agree on an equitable adjustment to the Contract Price and the

Time for Achieving Operational Acceptance and/or other relevant conditions of the Contract.

Article 4. Appendixes

4.1 The Appendixes listed below shall be deemed to form an integral part of this Contract Agreement.

4.2 Reference in the Contract to any Appendix shall mean the Appendixes listed below and attached to this Contract Agreement, and the Contract shall be read and construed accordingly.

APPENDIXES

Appendix 1. Supplier's Representative
Appendix 2. Adjudicator *[if there is no Adjudicator, state **"not applicable"**]*
Appendix 3. List of Approved Subcontractors
Appendix 4. Categories of Software
Appendix 5. Custom Materials
Appendix 6. Revised Price Schedules (if any)
Appendix 7. Minutes of Contract Finalization Discussions and Agreed-to Contract Amendments

IN WITNESS WHEREOF the Purchaser and the Supplier have caused this Agreement to be duly executed by their duly authorized representatives the day and year first above written.

For and on behalf of the Purchaser

Signed:

in the capacity of *[insert: **title or other appropriate designation**]*

in the presence of

For and on behalf of the Supplier

Signed:

in the capacity of *[insert: **title or other appropriate designation**]*

in the presence of

CONTRACT AGREEMENT

dated the *[insert: **number**]* day of *[insert: **month**]*, *[insert: **year**]*

BETWEEN

[insert: ***name of Purchaser*** *],* "the Purchaser"

and

[insert: ***name of Supplier*** *],* "the Supplier"

Appendix 1. Supplier's Representative

In accordance with GCC Clause 1.1 (b) (iv), the Supplier's Representative is:

Name: *[insert:* ***name and provide title and address further below,*** *or state* ***"to be nominated within fourteen (14) days of the Effective Date"*** *]*

Title: *[if appropriate, insert:* ***title*** *]*

In accordance with GCC Clause 4.3, the Supplier's addresses for notices under the Contract are:

Address of the Supplier's Representative: *[as appropriate, insert:* ***personal delivery, postal, cable, facsimile, electronic mail, and/or EDI addresses.*** *]*

Fallback address of the Supplier: *[as appropriate, insert:* ***personal delivery, postal, cable, facsimile, electronic mail, and/or EDI addresses.*** *]*

Appendix 2. Adjudicator

In accordance with GCC Clause 1.1 (b) (vi), the agreed-upon Adjudicator is:

Name: *[insert:* ***name*** *]*
Title: *[insert:* ***title*** *]*
Address: *[insert:* ***postal address*** *]*
Telephone: *[insert:* ***telephone*** *]*

In accordance with GCC Clause 43.1.3, the agreed-upon fees and reimbursable expenses are:

Hourly Fees: *[insert:* ***hourly fees*** *]*
Reimbursable Expenses: *[list:* ***reimbursables*** *]*

Pursuant to GCC Clause 43.1.4, if at the time of Contract signing, agreement has not been reached between the Purchaser and the Supplier, an Adjudicator will be appointed by the Appointing Authority named in the SCC.

Appendix 3. List of Approved Subcontractors

The Purchaser has approved use of the following Subcontractors nominated by the Supplier for carrying out the item or component of the System indicated. Where more than one Subcontractor is listed, the Supplier is free to choose between them, but it must notify the Purchaser of its choice sufficiently in advance of the time when the subcontracted work needs to commence to give the Purchaser reasonable time for review. In accordance with GCC Clause 20.1, the Supplier is free to submit proposals for Subcontractors for additional items from time to time. No subcontracts shall be placed with any such Subcontractors for additional items until the Subcontractors have been approved in writing by the Purchaser and their names have been added to this list of Approved Subcontractors, subject to GCC Clause 20.3.

[specify: ***item, approved Subcontractors, and their place of registration that the Supplier proposed in the corresponding attachment to its proposal and that the Purchaser approves that the Supplier engage during the performance of the Contract. Add additional pages as necessary.*** *]*

Item	Approved Subcontractors	Place of Registration

Appendix 4. Categories of Software

The following table assigns each item of Software supplied and installed under the Contract to one of the three categories: (i) System Software, (ii) General-Purpose Software, or (iii) Application Software; and to one of the two categories: (i) Standard Software or (ii) Custom Software and to one of the two categories: (i) Proprietary or (ii) Open Source.

	(select one per title)			(select one per title)		(select one per title)	
Title	System	General-Purpose	Application	Standard	Custom	Proprietary	Open Source
[insert Title]							
[insert Title]							
[insert Title]							
[insert Title]							
[insert Title]							
[insert Title]							

Appendix 5. Custom Materials

The follow table specifies the Custom Materials the Supplier will provide under the Contract.

Custom Materials
*[insert **Title and description**]*
*[insert **Title and description**]*
*[insert **Title and description**]*
*[insert **Title and description**]*
*[insert **Title and description**]*

Appendix 6. Revised Price Schedules

The attached Revised Price Schedules (if any) shall form part of this Contract Agreement and, where differences exist, shall supersede the Price Schedules contained in the Supplier's Proposal. These Revised Price Schedules reflect any corrections or adjustments to the Supplier's proposal price, pursuant to the ITP Clauses 30.3 and 38.2.

Appendix 7. Minutes of Contract Finalization Discussions and Agreed-to Contract Amendments

The attached Contract amendments (if any) shall form part of this Contract Agreement and, where differences exist, shall supersede the relevant clauses in the GCC, SCC, Technical Requirements, or other parts of this Contract as defined in GCC Clause 1.1 (a) (ii).

2. PERFORMANCE AND ADVANCE PAYMENT SECURITY FORMS

2.1 Performance Security Form (Bank Guarantee)

(Bank Guarantee)

[The bank, as requested by the successful Proposer, shall fill in this form in accordance with the instructions indicated]

[Guarantor letterhead or SWIFT identifier code]

*[insert: **Bank's Name, and Address of Issuing Branch or Office**]*

Beneficiary: *[insert: **Name and Address of Purchaser**]*

Date: *[insert: **date**]*

PERFORMANCE GUARANTEE No.: *[insert: **Performance Guarantee Number**]*

Guarantor: *[Insert name and address of place of issue, unless indicated in the letterhead]*

We have been informed that on *[insert: **date of award**]* you awarded Contract No. *[insert: **Contract number**]* for *[insert: **title and/or brief description of the Contract**]* (hereinafter called "the Contract") to *[insert: **complete name of Supplier which in the case of a joint venture shall be in the name of the joint venture**]* (hereinafter called "the Applicant"). Furthermore, we understand that, according to the conditions of the Contract, a performance guarantee is required.

At the request of the Applicant, we as Guarantor hereby irrevocably undertake to pay you any sum(s) not exceeding *[insert: **amount(s)**[12] **in figures and words**]* such sum being payable in the types and proportions of currencies which the Contract Price is payable upon receipt by us of the Beneficiary's statement, whether in the demand itself or in a separate signed document accompanying or identifying the demand, stating that the Applicant is in breach of its obligation(s) under the contract without the Beneficiary needing to prove or to show grounds or reasons for their demand or the sum specified therein.

On the date of your issuing, to the Supplier, the Operational Acceptance Certificate for the System, the value of this guarantee will be reduced to any sum(s) not exceeding *[insert: **amount(s)**[1] **in figures and words**]*. This remaining guarantee shall expire no later than *[insert: **number** and select: **of months/of years** (of the Warranty Period that needs to be covered by the remaining guarantee)]* from the date of the Operational Acceptance Certificate for the System,[13] and any demand for payment under it must be received by us at this office on or before that date.

---

[12] *The bank shall insert the amount(s) specified and denominated in the SCC for GCC Clauses 13.3.1 and 13.3.4 respectively, either in the currency(ies) of the Contract or a freely convertible currency acceptable to the Purchaser.*

[13] *In this sample form, the formulation of this paragraph reflects the usual SCC provisions for GCC Clause 13.3. However, if the SCC for GCC Clauses 13.3.1 and 13.3.4 varies from the usual provisions, the paragraph, and possibly the previous paragraph, need to be adjusted to precisely reflect the provisions specified in the SCC.*

This guarantee is subject to the Uniform Rules for Demand Guarantees, (URDG) 2010 Revision, ICC Publication No. 758, except that the supporting statement under 15 (a) is hereby excluded.

_____

[Signature(s)]

*[**Note**: All italicized text (including footnotes) is for use in preparing this form and shall be deleted from the final product.]*

2.2 Advance Payment Security Bank Guarantee

[Guarantor letterhead or SWIFT identifier code]

Beneficiary: *[insert: **Name and Address of Purchaser**]*

Date: ***[insert date of issue]***

ADVANCE PAYMENT GUARANTEE No.: *[insert: **Advance Payment Guarantee Number**]*

Guarantor: *[Insert name and address of place of issue, unless indicated in the letterhead]*

We have been informed that on *[insert: **date of award**]* you awarded Contract No. *[insert: **Contract number**]* for *[insert: **title and/or brief description of the Contract**]* (hereinafter called "the Contract") to *[insert: **complete name of Supplier, which in the case of a joint venture shall be the name of the joint venture**]* (hereinafter called "the Applicant").

Furthermore, we understand that, according to the conditions of the Contract, an advance payment in the sum of *[insert: **amount in numbers and words, for each currency of the advance payment**]* is to be made to the Supplier against an advance payment guarantee.

At the request of the Applicant, we as Guarantor, hereby irrevocably undertake to pay the Beneficiary any sum or sums not exceeding in total an amount of *[insert **amount in figures**] ([insert **amount in words**])*[14] upon receipt by us of the Beneficiary's complying demand supported by the Beneficiary's statement, whether in the demand itself or in a separate signed document accompanying or identifying the demand, stating either that the Applicant:

(a) has used the advance payment for purposes other than toward delivery of Goods; or

(b) has failed to repay the advance payment in accordance with the Contract conditions, specifying the amount which the Applicant has failed to repay.

A demand under this guarantee may be presented as from the presentation to the Guarantor of a certificate from the Beneficiary's bank stating that the advance payment referred to above has been credited to the Applicant on its account number *[insert **number**]* at *[insert **name and address of Applicant's bank**]*.

The maximum amount of this guarantee shall be progressively reduced by the amount of the advance payment repaid by the Applicant as specified in copies of interim statements or payment certificates which shall be presented to us. This guarantee shall expire, at the latest,

[14] *The Guarantor shall insert an amount representing the amount of the advance payment and denominated either in the currency(ies) of the advance payment as specified in the Contract, or in a freely convertible currency acceptable to the Purchaser.*

upon our receipt of a copy of the interim payment certificate indicating that ninety (90) percent of the Accepted Contract Amount, has been certified for payment, or on the *[insert **day**]* day of *[insert **month**]*, *[insert **year**]*, whichever is earlier. Consequently, any demand for payment under this guarantee must be received by us at this office on or before that date.

This guarantee is subject to the Uniform Rules for Demand Guarantees (URDG) 2010 Revision, ICC Publication No.758, except that the supporting statement under Article 15(a) is hereby excluded.

_____

[signature(s)]

*[**Note**: All italicized text (including footnotes) is for use in preparing this form and shall be deleted from the final product.]*

3. INSTALLATION AND ACCEPTANCE CERTIFICATES

3.1 Installation Certificate

Date: *[insert:* ***date*** *]*

Loan/Credit Number: *[insert:* ***loan or credit number from RFP*** *]*

RFP: *[insert:* ***title and number of RFP*** *]*

Contract: *[insert:* ***name and number of Contract*** *]*

To: *[insert:* ***name and address of Supplier*** *]*

Dear Sir or Madam:

Pursuant to GCC Clause 26 (Installation of the System) of the Contract entered into between yourselves and the *[insert:* ***name of Purchaser*** *]* (hereinafter the "Purchaser") dated *[insert:* ***date of Contract],*** relating to the *[insert:* ***brief description of the Information System],*** we hereby notify you that the System (or a Subsystem or major component thereof) was deemed to have been correctly installed on the date specified below.

1. Description of the System (or relevant Subsystem or major component: *[insert:* ***description*** *]*
2. Date of Installation: *[insert:* ***date*** *]*

   Notwithstanding the above, you are required to complete the outstanding items listed in the attachment to this certificate as soon as practicable. This letter shall not relieve you of your obligation to achieve Operational Acceptance of the System in accordance with the Contract nor of your obligations during the Warranty Period.

For and on behalf of the Purchaser

Signed:

Date:

in the capacity of: *[state:* ***"Project Manager"*** *or specify a higher level authority in the Purchaser's organization]*

3.2 Operational Acceptance Certificate

Date: *[insert: **date**]*

Loan/Credit Number: *[insert: **loan or credit number from RFP**]*

RFP: *[insert: **title and number of RFP**]*

Contract: *[insert: **name of System or Subsystem and number of Contract**]*

To: *[insert: **name and address of Supplier**]*

Dear Sir or Madam:

Pursuant to GCC Clause 27 (Commissioning and Operational Acceptance) of the Contract entered into between yourselves and the *[insert: **name of Purchaser**]* (hereinafter the "Purchaser") dated *[insert: **date of Contract**]*, relating to the ***[insert: brief description of the Information System**]*, we hereby notify you the System (or the Subsystem or major component identified below) successfully completed the Operational Acceptance Tests specified in the Contract. In accordance with the terms of the Contract, the Purchaser hereby takes over the System (or the Subsystem or major component identified below), together with the responsibility for care and custody and the risk of loss thereof on the date mentioned below.

1. Description of the System (or Subsystem or major component): *[insert: **description**]*
2. Date of Operational Acceptance: *[insert: **date**]*

This letter shall not relieve you of your remaining performance obligations under the Contract nor of your obligations during the Warranty Period.

For and on behalf of the Purchaser

Signed:_____

Date: *[insert: **date**]*

in the capacity of: *[state: **"Project Manager"** or specify a higher level authority in the Purchaser's organization]*

4. CHANGE ORDER PROCEDURES AND FORMS

Date: *[insert:* ***date*** *]*

Loan/Credit Number: *[insert:* ***loan or credit number from RFP*** *]*

RFP: *[insert:* ***title and number of RFP*** *]*

Contract: *[insert:* ***name or System or Subsystem and number of Contract*** *]*

General

This section provides samples of procedures and forms for carrying out changes to the System during the performance of the Contract in accordance with GCC Clause 39 (Changes to the System) of the Contract.

Change Order Log

The Supplier shall keep an up-to-date Change Order Log to show the current status of Requests for Change and Change Orders authorized or pending. Changes shall be entered regularly in the Change Order Log to ensure that the log is kept up-to-date. The Supplier shall attach a copy of the current Change Order Log in the monthly progress report to be submitted to the Purchaser.

References to Changes

(1) Request for Change Proposals (including Application for Change Proposals) shall be serially numbered CR-nnn.
(2) Change Estimate Proposals shall be numbered CN-nnn.
(3) Estimate Acceptances shall be numbered CA-nnn.
(4) Change Proposals shall be numbered CP-nnn.
(5) Change Orders shall be numbered CO-nnn.

On all forms, the numbering shall be determined by the original CR-nnn.

Annexes

4.1 Request for Change Proposal Form
4.2 Change Estimate Proposal Form
4.3 Estimate Acceptance Form
4.4 Change Proposal Form
4.5 Change Order Form
4.6 Application for Change Proposal Form

4.1 Request for Change Proposal Form

(Purchaser's Letterhead)

Date: *[insert:* ***date*** *]*

Loan/Credit Number: *[insert:* ***loan or credit number from RFP*** *]*

RFP: *[insert:* ***title and number of RFP*** *]*

Contract: *[insert:* ***name of System or Subsystem or number of Contract*** *]*

To: *[insert:* ***name of Supplier and address*** *]*

Attention: *[insert:* ***name and title*** *]*

Dear Sir or Madam:

With reference to the above-referenced Contract, you are requested to prepare and submit a Change Proposal for the Change noted below in accordance with the following instructions within *[insert:* ***number*** *]* days of the date of this letter.

1. Title of Change: *[insert:* ***title*** *]*
2. Request for Change No./Rev.: *[insert:* ***number*** *]*
3. Originator of Change: *[select* ***Purchaser / Supplier (by Application for Change Proposal)****, and add****: name of originator*** *]*
4. Brief Description of Change: *[insert:* ***description*** *]*
5. System (or Subsystem or major component affected by requested Change): *[insert:* ***description]***
6. Technical documents and/or drawings for the request of Change:

   Document or Drawing No. Description
7. Detailed conditions or special requirements of the requested Change: *[insert:* ***description*** *]*
8. Procedures to be followed:
   (a) Your Change Proposal will have to show what effect the requested Change will have on the Contract Price.
   (b) Your Change Proposal shall explain the time it will take to complete the requested Change and the impact, if any, it will have on the date when Operational Acceptance of the entire System agreed in the Contract.
   (c) If you believe implementation of the requested Change will have a negative impact on the quality, operability, or integrity of the System, please provide a detailed

explanation, including other approaches that might achieve the same impact as the requested Change.

(d) You should also indicate what impact the Change will have on the number and mix of staff needed by the Supplier to perform the Contract.

(e) You shall not proceed with the execution of work related to the requested Change until we have accepted and confirmed the impact it will have on the Contract Price and the Implementation Schedule in writing.

9. As next step, please respond using the Change Estimate Proposal form, indicating how much it will cost you to prepare a concrete Change Proposal that will describe the proposed approach for implementing the Change, all its elements, and will also address the points in paragraph 8 above pursuant to GCC Clause 39.2.1. Your Change Estimate Proposal should contain a first approximation of the proposed approach, and implications for schedule and cost, of the Change.

For and on behalf of the Purchaser

Signed:

Date:

in the capacity of: *[state: **"Project Manager"** or specify a higher level authority in the Purchaser's organization]*

4.2 Change Estimate Proposal Form

(Supplier's Letterhead)

Date: *[insert: **date**]*

Loan/Credit Number: *[insert: **loan or credit number from RFP**]*

RFP: *[insert: **title and number of RFP**]*

Contract: *[insert: **name of System or Subsystem and number of Contract**]*

To: *[insert: **name of Purchaser and address**]*

Attention: *[insert: **name and title]***

Dear Sir or Madam:

With reference to your Request for Change Proposal, we are pleased to notify you of the approximate cost of preparing the below-referenced Change in accordance with GCC Clause 39.2.1 of the Contract. We acknowledge that your agreement to the cost of preparing the Change Proposal, in accordance with GCC Clause 39.2.2, is required before we proceed to prepare the actual Change Proposal including a detailed estimate of the cost of implementing the Change itself.

1. Title of Change: *[insert: **title**]*
2. Request for Change No./Rev.: *[insert: **number**]*
3. Brief Description of Change (including proposed implementation approach): *[insert: **description**]*
4. Schedule Impact of Change (initial estimate): *[insert: **description**]*
5. Initial Cost Estimate for Implementing the Change: *[insert: **initial cost estimate**]*
6. Cost for Preparation of Change Proposal: *[insert: **cost in the currencies of the Contract],** as detailed below in the breakdown of prices, rates, and quantities.

For and on behalf of the Supplier

Signed:

Date:

in the capacity of: *[state: **"Supplier's Representative"** or specify a other higher level authority in the Supplier's organization]*

4.3 Estimate Acceptance Form

(Purchaser's Letterhead)

Date: *[insert: **date**]*

Loan/Credit Number: *[insert: **loan or credit number from RFP**]*

RFP: *[insert: **title and number of RFP**]*

Contract: *[insert: **name of System or Subsystem and number of Contract**]*

To: *[insert: **name of Supplier and address**]*

Attention: *[insert: **name and title**]*

Dear Sir or Madam:

We hereby accept your Change Estimate and agree that you should proceed with the preparation of a formal Change Proposal.

1. Title of Change: *[insert: **title**]*
2. Request for Change No./Rev.: *[insert: **request number / revision**]*
3. Change Estimate Proposal No./Rev.: *[insert: **proposal number / revision**]*
4. Estimate Acceptance No./Rev.: *[insert: **estimate number / revision**]*
5. Brief Description of Change: *[insert: **description**]*
6. Other Terms and Conditions: *[insert: **other terms and conditions**]*

   In the event that we decide not to order the Change referenced above, you shall be entitled to compensation for the cost of preparing the Change Proposal up to the amount estimated for this purpose in the Change Estimate Proposal, in accordance with GCC Clause 39 of the General Conditions of Contract.

For and on behalf of the Purchaser

Signed:

Date:

in the capacity of: *[state: **"Project Manager"** or specify a higher level authority in the Purchaser's organization]*

4.4 Change Proposal Form

(Supplier's Letterhead)

Date: *[insert: **date**]*

Loan/Credit Number: *[insert: **loan or credit number from RFP**]*

RFP: *[insert: **title and number of RFP**]*

Contract: *[insert: **name of System or Subsystem and number of Contract**]*

To: *[insert: **name of Purchaser and address**]*

Attention: *[insert: **name and title**]*

Dear Sir or Madam:

In response to your Request for Change Proposal No. *[insert: **number],*** we hereby submit our proposal as follows:

1. Title of Change: *[insert: **name**]*
2. Change Proposal No./Rev.: *[insert: **proposal number/revision**]*
3. Originator of Change: *[select: **Purchaser / Supplier;** and add: **name**]*
4. Brief Description of Change: *[insert: **description**]*
5. Reasons for Change: *[insert: **reason**]*
6. The System Subsystem, major component, or equipment that will be affected by the requested Change: *[insert: **description**]*
7. Technical documents and/or drawings for the requested Change:

   Document or Drawing No. Description
8. Estimate of the increase/decrease to the Contract Price resulting from the proposed Change: *[insert: **amount in currencies of Contract],*** as detailed below in the breakdown of prices, rates, and quantities.

   Total lump sum cost of the Change:

   Cost to prepare this Change Proposal (i.e., the amount payable if the Change is not accepted, limited as provided by GCC Clause 39.2.6):
9. Additional Time for Achieving Operational Acceptance required due to the Change: *[insert: **amount in days / weeks**]*
10. Effect on the Functional Guarantees: *[insert: **description**]*
11. Effect on the other terms and conditions of the Contract: *[insert: **description**]*

12. Validity of this Proposal: for a period of *[insert: **number**]* days after receipt of this Proposal by the Purchaser

13. Procedures to be followed:

    (a) You are requested to notify us of your acceptance, comments, or rejection of this detailed Change Proposal within *[insert: **number**]* days from your receipt of this Proposal.

    (b) The amount of any increase and/or decrease shall be taken into account in the adjustment of the Contract Price.

For and on behalf of the Supplier

Signed:

Date:

in the capacity of: *[state: **"Supplier's Representative"** or specify a other higher level authority in the Supplier's organization **]***

4.5 Change Order Form

(Purchaser's Letterhead)

Date: *[insert: **date**]*

Loan/Credit Number: *[insert: **loan or credit number from RFP**]*

RFP: *[insert: **title and number of RFP**]*

Contract: *[insert: **name of System or Subsystem and number of Contract**]*

To: *[insert: **name of Supplier and address**]*

Attention: *[insert: **name and title**]*

Dear Sir or Madam:

We hereby approve the Change Order for the work specified in Change Proposal No. *[insert: **number**]*, and agree to adjust the Contract Price, Time for Completion, and/or other conditions of the Contract in accordance with GCC Clause 39 of the Contract.

1. Title of Change: *[insert: **name**]*
2. Request for Change No./Rev.: *[insert: **request number / revision**]*
3. Change Order No./Rev.: *[insert: **order number / revision**]*
4. Originator of Change: *[select: **Purchaser / Supplier;** and add: **name**]*
5. Authorized Price for the Change:

   Ref. No.: *[insert: **number**]* Date: *[insert: **date**]*

   *[insert: **amount in foreign currency A**]* plus *[insert: **amount in foreign currency B**]* plus *[insert: **amount in foreign currency C]** plus *[insert: **amount in local currency]***
6. Adjustment of Time for Achieving Operational Acceptance: *[insert: **amount and description of adjustment**]*
7. Other effects, if any: *[state: **"none" or insert description**]*

For and on behalf of the Purchaser

Signed: _____

Date*: [insert **date**]*

in the capacity of: *[state: **"Project Manager"** or higher level authority in the Purchaser's organization]*

For and on behalf of the Supplier

Signed:_____

Date: *[insert **date**]*

in the capacity of: *[state **"Supplier's Representative"** or specify a higher level authority in the Supplier's organization]*

4.6 Application for Change Proposal Form

(Supplier's Letterhead)

Date: *[insert: **date**]*

Loan/Credit Number: *[insert: **loan or credit number from RFP**]*

RFP: *[insert: **title and number of RFP**]*

Contract: *[insert: **name of System or Subsystem and number of Contrac**t]*

To: *[insert: **name of Purchaser and address**]*

Attention**:** *[insert: **name and title**]*

Dear Sir or Madam:

We hereby propose that the below-mentioned work be treated as a Change to the System.

1. Title of Change: *[insert: **name**]*
2. Application for Change Proposal No./Rev.: *[insert: **number / revision**]* dated: *[insert: **date**]*
3. Brief Description of Change: *[insert: **description**]*
4. Reasons for Change: *[insert: **description**]*
5. Order of Magnitude Estimation: *[insert: **amount in currencies of the Contract**]*
6. Schedule Impact of Change: *[insert: **description**]*
7. Effect on Functional Guarantees, if any: *[insert: **description**]*
8. Appendix: *[insert: **titles (if any);** otherwise state **"none"**]*

For and on behalf of the Supplier

Signed:

Date:

in the capacity of: *[state: **"Supplier's Representative"** or specify a higher level authority in the Supplier's organization]*