BID SPECIFICATION

STATE INFORMATION TECHNOLOGY AGENCY (SOC) LTD
Registration number 1999/001899/30

RFB REF. NO:	**RFB 2674-2022**
DESCRIPTION	**PROCUREMENT OF SOLUTION DESIGN, MIGRATION AND SOFTWARE DEVELOPMENT SERVICES FOR FIREARMS CONTROL SOLUTION FOR THE SOUTH AFRICAN POLICE SERVICE FOR A PERIOD OF THREE (3) YEARS.**
PUBLICATION DATE	**11 OCTOBER 2022**
BRIEFING SESSION	**COMPULSORY BRIEFING SESSION:** **DATE: 18 OCTOBER 2022** **TIME: 10:00 AM – 11:30 AM** **Virtual Briefing Session:** Click here to join the meeting
CLOSING DATE FOR QUESTIONS AND ANSWERS	**21 OCTOBER 2022**
RFB CLOSING DETAILS	**DATE: 02 NOVEMBER 2022** **TIME: 11:00 AM (SOUTH AFRICAN TIME)** **PLACE: TENDER OFFICE, PONGOLA IN APOLLO, 459 TSITSA STREET, ERASMUSKLOOF, PRETORIA (HEAD OFFICE)**
PUBLIC OPENING OF RFB RESPONSES	**02 NOVEMBER 2022**
RFB VALIDITY PERIOD	**120 DAYS FROM THE CLOSING DATE**

PROSPECTIVE BIDDERS MUST REGISTER ON NATIONAL TREASURY'S CENTRAL SUPPLIER DATABASE PRIOR TO SUBMITTING BIDS

Contents

ANNEX A: INTRODUCTION

1. PURPOSE AND BACKGROUND

1.1. PURPOSE

The purpose of this Request for Bid (RFB) is to invite Suppliers (hereinafter referred to as "Bidders") to submit bids to "supply, design, do migration, and development of services for the Firearms Control Solution for the South African Police Service (SAPS) in order to establish an FCS within a period of thirty-six (36) months.

The SAPS FCS solution proposed can either be fully bespoke, fully COTS or hybrid bespoke/COTS. Any COTS component ownership must be fully rendered to SITA with no further future license or ownership claim or dependency. Furthermore, the COTS ownership must include the rights to customise any aspect of the COTS component without any infringement in any regard. With the transfer of ownership to SITA, SITA must be permitted, without limitation, to alter the design and product artefacts as and when required. The software will be transferred in entirety with no restriction by any third-party ownership/license. The service provider relinquishes all rights of ownership to the delivered solution, including all related artefacts and components.

1.2. BACKGROUND

The Firearms Control Act 60 OF 2000 (FCA) was promulgated in 2004 to give effect to a comprehensive, structured and effective System for the control of firearms. The Act's intent, among others, is to prevent the proliferation of illegally possessed firearms, improve control over legally possessed firearms, and prevent crime involving the use of firearms, by contributing to the creation of a safe and secure environment for all people of South Africa.

The FCA, among others, regulate the application, issuing and approval of firearm licenses, permits and related applications, and specifies certain requirements that must be met by individuals, businesses and various institutions to legally possess and use firearms.

The development services are to specify the design, migration and development of the solution to effectively and efficiently administer all the firearm processes, based on the digitised vision of the SAPS.

The goal of the project is to develop a secure, digitised and reliable solution to ensure effective service delivery throughout the SAPS.

The Firearms Control Solution must provide the following:

(a) Verification and Identification of a person;

(b) Establishment of electronic applications via portal capability and diary management;

(c) Establishment of persons (juristic and natural), firearm registration and warrants, including non-repudiation and management capability as further detailed in this bid specification;

(d) Establishment of *all* the processes required to manage the firearms, firearm owners, Commercial Agents, Institutions and warrants efficiently and effectively;

(e) Establishment of the required integration functionality (e.g. electronic payments, person verification), management, processing and storage of all related processes;

(f) Establishment of an electronic verification and dashboard capability;

(g) Enhanced enquiry (dashboard) and reporting capability;

(h) Single view of a firearm, its relationships and history; and

(i) Single view of a person's (juristic and natural) status within the solution.

2. SCOPE OF BID

2.1. SCOPE OF WORK

The scope of work includes the design and development/implementation of a credible, secure and reliable solution to effectively and efficiently administer all the firearm processes based on the digitised vision of the SAPS.

The diagram below provides an overview of the four (4) primary objects and relationships within the Firearms Solution, i.e. Person (Individual or Juristic), Application, Warrant and related Firearm.

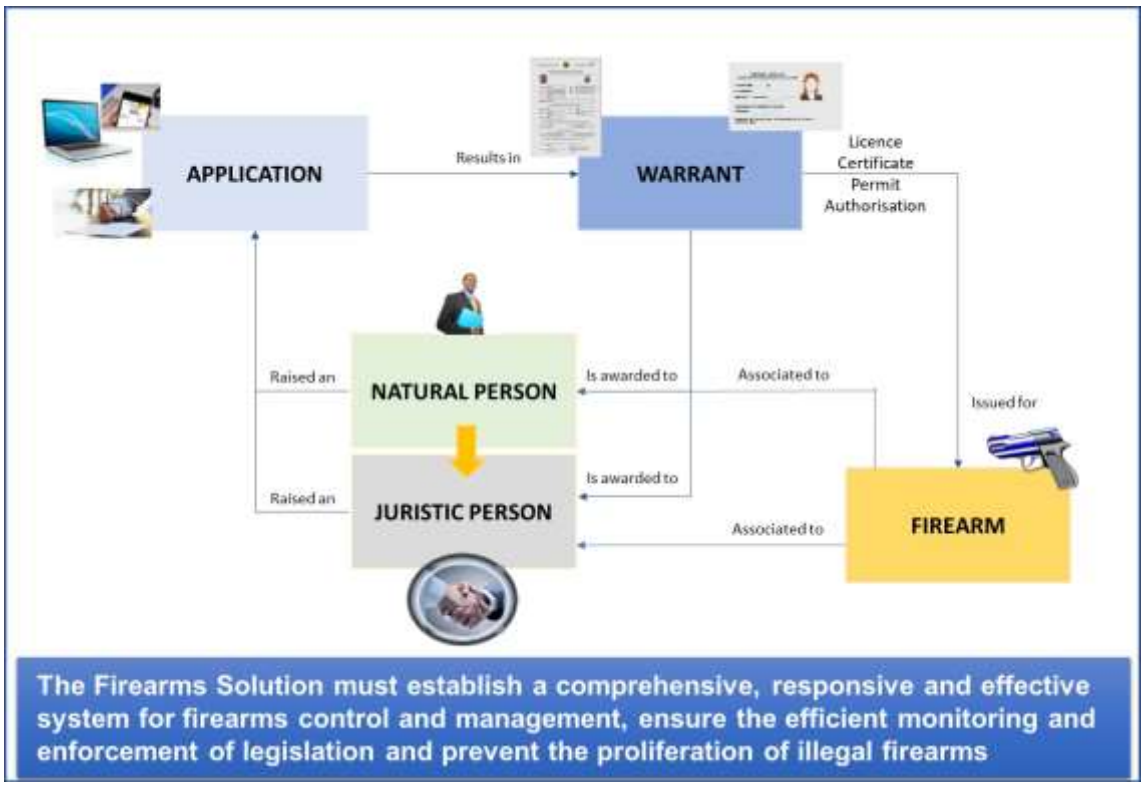

Figure 1: Four Primary Objects and Relationships in FCS

2.2. PROJECT PHASES

Table 1: Project Phases

No.	Phase	Description	Performed by
1.	Project initiation and planning Duration: Initiation	Confirm scope with client, confirm validity of previously compiled requirement/specification documents, review/acknowledge the current data to be migrated and perform detailed planning for the project. This Project Phase includes the following minimum requirements to establish information management, organisational structure as well as stakeholder roles and responsibilities required to establish control and assurance that the business expectations must be achieved: • Project initiation and planning • Project Financials (including Billing) • Project resources and stakeholder Management • Project Risks/Issue Management • Project Implementation Management • Project Time Management • Scope Management	Service Provider SITA SAPS

No.	Phase	Description	Performed by
		• Schedule Management • Quality Management • Project Change Control Management • Project and product Artefacts Control Minimum project products: • Project Charter • Project schedule • Implementation plan/approach • Project risk/issue register • Payment schedule aligned to accepted milestones The Project must comply with PMP and/or Prince2 or a recognised Agile methodology. The standard project management methodology may be tailored and must be agreed to by SITA prior to the project initiation. The Supplier must for the duration of the contract ensure compliance with General Quality Standards, ISO 9001. The Project Manager has more than 10 years' experience managing and executing similar types and size of projects.	
2.	Project Execution, Control and Monitoring Duration: Project duration	Project performance monitoring, risk management, financial control, steering committees, change control, project meetings, schedule management and project reporting. The following minimum activities are required: • Resources tasking and progress tracking • Ensure that the work is continually justified • Monitor and control performance • Ensure that information is accurate, current and accessible • Establish and maintain the management team • Identify and communicate with the stakeholders affected by the work • Ensure that the management of the work is relevant and effective • Ensure that the risks and issues are effectively managed • Ensure that the repositories reflect the current and relevant artefacts • Ensure that the released product conforms to the quality requirements • Ensure that the release management procedures are established and effectively managed Minimum project products: • Project meeting agenda and minutes • Project risk/issue register • Project performance reports • Product acceptance certificates required for payments	SITA/ Service Provider
3.	Definition of solution architecture Duration: For Release 1, 2, 3 and 4.	Detailing the acquisition of required services and products required for the development/delivery of the solution as a whole and for baseline in Release 1 and subsequent maintenance across the various releases. Minimum products to be delivered for this phase: • Solution Architecture document drafted for Release 1 and updated as required. The solution architecture and solution must comply with the Protection of Personal Information Act (POPIA); ISO27001 IT Security; and Business Continuity Management (BCM) ISO22301 compliant.	Service Provider

No.	Phase	Description	Performed by
4.	Definition of Security Architecture Duration: For Release 1, 2, 3 and 4.	Detailing the acquisition of required services and products required for the development/delivery of the security architecture for baseline in Release 1 and subsequent maintenance across the various releases. Minimum products to be delivered for this phase: • Security Architecture document drafted for Release 1 and updated as required.	Service Provider
5.	Definition of data architecture Duration: For Release 1,2,3 and 4.	This phase of the project will be delivered in the form of data architecture documents as baseline for the migration from the existing System the New FCS; and enhanced/refined per specified release. Minimum products to be delivered for this phase: • Data Architecture document drafted for Release 1 and updated as required. The Security Architecture is developed and implemented by a certified IT Security Architect with more than 10 years' experience. The security testing is done by a certified Ethical Hacker with more than 10 years' experience.	Service Provider
6.	Definition of Migration Duration: For Release 1,2,3 and 4.	This phase of the project will be delivered in the form of migration analyses and migration plans/schedules together with data architecture and functional services /components per specified release. Refer to par 2.5.2 and par 8.2(24)(d) for the existing EFRS data sources. The complete list of data sources, with data capacity, will be determined during the analysis and design phase. Minimum products to be delivered for this phase: • Data Migration Strategy drafted for Release 1 and updated as required. • Data Migration Plan drafted for each release.	Service Provider
7.	Definition of business architecture Duration: For Release 1,2,3 and 4.	This phase of the project will be delivered in the form of business architecture documents, as per business process models for baseline and per specified release. Verify the to-be business process models. Minimum products to be delivered for this phase: • Business Architecture document drafted for Release 1 and updated as required. • Verified to-be business process models.	Service Provider
8.	Definition of functional requirements Duration: For Release 1,2,3 and 4.	This phase of the project will be delivered in the form of Functional Design Specification (FDS) documents for baseline and per process per specified release. Minimum products to be delivered for this phase: • Functional Design Specification (FDS) document drafted for each release.	Service Provider
9.	Definition of technical requirements Duration: For Release 1,2,3 and 4.	This phase of the project will be delivered in the form of Technical Design Specification (TDS) documents for baseline and enhanced/refined per specified release. Specify the capacity requirements for the development, testing, production infrastructure on which the application will be develop/tested/deployed for production utilisation. Minimum products to be delivered for this phase: • Technical Design Specification (TDS) document drafted for each release.	Service Provider
10.	Definition of integration requirements Duration: For Release 1,2,3 and 4.	This phase of the project will be delivered in the form of Integration Control Documents (ICD) for baseline and enhanced/refined per specified release. Minimum products to be delivered for this phase: • Integration Control Document (ICD) for each integration between the new FCS and any other electronic interface/application/system.	Service Provider

No.	Phase	Description	Performed by
11.	Definition of integration design Duration: For Release 1,2,3 and 4.	This phase of the project will be delivered in the form of Integration Design Documents (IDD), per specified release. Minimum products to be delivered for this phase: • Integration Design Document (IDD) for each integration between the new FCS and any other electronic interface/application/system.	Service Provider
12.	Development and unit testing Duration: For Release 1,2,3 and 4.	This phase entails development and unit testing per specified release including prior releases, including all the integrations. This phase includes the development of test use cases that is required for the acceptance of the respective release. Minimum products to be delivered for this phase: • Test use cases that is required for the acceptance of each release. • Unit test results.	Service Provider
13.	Training Material and Help Guidelines Duration: For Release 1, 2, 3 and 4.	This phase entails development of Training Material and Help Guides for the complete Solution. Required for each release and UAT user training as well as for the subsequent user training. SAPS will be responsible for training the SAPS users. Minimum products to be delivered for this phase: • Training Material for each release. • Help Guidelines for each release. • Artificial Intelligence (AI) based Chatbot.	Service Provider
14.	Testing phases Duration: For Release 1, 2, 3 and 4.	This phase entails software integration, System integration and product acceptance testing per phase. Minimum products to be delivered for this phase: • Test plans for each release. • System Integration test results. • User acceptance test results. • User Acceptance Certificate. • Security testing Acceptance Certificate. • Security test report with the security findings. • IT Audit report with supporting audit findings. The security testing of the system and the IT Audit must be conducted by a respective Certified Expert.	SITA/SAPS/ Service Provider
15.	Deployment/ Implementation phases Duration: For Release 1, 2, 3 and 4.	During this phase the specified release of the solution will be deployed to the pre-production and/or production environments and access will be given to the system users based on their respective roles and responsibilities. Furthermore, this phase includes: • All data migration as identified during “definition of migration phase” per release. • Train the trainer. • Training to SITA IFASS and AM on the solution, prior to handover. • Release management activities relating to the deployment of accepted projects and related deliverables. Minimum products required for each release: • Successfully migrated data. • Data migration reconciliation. • Data migration certificate. • Production acceptance deployment certificate. • Source code of developed product and related artefacts. • If any, customised and/or standard COTS components and related artefacts. • Packaged components with the deployment instructions. • Trained trainers. • Release management deployment guide. • Release management release note. • Release management change authority board note.	SITA/ Service Provider

No.	Phase	Description	Performed by
16.	Post implementation phases Duration: For Release 1, 2, 3 and 4.	Post implementation support forms part of the project for a period of three (3) months after each release, in order to stabilise the solution before being deployed to production and accepted by the client. SITA release management must be included to govern the release(s) of the product to pre-production and production. During the **3 months of post-go-live support**, per release, the respective functional application support and application maintenance support must be onboarded to support and maintain the product. After this period the release must be maintained through a maintenance service. Minimum activities to be performed: • Hand over documents per release. • Hand over developed products to SITA AM and FASS. • Verify source code in the SITA source code repository. Minimum products to be delivered for this phase: • Functional support. • Technical support. • Knowledge/skills transfer to SITA Application Maintenance and Functional Application Support teams.	SITA/SAPS/ SITA CAB Service Provider
17.	Project closure Duration: End of project	During this phase the close out administration for the project should be conducted. Minimum activities to be performed: • Verify project and product repositories to ensure that the applicable standards are complied with and that all required artefacts are correctly classified and available. • Hand over project and products to SITA prior to project closure. • Remove all service provider access from the SITA and SAPS networks and systems. Minimum project products: • Project closure report. • Project artefacts stored in the SITA project repository. • Project change control related artefacts. • Project handover certificate issued to SITA.	SITA/SAPS/ Service Provider
18.	Maintenance and Support Duration: For Release 1, 2, 3 and 4.	A service level agreement separate, to this RFB/contract, will be entered into between SITA and SAPS.	SITA/SAPS
19.	Project Change Control Management Duration: Ad hoc	This phase depends on the applicable contract and responsibilities established during the project initiation phase and requirement to manage changes relating to the contract and project charter. This phase focuses on the change control relating to the changes that may impact on the project timeline, scope and/or cost.	SITA/SAPS/ Service Provider

2.2.1. QUALITY ASSURANCE

(a) Conduct Quality Stage Gates;
(b) Evaluating and monitoring the agreement and process by which the product is developed;
(c) Review existence and conformance quality of delivered project deliverables, including documentation;
(d) Management and monitoring improvement initiatives that are aligned with audit findings; and
(e) Evaluating the quality of the product and processes utilizing checklists.

2.3. PRODUCT DELIVERY APPROACH

(a) It is required that an Agile Project Management and Product Development approach be adopted to deliver the respective releases as documented in this specification.

(b) The Software Development Lifecycle (SDLC) defines the following activities which must be utilised in order to ensure that the product is delivered according to the selected project management and development approaches. In general, the SDLC covers the following activities:
  (i) Analysis;
  (ii) Design/Architecture;
  (iii) Development and unit testing;
  (iv) Testing and acceptance;
  (v) Quality Assurance
  (vi) Deployment;
  (vii) Post-go-live Maintenance and Support; and
  (viii) Hand over product for SITA Application Maintenance and Functional Application Support.

(c) The various products that must be delivered, during this project, to achieve the respective project phase, are defined in this specification.

(d) In the event that the Bidder proposes a fully COTS solution, or a hybrid COTS/Bespoke solution, the Bidder's implementation methodology must be followed to realise the functional requirements, within the time constraints and in compliance with the technology stack as specified herein. The implementation includes the configuration and any customisation required to deliver the SAPS FCS business objectives in full. The COTS solution must fully implement the stated functionalities.

2.4. DELIVERY ADDRESS

The services must be supplied or provided at the following physical address:

Table 2: Delivery Address

No	Physical Address
1	SITA Centurion Offices: 1 John Vorster Drive Centurion Pretoria

2.5. CUSTOMER INFRASTRUCTURE AND ENVIRONMENT

The below infrastructure environments and technology stacks describe the technical requirements to develop the respective products as described in the respective releases. The respective architectures must reflect the technology stacks, agreed to with SAPS, prior to the development of the releases. The service provider must conform to the agreed technologies as specified by SAPS.

(a) The client has two current technology stacks:
  (i) The first technology stack is Microsoft Based and includes:
    1) Microsoft. Net development environment
    2) Microsoft SQL database
    3) Microsoft Windows Server operating system
    4) Microsoft IIS application Server
  (ii) The second technology stack is Oracle based and includes:
    1) JEE framework development environment
    2) Oracle Database
    3) Oracle Solaris operating system
    4) Oracle WebLogic application server

(b) ECM related servers
  (i) Documentum ECMS
  (ii) SharePoint

(c) Integration Platforms
  (i) MQ
  (ii) IBM Integration Bus

(d) Biometrics
  (i) Sagem / Morpho device

Note: The successful service provider will be required to specify the capacity requirements for the respective targeted infrastructure that must be specified before the deployment phase for each release to enable proactive acquisition of the required infrastructure. The capacity requirements must not delay the deployment of the respective release.

2.5.1. SITA CLOUD HOSTING INFRASTRUCTURE AND ENVIRONMENT

The Bidders are required to be compliant with the above current SAPS technology stack and the Bidders are scored against that criteria during the evaluation. The SITA Cloud Hosting Technology Stacks are included for information purposes.

The client is currently considering the following future cloud-based technology stacks. SAPS will decide, during the design stages,which of the below targeted platforms will be utilised to host the solution. Infrastructure-as-a-Service (IaaS):

1) Private On-Premise OEM Cloud (Oracle):
   (i) Oracle Linux;
   (ii) Oracle DB; and
   (iii) MySQL.
2) Private On-Premise Cloud Foundation Infrastructure (CFI) based on Huawei FusionSphere:
   (i) **Microsoft Windows Operating System (OS);**
   (ii) **SUSE (SLES) OS; and**
   (iii) **Ubuntu OS.**
   (iv) MS SQL
   (v) MySQL

(i) Private On-Premise Container-as-a-Service Platform (CaaSP) available on CFI:
1) Containers similar to Virtual Machines (VMs);
2) Kubernetes;
3) Docker; and
4) Rancher.

2.5.2. CURRENT SAPS SYSTEM PRIMARY DATA SOURCES

The exiting solution, EFRS, provides the functionality to register, update, enquire and control of legally owned firearms, as well as gunsmiths, dealers and manufacturers of firearms. It furthermore manages the information of a firearm from the time it is manufactured in the RSA or imported into the RSA until it is permanently exported or totally destroyed by the SAPS or a dedicated authority. The data in the existing solution must be fully migrated to the new FCS solution.

The complete list of data sources, with data capacity, will be determined during the analysis and design phase.

3. TECHNICAL REQUIREMENT OVERVIEW

3.1. PRODUCT DESCRIPTION

The new Firearms Control Solution will provide the following:

(a) Interface to the SPVS (SAPS Person Verification Service) for electronic verification of applicants;
(b) The technical capacity to process electronic forms, versioning, capture/digitise and relate additional information where relevant, process, verify, store, safeguard, administer and retrieve specified firearms and firearm owners related data and/or information;
(c) Electronic integrated scheduling capability (including diary management);
(d) Effective and efficient workflow management;

(e) Effective firearms management and control by means of accurate, relevant, and timely business intelligence;
(f) Secure (including 2FA and biometric access or confirmation capability) and user-friendly management throughout the life cycle of all application processes and firearms from the time of manufacture/import until deactivation, destruction and/or export;
(g) Manage the manufacturing/altered/custom built firearms, import/export, transport and/or destruction/deactivation of firearms;
(h) Seamless integration with existing legacy systems of the SAPS (including electronic payment integration) and identified external stakeholder systems;
(i) Electronic management of all firearms business/owners related documentation;
(j) Elimination of transactional related corruption via effective audit trails;
(k) Operational requirements pertaining to System performance;
(l) Accurate and advanced reporting and enquiry functionality including escalation of suspicious transactions (e.g. multiple changes on a specific entry of an application).

For illustrations purposes only, a high-level process flow of the Firearms Solution is depicted in the diagram below. As part of the analysis and design phases, the detailed designs will be developed by the service provider.

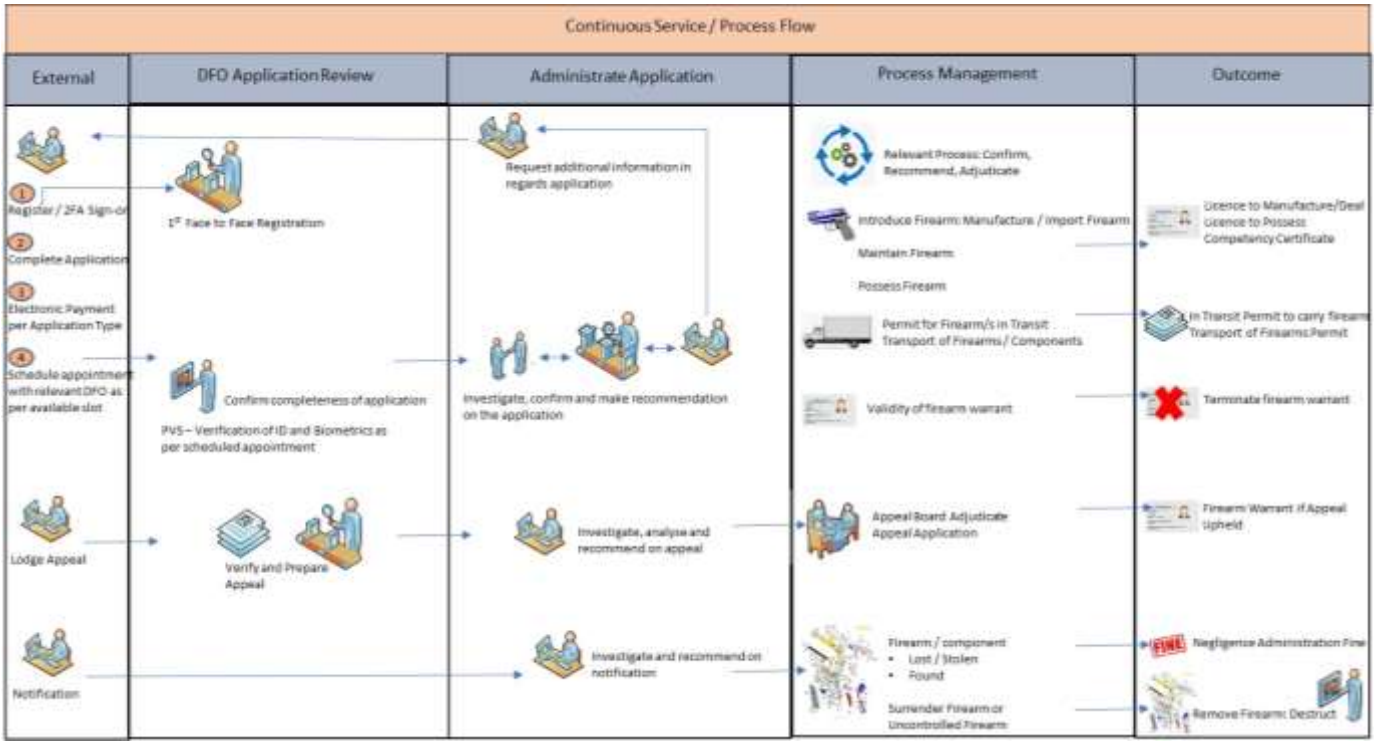

Figure 2: High level FCS Process Flow

3.2. FUNCTIONAL COMPONENTS TO BE DEVELOPED

The table below lists the cohesive solution components that needs to be developed in context of the respective project phases and release descriptions as stated in this document.

Table 3: Solution Components to be developed

Release	Solution component
1.	Develop, test and deploy **FCS Release 1 – Baseline**
2.	Develop, test and deploy **FCS Release 2 – Warrants**

Release	Solution component
3.	Develop, test and deploy **FCS Release 3 - Firearms Administrative Components**
4.	Develop, test and deploy **FCS Release 4** - **System Administrative Components**

Note 1: Release 1 forms the standardised base of the New FCS to ensure conformity and consistency for reuse in the other releases. Some of the other releases in the table above (save Release 1) can be delivered in parallel and will form part of the contract negotiations.

Note 2: Interfaces, Reports, Enquiries and Dashboard are repeated in each Phase of which some could be new in a specific phase and others are enhanced/extended in other phases.

3.2.1. DETAIL FUNCTIONAL COMPONENTS TO BE DEVELOPED

The Bidder's attention is drawn to Section 8 "Special Conditions of Contract" for information e.g. concurrent users as well as trainers to be trained.

3.2.1.1. FCS RELEASE 1 - BASELINE

(a) Register Applicant or Stakeholder (Front-end - enrol for electronic submissions).
(b) System Security: Portal, 2 Factor Access (including biometric access for internal users), User Profiles, 1st face to face Registration.
(c) Capture biometric identification including the scanning of fingerprints.
(d) User Interface (Front-end).
(e) Schedule Management.
(f) Develop electronic submission/form capability.
(g) Licence and Inspections for Dealers, Manufacturers, Gunsmiths (DMGs).
(h) Replace interim eSubmission process for DMG and Official Institution.
(i) Creation of electronic connectivity with Official Institutions: (i.e. Registers kept by Official Institutions, Establishment of central Official Institution firearms databases and Official Institution's workstations - Section 99 - 101 and Regulations 82-85 of the Firearms Control Act, Act 60 of 2000).
(j) Competencies.
(k) Licence Printing – DMG Licence and Competency.
(l) Integration (External via SiBus):
    (i) SPVS: ID Verification – integration to DHA
    (ii) 2FA
    (iii) HANIS (Deceased) - DHA
    (iv) Competency Verification - Accredited Association
    (v) Licence Printing - via IJS hub
(m) Integration (Internal via SiBus):
    (i) Data migration from EFRS to new FCS
    (ii) CRIM to verify applicant's criminal record
    (iii) ICDMS/CAS to update firearm status lost/stolen/found
    (iv) Profiling to verify and confirm applicant's information
    (v) Circulation (CIR) to verify person status
    (vi) NPIS retrieval of images
    (vii) POLFIN electronic payment
    (viii) PAS – firearm detail
    (ix) PERSAL retrieval of user information
(n) Notification messages (e.g. SMS, email or other) to Applicants and/or other SAPS personnel regarding:
    (i) Application Status
    (ii) Information Request; and
    (iii) Escalations/Follow-up
(o) Phase 1 Enquiries/Dashboard.
(p) Phase 1 Reporting.

(q) System Support: Scanning and Indexing.
(r) System Administration: User Roles and Profiles.
(s) Comprehensive Transaction Audit Trail.

3.2.1.2. FCS RELEASE 2 – Warrants

(a) Enhance User Interfaces: Additional screens (Front end) and develop the processes relating to business process requirements per application type.
(b) Licences.
(c) Renewals.
(d) Accreditations.
(e) Import/Export/In-Transit/Transport Permits.
(f) Temporary Authorisation.
(g) Duplicates.
(h) Notifications.
(i) Submission of Annual Reports for Accredited Institutions, Accredited Official Institutions and exempted DMGs.
(j) Enhanced Integration (Internal via SiBus):
    (i) Data migration from EFRS to new FCS
    (ii) CRIM & AFIS to verify applicant's criminal record
    (iii) ICDMS/CAS to update firearm status lost/stolen/found
    (iv) Profiling to verify and confirm applicant's information
    (v) Circulation (CIR) to verify person status
    (vi) NPIS retrieval of images
    (vii) SAPS 13 Property Register (handing in of firearms)
    (viii) SAPS43 Register of Exhibits
    (ix) Registration
    (x) POLFIN electronic payment
    (xi) PAS
    (xii) PERSAL
(k) Enhanced Integration (External via SiBus):
    (i) SPVS: ID Verification – integration to DHA
    (ii) 2FA
    (iii) HANIS (Deceased) - DHA
    (iv) Competency Verification - Accredited Association
    (v) Licence Printing - via IJS hub
    (vi) PSIRA for registered security officials
(l) Notification messages (e.g. SMS, email or other) to Applicants and/or other SAPS personnel regarding
    (i) Application Status;
    (ii) Information Request and
    (iii) Escalations / Follow-up.
(m) Phase 2 Extended Enquiries / Dashboard.
(n) Phase 2 Extended Reporting.
(o) Enhanced Access to System.
(p) Enhanced/Extended Data Migration from EFRS to new FCS.
(q) Enhanced/Extended Transaction Audit Trail.
(r) Enhanced/Extended Schedule Management, System Administration and Support.

3.2.1.3. FCS RELEASE 3 - Firearms Administrative Components

(a) Estates including execution of estates executor appointed by High Court.
(b) Circulations: Lost/Stolen/Found Firearms.
(c) Appeals.
(d) Surrendering.

(e) Disposal: Deactivation and Destruction.
(f) Declaration of Unfitness including declaration of unfitness by courts.
(g) Cancellation and Extension.
(h) Firearm Free Zones.
(i) Administrative Fines.
(j) Alteration of Firearms.
(k) Custom Built Firearms.
(l) Manufacturing of Firearms.
(m) Phase 3 Enhanced/Extended Integrations (Internal & External).
(n) Phase 3 Enhanced/Extended Queries / Dashboard.
(o) Phase 3 Enhanced/Extended Reporting.
(p) Enhanced Access to System.
(q) Enhanced System Administration.
(r) Enhanced Audit trail.

3.2.1.4. FCS RELEASE 4 - System Administrative Components and Reports

(a) Final Review and Confirmation of Data Migration (End to end).
(b) Enhance / change relevant processes if required to align with amendments in FCA.
(c) Manage paper documents.
(d) Support Registration and Administration.
(e) User Documentation (Guidelines).
(f) User Training.
(g) Enhanced Access to System.
(h) Enhanced System Administration.
(i) Enhanced Audit Trail.
(j) Phase 4 Enhanced\Extended Integrations (Internal & External).
(k) Finalisation and Review of Enquiries / Dashboard.
(l) Finalisation and Review of Operational Reports developed per Phase. The table below contains a summary list of the Reports.

Table 4: Summary List of FCS Operational Reports

No.	Report Name	Report Attributes
1.	Applications with outstanding information per Application Type	Province, District, Police Station, ***Application Type, Application Number, Reason, Application Details per specified period/weekly /monthly/per annum.
2.	Applications Referred Back to DFO	Province, District, Police Station, ***Application Type, Application Number, Reason, Application Details per specified period/weekly / monthly/per annum.
3.	Totals of Applications Received, Outstanding, Approved and Refused	Totals per Province, District, Police Station, ***Application Type (including sub-type) for Received, Outstanding >90 Days, Approved, Refused, per specified period, weekly, monthly, quarterly and per annum with option of all/relevant details per Application Type if required.
4.	Total Warrants (Licences/Competency/ Permit/Certificates) Issued per Type	Totals per Province, District, Police Station, ***Warrant Type (including sub-type), per specified period, weekly, monthly, quarterly and per annum with option of all/relevant details if required including date of approved, dated printed, date issued to applicant.
5.	Registered Type of Juristic (Type Accredited Institution /DMG/Official Institution)	Totals per Type per Province, per District per Police Station, per period, weekly, monthly, quarterly and per annum with option of all details of Registered Type of Juristic including status and registered/approved date.

No.	Report Name	Report Attributes
6.	Total Warrants (Licences/Competency/ Permit/Certificates) Expired	Totals per Province, District, Police Station, ***Warrant Type (including sub-type), per specified period, weekly, monthly, quarterly/per annum with relevant details including owner details, address, issued date, expiry date and date of renewal application submitted (if any) with indication of Not Renewed, Renewed Late or In Process.
7.	Total Warrants that Expire in a Certain Period	Totals per Province, District, Police Station, ***Warrant Type (including sub-type), per specified period, weekly, monthly, quarterly/per annum with relevant details including owner details, address, issued date, expiry date.
8.	Applications Cancelled with options of Application Types and period	List of all the applications which were cancelled per type, as well as their statuses at the time of the cancellation: with totals, per Province, per District, per Police Station, ***Application Type, Status of Application, Cancellation Date, Received Date for specified period (specified dates/weekly/monthly/quarterly/ annum) and with option of relevant details if required.
9.	List of eSubmission Firearm Transactions Transferred to next Owner	List of all the eSubmission transactions of firearms transferred to next owner, with totals, per Province, District, Police Station, Firearm Details, Transaction Date, Submission Date, Owner Transferred to and Submitter detail for specified period, monthly, quarterly and per annum.
10.	Annual Reports Not Submitted for a Specific Period	List of Annual Reports Not Submitted for a Specific Period from Accredited Association, Businesses and Official Institution.
11.	List of Total Accredited Institutions whom Ceased to Carry on Business	List of the total number of Accredited Institutions which ceased to carry on business: with totals, per Type per Province, per District, per Police Station for specified period (specified dates/weekly/ monthly/quarterly/annum) and with option of relevant details if required.
12.	Report of Applications for Export/In-transit Permits Referred to Scrutiny Committee and NCACC	List of Applications for Export/In-transit Permits Referred to Scrutiny Committee and NCACC, per Type, per Province, per Police Station for specified period (specified date/weekly/monthly/ quarterly/annum) and Application details.
13.	Firearms Physically Imported/Exported	List the total number of exported firearms on National Level, per Type, per Province, per Police Station, per Port for specified period (specified dates/weekly/monthly/quarterly/annum) and details of permit.
14.	Ammunition Physically Imported/Exported	List the total number of exported ammunition on National Level, per Type per Province, per Police Station, per Port for specified period (specified dates/weekly/monthly/quarterly/annum) and details of permit.
15.	Outstanding Notifications for Change of Commercial Agent Premises	List of notifications for change of Commercial Agent premises that are outstanding for a specific period (specified dates/weekly/ monthly/quarterly/annum) and details, per Notification, per Province, per Police Station including notification details, received date, address and status of warrant.
16.	List of Warrants Issued/not issued for all Approved Applications to Applicants	Check list of warrants that are approved and issued/not issued for approved applications per ***Application Type, per Province, per Police Station for specified period (specified dates/weekly/ monthly/quarterly/annum) and details of warrant.
17.	List of Outstanding Requests for the Deactivation of a Firearm	List the total number of outstanding requests for Deactivation on National Level per Firearm Type, per Province, per Police Station for specified period (specified dates/weekly/monthly/quarterly/ annum) and details of requestor, firearm/s and registered owner if relevant.

No.	Report Name	Report Attributes
18.	List of Destroyed Firearm Items	List the total number of Destroyed Firearms per Firearm Type, per Province, per District, per Police Station and details of reason for destruction, firearms owner details and firearm details for specified period (specified dates, weekly/monthly/quarterly and per annum).
19.	List of Deceased Person with the Total Number of Firearm Warrants	List the total number of Deceased Persons, per Province, per Cluster, per Police Station including deceased Persons' details, firearm warrant/s and firearm detail/s for the specific period, weekly, monthly, quarterly and per annum.
20.	List of All Inactive Firearm Warrant Holders	List the total number of Inactive Firearm Warrant Holders, per Province, per Cluster, per Police Station including inactive firearm owner details, firearm warrant/s and firearm detail/s for the specific period (specified dates, weekly/monthly/quarterly/ annum).
21.	Total Firearm Licences Issued per Design Type/ Calibre/ Make	List the total number of Firearm Licences Issued per Firearm Type, Design, Calibre, Make, per Province, per District, per Police Station for specified period, weekly, monthly, quarterly and per annum.
22.	List of Firearms Forfeited to the State	List the total number of Firearms Forfeited to the State, per Firearm Type, Design, Calibre, Make, per Province, per District, per Police Station for specified period, weekly, monthly, quarterly and per annum.
23.	List of All Found Firearms	List the total number of Found Firearms per Firearm Type, Design, Calibre, Make, Status date, including the Firearm Owner details, per Province, per District, per Police Station for specified period, weekly, monthly, quarterly and per annum.
24.	List of All Found Firearms against Lost or Stolen Firearms	List the total number of Found Firearms against Lost or Stolen Firearms, per Firearm Type, Design, Calibre, Make, Status date, including the Firearm Owner details, per Province, per District, per Police Station for specified period, weekly, monthly, quarterly and per annum.
25.	List of Lost or Stolen Firearms	List the total number of Lost or Stolen Firearms per Firearm Type, Design, Calibre, Make, Status date, including the Firearm Owner details, per Province, per District, per Police Station for specified period, weekly, monthly, quarterly and per annum.
26.	List of All Found Firearms Handed Back to Owner	List the total number of Found Firearms Handed Back to Owner per Firearm Type, Design, Calibre, Make, Status date, including the Firearm Owner details, per Province, per District, per Police Station for specified period, weekly, monthly, quarterly and per annum.
27.	List of Negligence Cases Opened	List the total number of Negligence Cases Opened including the Firearm Details, the Firearm Owner details per Province per District per Police Station for specified period, weekly, monthly, quarterly and per annum.
28.	List of All Firearm Identification Numbers (FIN) Issued	List the total number of all the Firearms issued with FIN (Firearm Identification Number) including the Firearm Details, the Firearm Owner details, per Province, per District, per Police Station for specified period, weekly, monthly, quarterly and per annum.
29.	List of System Hardware and Software Problems	List total number of the system/software problems registered, per Province, Area, Police Station, Reporting person details, Description of problem, Status and Date for specified period and monthly.
30.	List of Requests for System Service	List total number of all the Requests for System Service (data errors, maintenance and enhancement), per service type, description and date per specified period, monthly, quarterly and per annum.

No.	Report Name	Report Attributes
31.	Outstanding Notifications of Change in Circumstances	List the total number of Outstanding Notifications of Change in Circumstances, the Firearm Owner details, per Province, per District, per Police Station for specified period, weekly, monthly, quarterly and per annum.
32.	Total Notifications for Appointment of New Responsible Person for a Juristic Person Received	List the total number of all the Notifications of the Appointment of New Responsible Person Received for a Juristic Person, details of Juristic Person, New Responsible Person details, Previous Responsible Person ID, per Province, per Area, per Police Station for specified period, weekly, monthly, quarterly and per annum.
33.	Issue of Warrants After Notification of Appointment of New Responsible Person	List of total number of warrants issued after Notification of new Responsible Person, per Province, Area, Police Station, Notification number, Status, received date, Status date, Type of warrant, Warrant number and Warrant details for specified period, monthly, quarterly and per annum.
34.	Outstanding Notifications of Appointment of New Responsible Person not Processed Completely	List the total number of Outstanding Notifications of Appointment of New Responsible Person not finalised, per Province, per Area, per Police Station Juristic Person details, the New Responsible Person details and Current Responsible Person ID for specified period, weekly, monthly, quarterly and per annum.
35.	Total Notifications Received after Change of Address	List the total number of Notifications Received after Change of Address including the Juristic Person details, address details, per Province, per Area, per Police Station for specified period, weekly, monthly, quarterly and per annum.
36.	List of Firearms Transferred to New Owners by DMGs/Official Institutions	List the total number of Firearms Transferred to New Owners by DMGs/Official Institutions including transfer dates, Transferring Juristic Person details, firearm details, per Province, per Area, per Police Station, per Juristic Person, per Firearm Type for specified period, weekly, monthly, quarterly and per annum.
37.	List of Firearms Destroyed by Official Institutions	List the total number of Firearms Destroyed by Official Institutions, per Province, per District, per Police Station per Official Institution, per Firearm Type, Design, Calibre, Make for specified period, weekly, monthly, quarterly and per annum.
38.	List of Firearms Deactivated by Official Institutions	List the total number of Firearms Deactivated by Official Institutions, per Province, per District, per Police Station, per Official Institution, per Firearm Type, Design, Calibre, Make for specified period, weekly, monthly, quarterly and per annum.
39.	List of Persons Declared Unfit to Possess a Firearm	List the total number of Persons Declared Unfit to Possess a Firearm, per Province, per District, per Police Station including Person details, per Firearm Type, firearm details for specified period, weekly, monthly, quarterly and per annum.
40.	List of Persons where the Unfitness was Reversed	List the total number of Reversed Persons Declared Unfit to Possess a Firearm, per Province, per District, per Police Station including Person details for specified period, weekly, monthly, quarterly and per annum.
41.	List of Firearms and Ammunition in Safe Storage at Border Post	List the total number of Firearms and Ammunition Storage at Border Post, per Province, per District, per Border Post including Firearm Owners details, Firearm details, Ammunition details for specified period, weekly, monthly, quarterly and per annum.

No.	Report Name	Report Attributes
42.	List of Firearm Warrants Surrendered	List the total number of Firearm Warrants Surrendered, per Province, per District, per Police Station including Person details, Firearm Warrant details for specified period, weekly, monthly, quarterly and per annum.
43.	List of Surrendered Firearm Items	List the total number of Surrendered Items, per Province, per District, per Police Station including Person details, Firearm Item details for specified period, weekly, monthly, quarterly and per annum
44.	List of Firearm Warrants Suspended / Extended / Uplifted / Reinstated	List the total number of Firearm Warrants Suspended/Extended/ Uplifted/Reinstated, per Province, per District, per Police Station, per Status including Person details, Firearm Warrant details for specified period, weekly, monthly, quarterly and per annum.
45.	List of Registered Users: Active, Inactive, Revoked	List the total number of Registered Users, per Status of Active/ Inactive/Revoked, per Province, per District, per Police Station including Person details for specified period, weekly, monthly, quarterly, or per annum.
***	**List of all Application or Warrant Types** Accreditations: Competency:	- Official institution - Accreditation, as a hunting association - Accreditation, as a sport shooting association - Accreditation, as a collectors' association - Accreditation for hunting purposes - Accreditation, as provider of security services for own use - Accreditation for other business purposes - Accreditation, as a game rancher - Accreditation, as a public collector - Accreditation, as a shooting range where ammunition may be sold - Accreditation to provide firearms for theatrical, film and television production - Accreditation, as a provider of training - Accreditation, as a museum - Accreditation, as a hunting association - Accreditation, as a sport shooting association - Accreditation, as a collectors' association - Accreditation for hunting purposes - Accreditation, as provider of security services for own use - Accreditation for other business purposes - Accreditation, as a game rancher - Accreditation, as a public collector - Accreditation, as a shooting range where ammunition may be sold - Accreditation to provide firearms for theatrical, film and television production - Accreditation, as a provider of training - Accreditation, as a museum - Competency certificate to possess a firearm as a collector - Competency certificate to possess a firearm. Types e.g. Handgun/Shotgun/Rifle/ S/L-RIFLE/CARB/PIST CAL CARB/ Muzzle loading etc. - Competency certificate for Commercial Agents (Dealer/ Manufacturer/Gunsmith) - Further Competency

No.	Report Name	Report Attributes
	Licences:	- Licence to Possess a Firearm - Additional Licence to Possess a Firearm - Commercial Agents Licence (Dealer/Manufacturer/Gunsmith) - Manufacture New Firearm or Ammunition Type - to Possess More than 200 Cartridges - to Possess More than 2400 primers
	Permits:	- Permit to collect ammunition - Permit for acquisition of firearms by Accredited Official Institutions - Permit to Import/Export/Multiple/In-transit /Transport
	Temporary Authorisations:	- Temporary Authorisations for Licence to Possess - Temporary Authorisations for Commercial Agents (DMGs)
	**Warrants:	- Firearm warrant renewals (on All the warrant types listed above) - Firearm warrant duplicates (on All the warrant types listed above - Compensation
	**Including Applications for:	- Firearm Free Zone

3.2.2. RELEASE HANDOVER TO SITA APPLICATION MAINTENANCE AND FUNCTIONAL APPLICATION SUPPORT

As part of the transition in the releases from development, after the post-go-live support period is ended, the service provider will be required to hand the related release artefacts and source code over to the SITA AM and FASS maintenance and support teams to enable them to maintain and support the various products.

In-between implementation services and application support, there will be a transition period of approximately eight weeks during which the required competencies, to maintain and support the products, will be established by SITA.

3.2.3. GENERAL FUNCTIONAL/USER REQUIREMENTS

The service provider must, as part of the analysis, formalise the detail user requirement to ascertain compliance with the desired outcome of the client in consideration of the provision of this specification.

3.2.3.1. CUSTOMIZABLE/MAINTAINABLE USER INTERFACE

(a) User interface can be customised/maintained to match changing business rules and needs, and adapts to the specific roles and responsibilities of different users and user levels.
(b) User configurable home page (portal) giving the information each user needs on login and during each session.
(c) Provide for calendar scheduling to enable users to choose available slot or appointment with relevant DFO.
(d) Solution must connect to both SAPS network and Internet via DMZ and SiBuS.

3.2.3.2. DATA COLLECTION AND INPUT

(a) Provides for structured data capturing.
(b) Provides for structured and configurable workflow.

(c) Automated input/import and indexing of electronic files including Microsoft Office, Email, Adobe, HTML, as well as visual artefacts.
(d) Provide for automated data migration to new data structure.
(e) Batch and transactional input from internal and external data sources.
(f) Confidential source management: Secure management of sensitive and confidential person and firearm data.
(g) Non-electronic documents: Automated loading and indexing of scanned images of non-electronic documents with specific indexes relating to applications.
(h) Capturing of fingerprints data from biometric scanners.
(i) Confirm compatibility of Browsers used by SAPS.

3.2.3.3. INFORMATION SHARING

(a) Enabled data exchange via the SAPS SiBus internal and external to the SAPS, including via the IJS hub.
(b) Secure and configurable workflow per relevant business process.
(c) Secure infrastructure for compatibility with existing Systems via industry standard technologies; e.g. PERL, SOAP, Web Services, etc.
(d) Real-time search of all firearm related database information and notification of results via mobile technology and Web technology.

3.2.3.4. HELP FUNCTION

(a) Context sensitive help on every System dialogue and guidelines documentation.
(b) Artificial Intelligence (AI) based Chatbot.

3.2.3.5. TRAINING MATERIAL

(a) Editable training material on every component / business process functionality.

3.2.4. SOLUTION ADMINISTRATION REQUIREMENTS

The service provider must, as part of the analysis, formalise the detail user requirement to ascertain compliance with the desired outcome of the client in consideration of the provision of this specification.

3.2.4.1. USER ADMINISTRATION

(a) User administrators from the SAPS are able to create user profiles.
(b) User administrators manage access control to users according to defined data groups and user classifications/roles.
(c) User administrators can distribute user management responsibilities to specific users, units or departments.
(d) User administrators manage/configure users on workflow capability.
(e) Data security is based on user group and individual profile settings.
(f) User friendly interface to allow non-technical staff to add, change, edit, group, remove and reallocate users.

3.2.4.2. SYSTEM ADMINISTRATION

(a) Data integrity facilities to ensure non-repudiation where required and System configuration (application functionality and workflow) and data remain in optimal condition.
(b) System administrator manages configurable codes and descriptions to add, change, edit and set status as will be described in the detailed requirements conducted by the service provider during analysis.

3.2.4.3. EXTENSIBILITY

(a) The capability to integrate third party tools and plug-ins to comply with modern investigative methods, by means of interface through Application Programming Interfaces (APIs).

3.2.4.4. USER ACCESS CONTROL

(a) Suitable level of user access control mechanisms for internal and external users' management as per the respective roles and responsibilities.
(b) Dissemination of data within defined security rules of user profile.

3.2.4.5. AUDITING

(a) Provide comprehensive audit trail that records all user and administrative activity performed on the system.
(b) Audit trail is immediately available for search/review/analysis by appropriate staff, without IT support.
(c) All administration actions on the System are recorded and audited.

3.2.4.6. SECURITY

(a) 2 Factor Authenticating (2FA) is required for every user assigned with a unique log-in and password that can integrate with Microsoft Active Directory login, biometric for internal and OTP capability for external users.
(b) Provide security groups based on multiple security clearance levels.
(c) Access control mechanisms, including privileges that control and confirm where relevant every operation on the System – including read, write, update, delete, print, export, secure and link.
(d) The requirements to deliver the solution must conform to the following security related concerns:

(i) Authentication-The authenticity of the identity of person or entity related to a system;

(ii) Authorisation-The definition and enforcement of permitted capabilities for a person or entity whose identity has been established;

(iii) Audit- The ability to provide forensic data attesting that the system was used in accordance with stated security policies;

(iv) Assurance- The ability to test and prove that the system has the security attributes required to uphold the stated security policies;

(v) Availability- The ability of the system to function without service interruption or depletion despite abnormal or malicious events;

(vi) Asset protection- The protection of information assets from loss or unintended disclosure, and resources from unauthorized and unintended use; and

(vii) Administration- The ability to add and change security policies, add or change how policies are implemented in the system, and add or change the persons or entities related to the system;

(e) Database Security-Ensure databases are secured and managed correctly by use of encryption.
(f) Data Security-Employ mechanism that ensures no data loss or duplication while capturing or importing data.
(g) The system must demonstrate stored data confidentiality, integrity and availability and must be securely accessed.
(h) The system must comply with the Protection of Personal Information Act (POPIA) and ISO27001 IT Security Certified Solution.

3.2.5. DATA PROCESSING AND SEARCHING REQUIREMENTS

The service provider must, as part of the analysis, formalise the detail user requirement to ascertain compliance with the desired outcome of the client in consideration of the provision of this specification.

3.2.5.1. DATA PROCESSING

(a) Consolidation of applications submitted to centralised data sources after initial validations in Sandbox.
(b) Provide automated standardised validations and escalations and/or workflow capability.
(c) Access, search, visualisation and analysis of information from central data sources.

(d) Provide multiple enquiry methods internal and external to the SAPS.
(e) Secure data processing without data corruption.

3.2.5.2. AUTOMATED SEARCHING

(a) Automated searches of target datasets internal and external to the SAPS.
(b) Ensure that the search only produce expected results for data confidentiality.

3.2.5.3. FEDERATED SEARCHING

(a) Single point searching of internal and external database Systems.
(b) Simultaneous search of locally held and external data.

3.2.5.4. DATA OUTPUT

(a) Capabilities for comprehensive and intelligent reporting on all relevant data within the solution.
(b) Provide alerting/notification, auditing and dashboards.
(c) Provide automated standardised warrants.

3.3. TECHNOLOGY REQUIREMENTS

The technology requirements to deliver the solution must conform to the customer infrastructure and environment as described in this specification. The technology goal is to be technology agnostic and utilise open-source technologies, as far as possible to reduce the impact on procuring and maintaining software licenses. The solution must be secure and enable and implement data protection and privacy principles.

3.4. SERVICE DELIVERABLES

The following artefacts must be delivered for the FCS Project with enhancements for each of the release phases in compliance with the SAPS standards:

(a) Project Management deliverables including the detailed project plan reflecting the scope of work, details of all work breakdown elements, start and finish dates, quantity and type of resources assigned per Release (indicated above), per task and the budgeted cost for work scheduled.
(b) The below product listing indicates during which Release the respective product must be delivered and/or maintained.

Product	**Release Number**
Project Charter	Project Management
Project Schedule	Project Management
Implementation plan and approach	Project Management
Project risk/Issue register	Project Management
Payment Schedule aligned to the accepted milestones	Project Management
Project meeting agenda and minutes	Project Management
Project performance reports	Project Management
Product acceptance certificates required for payments	Project Management
Project closure report	Project Management
Project artefacts stored in the SITA project repository.	Project Management
Project handover certificate issued to SITA	Project Management
Solution Architecture	1 updated in 2,3,4
Security Architecture	1 updated in 2,3,4
Data Architecture	1, updated in 2,3,4
Data Migration Strategy	1, updated in 2,3,4
Data Migration Plan	1,2,3,4
Business Architecture	1, updated in 2,3,4

Verified to-be Business Process Models	1,2,3,4
Functional Design Specification (FDS)	1,2,3,4
Technical Design Specification	1,2,3,4
Integration Control Documents (ICD)	1,2,3,4
Integration Design Documents (IDD)	1,2,3,4
Developed components and services	1,2,3,4
Integrated components and services	1,2,3,4
Integrated source code	1,2,3,4
Test Use Cases	1,2,3,4
Unit test results	1,2,3,4
Training Material	1,2,3,4
Security testing Acceptance Certificate	1,2,3,4
Security test report with the security findings.	1,2,3,4
IT Audit report with supporting audit findings	1,2,3,4
Help Guideline	1,2,3,4
Artificial Intelligence (AI) based Chatbot	1,2,3,4
Test plans	1,2,3,4
System Integration test results (SIT)	1,2,3,4
User acceptance test results (UAT)	1,2,3,4
User Acceptance Test Certificate	1,2,3,4
Migrated data	1,2,3,4
Data migration reconciliation	1,2,3,4
Data migration certificate	1,2,3,4
Production deployment acceptance certificate	1,2,3,4
Packaged components with the deployment instructions for SITA to independently deploy the released products into production environments	1,2,3,4
Trained trainers	1,2,3,4
Release management deployment guide.	1,2,3,4
Release management release note.	1,2,3,4
Release management change authority board note	1,2,3,4
If any, COTS components, COTS source code and/or any other COTS artefacts.	1,2,3,4
If any, licenses.	1,2,3,4, Project closure

3.5. PROJECT GOVERNANCE

The following tools, techniques and documents will be utilised for project control throughout the project life cycle. The service provider project manager will be responsible for the compilation of the required documentation specified according to SITA quality requirements. These documents will be submitted at the specified frequency to the SITA project manager for approval and presentation to the appropriate client forum. All submitted documents will be recorded in the Project Master Record Index (MRI) under SITA document configuration control. The Agile activities, to manage the project, and related products, must complement the below general project governances/functions.

No.	Control Measure	Tool/Technique/Document	Frequency	Stakeholder
1.	Project Financials including Billing	Microsoft Project Plan/Schedule Payment Schedule Invoicing Acceptance Certificates	• Monthly	Project Manager (SITA) Project Manager (Service Provider) Project Steering Committee

No.	Control Measure	Tool/Technique/Document	Frequency	Stakeholder
2.	Project resources and stakeholder Management	Stakeholders engagement plan/ project structures Decision and escalation/reporting lines	• Daily • Weekly • Monthly	Project Manager (SITA) Project Manager (Service Provider)
3.	Project Progress/ Performance Management	Project Progress meetings/ reports Steering Committee meetings/ reports	• Weekly • Monthly • Monthly	Project manager (SITA) Project Manager (Service Provider) Project Steering Committee
4.	Project Risks/Issue Management	Risk and Issue identification and management plan as per • Risk register • Issue log	• Weekly • Monthly	Project Manager (SITA) Project Manager (Service Provider) Project Steering Committee
5.	Project Implementation Management	Project implementation plan/approach Previous Lessons learnt Previous Close out reports Previous Release Management inputs	• Monthly	Project Manager (SITA) Project Manager (Service Provider) Project Steering Committee
6.	Project Time Management	Microsoft Project Plan/Schedule	• Monthly	Project Manager (SITA) Project Manager (Service Provider)
7.	Scope Management	Project Charter User requirements specification Change Control	• Weekly • As and when required • Monthly	Project Manager (SITA) Project Manager (Service Provider) Project Steering Committee
8.	Schedule Management	Microsoft Project Plan/Schedule Project Progress Reports Change Control Project Steering Committee report Time tracking	• Weekly • Weekly / Monthly • As and when required • Monthly	Project Manager (SITA) Project Manager (Service Provider) Project Steering Committee
9.	Quality Management	Bi - weekly product quality verification demonstrations Project charter System Specifications Test Plan SIT UAT Signoff Certificates	• Bi-weekly • Per release	Project Manager (SITA) Project Manager (Service Provider) Senior Quality Assurance Analyst (SITA) SAPS Users Steering Committee
10.	Project Artefacts Control	Project repository SITA ERP and BPS systems evidence attachments	• Weekly	Project Manager (SITA) Project Manager (Service Provider) SITA EPMO

3.6. SERVICE DURATION

Start Date: Date of contract signature (ASAP).

Finalised and Handed Over in Production as per agreed upon project delivery schedule as per this tender specification that will be used to establish the contract duration. SAPS is expected to deliver the system on or before 05 August 2023 as per court order. The service provider shall endeavour to meet the aforesaid deadline.

3.7. PROJECT DELIVERY PERFORMANCE METRICS

The evidence for a specified deliverable is required, as follows:

(a) Deliverable based as per 3.4 SERVICE DELIVERABLES;
(b) Compliance to 3.5 PROJECT GOVERNANCE;
(c) Compliance to SAPS/SITA document and governance standards;
(d) Compliance to user and design specifications;
(e) Weekly submitted source code into SITA source code repository;
(f) Weekly submitted authored documents to a common shared project repository and the SITA ERP/BPS systems;
(g) Unit test results verified by the responsible SITA Test Analyst;
(h) SIT test results certified by the responsible SITA Test Analyst;
(i) UAT test results certified by the SAPS and the responsible SITA Test Analyst;
(j) SITA certified deliverables – all documents as per 3.4. SERVICE DELIVERABLES signed by SITA; and
(k) SAPS certified deliverables – all documents as per 3.4. SERVICE DELIVERABLES signed by SAPS.
(l) Document references:
    (1) SITA Quality Management Policy, eNSQS114_2-0, 2018-08-31
    (2) SITA Way Project Management Methodology Manual, eEPMO-00229, v1.0, 2015
    (3) SITA Risk Management Policy, eSCRM00002 v2, 2021-12-01
    (4) SITA Information Security Policy No: eGISS-00040_2-1, 2021-03-04.
    (5) Procedure for Document Configuration Management for SITA, eKMRC00022 v1.0, 2013-01-30
    (6) MIOS, Minimum Interoperability Standards (MIOS) Framework for Government Information Systems revision 6.00 march 2017

4. BID EVALUATION STAGES

The bid evaluation process consists of several stages that are applicable according to the nature of the bid, as defined in the table below.

Table 5: BID Evaluation Stages

No.	Stage	Description	Applicable for this bid
1.	Stage 1A	Administrative pre-qualification verification	YES
2.	Stage 1B	Compulsory Virtual briefing session	YES
3.	Stage 2A	**Technical Mandatory** requirement desk top evaluation	YES
4.	Stage 2B	**Technical Functionality** requirement desk top evaluation	YES
5.	Stage 2C	**Solution Due Diligence** evaluation	YES
6.	Stage 3	Special Conditions of Contract verification	YES
7.	Stage 4	Price/B-BBEE evaluation	YES

The bidder must qualify for each stage to be eligible to proceed to the next stage of the evaluation.

ANNEX A.1: ADMINISTRATIVE PRE-QUALIFICATION

5. ADMINISTRATIVE PRE-QUALIFICATION REQUIREMENTS

5.1. ADMINISTRATIVE PRE-QUALIFICATION VERIFICATION

(1) The bidder **must comply** with ALL of the bid pre-qualification requirements in order for the bid to be accepted for evaluation.

If the Bidder failed to comply with any of the administrative pre-qualification requirements, or if SITA is unable to verify whether the pre-qualification requirements are met, then SITA reserves the right to

(a) Reject the bid and not evaluate it; or

(b) Accept the bid for evaluation, on condition that the Bidder must submit within seven (7) days, any supplementary information to achieve full compliance, provided that the supplementary information is administrative and not substantive in nature.

5.2. ADMINISTRATIVE PRE-QUALIFICATION REQUIREMENTS

(1) **Submission of bid response**: The bidder has submitted a bid response documentation pack –

(a) that was delivered at the correct physical or postal address and within the stipulated date and time as specified in the "Invitation to Bid" cover page; and

(b) in the correct format, as one original document, two (2) copies and a copy on memory stick.

(2) **Attendance at briefing session**: A **Compulsory Virtual** briefing session will be held. The bidder will be required to sign the briefing session attendance register using the same information (bidder company name, bidder representative person name and contact details), as submitted in the bidder's response document. The attendance of the briefing session is compulsory.

(3) **Registered Supplier**. The bidder is, in terms of National Treasury Instruction Note 3 of 2016/17, registered, as a Supplier on National Treasury Central Supplier Database (CSD).

ANNEX A.2: TECHNICAL MANDATORY, FUNCTIONALITY AND DUE DILIGENCE REQUIREMENTS

6. TECHNICAL MANDATORY

6.1. INSTRUCTION AND EVALUATION CRITERIA

(1) The bidder **must comply with ALL the requirements by providing substantiating evidence** in the form of documentation or information, failing which it will be regarded as "NOT COMPLY".

(2) The bidder **must provide a unique reference number** (e.g. binder/folio, chapter, section, page) to locate substantiating evidence in the bid response. During evaluation, SITA reserves the right to treat substantiation evidence that cannot be located in the bid response as "NOT COMPLY".

(3) The bidder **must complete the declaration of compliance,** as per section 6.3 below by marking with an "X" either "COMPLY", or "NOT COMPLY" with ALL of the technical mandatory requirements, failing which it will be regarded, as "NOT COMPLY".

(4) The bidder must comply with ALL the TECHNICAL MANDATORY REQUIREMENTS in order for the bid to proceed to the next stage of the evaluation.

(5) No URL references or links will be accepted as evidence.

(6) SITA reserves the right to verify the information pertaining to the evidence provided by the bidder.

The bidder will be required to present their proposal where the Bid Evaluation Committee will clarify bids received.

6.2. TECHNICAL MANDATORY REQUIREMENTS

No	TECHNICAL MANDATORY REQUIREMENTS	*Substantiating evidence of compliance* *(used to evaluate bid)*	*Evidence reference* *(to be completed by bidder)*
1.	**BIDDER EXPERIENCE AND CAPABILITY REQUIREMENTS** The bidder must have developed information system(s) comparable in size and complexity as stated in this bid specification in section 2.2, section 3.2, prescribed technology stack in section 2.5. as well as time constraints in section 3.6, for at least one (1) customer in the last five (5) years.	The bidder must have developed information system(s) comparable in size and complexity as stated in this bid specification in section 2.2, section 3.2, prescribed technology stack in section 2.5. as well as time constraints in section 3.6, for at least one (1) customer in the last five (5) years. The Bidder is required to complete Annex B section 11.1. **Note:** SITA reserves the right to verify the information provided. **Note:** The effort to deliver a solution, of this complexity, scope of work and time constraint, on the technology stated in this specification must be considered.	<provide unique reference to locate substantiating evidence in the bid response – see Annex B section 11.1>

No	TECHNICAL MANDATORY REQUIREMENTS	*Substantiating evidence of compliance* *(used to evaluate bid)*	*Evidence reference* *(to be completed by bidder)*
2.	**PRODUCT OR SERVICE TECHNICAL AND FUNCTIONAL REQUIREMENTS** The bidder must confirm that the solution to be implemented complies with the Technical and Product Service Requirements for the Firearms Control Solution as detailed in this Specification.	**Requirement 1**: The bidder must comply with the Technical and Product Service Requirements by completing ANNEX C: Addendum1. **and;** **Requirement 2**: The Bidder is required to provide a logical architecture that depicts the proposed solution, conforming to the functional and technical requirements as stated in this specification, with a supporting catalogue that lists and describes the architectural components and related relationships between the components. ANNEX B, section 11.2 to be completed in this regard. **Note:** SITA reserves the right to verify the information provided.	<provide unique reference to locate substantiating evidence in the bid response – see Annex B section 11.2 and Annex C: Addendum 1>
3.	**SPECIAL CONDITIONS OF CONTRACT** Bidder needs to Accept all the Special Conditions of Contract	Bidder needs to accept all the Special Conditions of Contract **referred** to in Section 8, by completing section 8.3 **Note:** Failure not to Accept all the Special Conditions of Contract will result in disqualification.	<provide unique reference to locate substantiating evidence in the bid response – see Sec 8.3 >
4.	**THIRD PARTY RISK MANAGEMENT ASSESMENT** The bidder must confirm compliance to Third Party Risk Management Assessment.	The Bidder **must** comply to the Third-Party Risk Management Assessment requirement by completing All the questions in **Annex E.**	<provide unique reference to locate substantiating evidence in the bid response – see Annex B, section 11.3 and Annex E>

6.3. DECLARATION OF COMPLIANCE

	Comply	Not Comply
The bidder declares by **indicating with an "X"** in either the "COMPLY" or "NOT COMPLY" column that: (a) The bid complies with each and every TECHNICAL MANDATORY REQUIREMENT, as specified in SECTION 6.2 above; AND (b) Each and every requirement specification is substantiated by evidence as proof of compliance.		

7. TECHNICAL FUNCTIONALITY

7.1. INSTRUCTION AND EVALUATION CRITERIA

(1) The bidder **must complete, in full, all of the TECHNICAL FUNCTIONALITY requirements**.

(2) The bidder, where applicable, **must provide a unique reference number** (e.g. binder/folio, chapter, section, page) to locate substantiating evidence in the bid response. During evaluation, SITA reserves the right to treat substantiation evidence that cannot be located in the bid response, as "NOT COMPLY".

(3) Evaluation per requirement. The evaluation (scoring) of bidders' responses to the requirements will be determined by the completeness, relevance and accuracy of substantiating evidence, where applicable.

(4) Functionality will be evaluated by conducting the following two (2) consecutive independent stages in the tender processes:

(a) Desk Top Evaluation of TECHNICAL FUNCTIONALITY REQUIREMENTS (Stage 2B)

(b) Evaluation of the Proposed Solution DUE DILIGENCE (Stage 2C)

(5) **Weighting of requirements:** The score for the desktop evaluation of TECHNICAL FUNCTIONALITY REQUIREMENTS will be calculated as follows:

(a) Each Bidder will be evaluated on each individual requirement as indicated in the tables in sections 7.2 below.

(b) The value scored for each requirement will be multiplied with the specified weighting for the relevant requirement to obtain the percentage achieved for each requirement.

No.	Technical Functionality Requirements	Weighting
1.	Technology Stack	25%
2.	Competency to utilise specified technologies	25%
3.	Achievement of Business Objectives	25%
4.	Solution implementation must be POPIA and ISO27001 compliant	25%
	TOTAL	**100%**

(6) **Minimum threshold**. The individual scores will be converted to a cumulative percentage and only those bidders that achieve or exceed the minimum threshold score of **60%** will be eligible to proceed to the next stage, i.e. the Demonstrations Stage.

(7) **Note: The Yes/No Answers for the questionnaire below must be attached to Annex B, section 11.4.**

7.2. TECHNICAL FUNCTIONALITY REQUIREMENTS

No.	TECHNICAL FUNCTIONALITY REQUIREMENT	Substantiating evidence and evidence reference to be completed by bidder. Evaluation per requirement: Each question indicated in the tables below must be completed and will be scored. In column marked Y/N: Mark as Y for "comply" and N for "not-comply", if not marked Y/N it is regarded as N In column marked Evidence: Provide evidence Point will be scored according to relevant evaluation criteria specified for each question per 'Y/N'.			Weight
1.	**Technology Stack** (a) Front-end (b) Middleware		Y/N	**Evidence:** The Bidder must provide your detailed technology stack that will be used to develop	25%

<table>
<tr><th>No.</th><th>TECHNICAL FUNCTIONALITY REQUIREMENT</th><th>Substantiating evidence and evidence reference to be completed by bidder. Evaluation per requirement: Each question indicated in the tables below must be completed and will be scored.
In column marked Y/N: Mark as Y for “comply” and N for “not-comply”, if not marked Y/N it is regarded as N
In column marked Evidence: Provide evidence
Point will be scored according to relevant evaluation criteria specified for each question per ‘Y/N’.</th><th>Weight</th></tr>
<tr><td></td><td>(c) Back-end
(d) Provide list of all the open source licensed components
(e) Provide a list of all the commercially licensed components
(f) Integration Technology</td><td>
<table>
<tr><td></td><td></td><td>and host the production solution that is categorised into commercial and open source technology. <provide unique reference to, including page and paragraph number, locate substantiating evidence in the bid response – add to Annex D: Addendum 2>
The Bidder must indicate Yes (Y) or No (N) by selecting the appropriate item below that supports the evidence provided.</td></tr>
<tr><td>a.</td><td></td><td>Open source and utilising existing SAPS licenses.</td></tr>
<tr><td>b.</td><td></td><td>Combination of open source, additional commercial licences and existing SAPS licenses.</td></tr>
<tr><td>c.</td><td></td><td>Additional commercial licenses required, over and above existing SAPS licenses.</td></tr>
<tr><td>d.</td><td></td><td>Not Specified</td></tr>
</table>
Evaluation: Each point will be scored according to the following criteria:
(a) 20 = Open source and utilising existing SAPS licenses.
(b) 15 = Combination of open source, additional commercial licences and existing SAPS licenses.
(c) 10 = Additional commercial licenses required, over and above existing SAPS licenses.
(d) 0 = Not Specified
Note 1: SITA reserves the right to verify the information provided.

Note 2: Complete declaration in Annex D: Addendum 2.</td><td></td></tr>
</table>

No.	TECHNICAL FUNCTIONALITY REQUIREMENT	Substantiating evidence and evidence reference to be completed by bidder. Evaluation per requirement: Each question indicated in the tables below must be completed and will be scored. In column marked Y/N: Mark as Y for "comply" and N for "not-comply", if not marked Y/N it is regarded as N In column marked Evidence: Provide evidence Point will be scored according to relevant evaluation criteria specified for each question per 'Y/N'.	Weight
2.	**Competency to utilise specified technologies** Select the technologies for which the bidder is competent, and has the required skill and experience.	Y/N — The Bidder must indicate Yes (Y) or No (N) to indicate whether the Bidder is competent, skilled and have suitable experience for each respective technology listed below. a. — Current Microsoft Based technology stack i. — Microsoft .Net ii. — Microsoft SQL Database iii. — Microsoft Windows Server operating system iv. — Microsoft IIS application server b. — Current Oracle technology stack i. — JEE framework ii. — Oracle Database iii. — Oracle Solaris operating system iv. — Oracle WebLogic application server ***Evaluation:*** Each point will be scored according to the following criteria: 0 = None selected 10 = 4 Technologies selected 15 = 6 or more Technologies selected 20 = 8 or more Technologies selected **Note 1:** SITA reserves the right to verify the information provided. **Note 2**: Selecting Yes, implies that the Bidder indicates that it is fully competent, well skilled and suitably experienced in utilising each of the selected technologies to deliver the solution.	25%
3.	**Achievement of Business Objectives** Proposed solution's ability to support the business objectives in relation to the following core items: (a) Provide a Register structure for Applicant / Stakeholder / firearm	Y/N — The Bidder must indicate Yes (Y) or No (N) to indicate whether the Bidder's proposed solution will or will not support the business objectives as outlined below: (a) Provide a Register structure for Applicant / Stakeholder / firearm (b) Front-end/portal: enrol to submit electronic submissions	25%

No.	TECHNICAL FUNCTIONALITY REQUIREMENT	Substantiating evidence and evidence reference to be completed by bidder. Evaluation per requirement: Each question indicated in the tables below must be completed and will be scored. In column marked Y/N: Mark as Y for "comply" and N for "not-comply", if not marked Y/N it is regarded as N In column marked Evidence: Provide evidence Point will be scored according to relevant evaluation criteria specified for each question per 'Y/N'.	Weight
	(b) Front-end/portal: enrol to submit electronic submissions (c) System Security: Portal, 2 Factor Access (biometric access for internal users) (d) Interface with biometric identification (including the scanning of fingerprints) (e) Electronic submission/form licence process (f) Interface with financial system for electronic payments (g) Migration/interface with existing firearms system (h) Schedule and dairy Management (i) Administration: User Profiles, 1st face to face Registration	(c) System Security: Portal, 2 Factor Access (biometric access for internal users) (d) Interface with biometric identification (including the scanning of fingerprints) (e) Electronic submission/form licence process (f) Interface with financial system for electronic payments (g) Migration/interface with existing firearms system (h) Schedule and dairy Management (i) Administration: User Profiles, 1st face to face Registration	
		a. Comply with all 9 specified core objectives listed above in full.	
		b. Comply with at least 8 specified core objectives listed above.	
		c. Comply with at least 7 specified core objectives above.	
		d. Comply with less than 7 specified core objectives above, or did not respond.	
		Evaluation: Each point will be scored according to the following criteria: 25 = a 20 = b 15 = c 0 = d	
4.	**Solution implementation must be POPIA and ISO27001 compliant** The bidders are required to implement the full scope of the solution in the shortest period of time and duration depicted in this specification. Refer to section 1.1. above and must be POPIA and ISO27001compliant	Y/N: The Bidder must indicate Yes (Y) or No (N) to indicate the applicable duration for the implementation of the full scope of the specified solution.	25%
		a. Implement the full scope of the solution in more than 24 months after the court order constraints. **Refer to sec 3.6 above.**	

No.	TECHNICAL FUNCTIONALITY REQUIREMENT	Substantiating evidence and evidence reference to be completed by bidder. Evaluation per requirement: Each question indicated in the tables below must be completed and will be scored. In column marked Y/N: Mark as Y for "comply" and N for "not-comply", if not marked Y/N it is regarded as N In column marked Evidence: Provide evidence Point will be scored according to relevant evaluation criteria specified for each question per 'Y/N'.	Weight
		b. Implement the full scope of the solution within 24 months after the court order constraints. **Refer to sec 3.6 above.** c. Implement the full scope of the solution within 12 months after the court order constraints. **Refer to sec 3.6 above.** d. Implement the full scope of the solution within the court order constraints. **Refer to sec 3.6 above.** ***Evaluation:*** Each point will be scored according to the following criteria: (a) 5 = a (b) 10 = b (c) 15 = c (d) 20 = d	

7.3. SOLUTION DUE DILIGENCE

7.3.1. INSTRUCTION AND EVALUATION CRITERIA

(1) Only those bids that successfully passed all of the previous evaluation stages will progress to this evaluation stage, namely SOLUTION DUE DILIGENCE (Stage 2C).

(2) The bidder will be required to perform a due diligence, in conjunction with SITA, regarding their proposed solution as per Stage 2 to verify that the Bidder can supply a solution to support the business objectives in relation to the required technology infrastructure, the required functional components as well as express their understanding and technical capabilities and acknowledge the timeline of this project.

(a) A logical high-level architecture diagram which depicts the design intent, the objectives including the technology and functional components, an indication of the migration approach, security and electronic forms capability.

(b) Provide a catalogue that describes the architecture components and relationships.

(c) Provide a summarised Project Schedule that depicts the key milestones that reflects the various releases in context of the time constraints within the specification. The schedule must align to the project phases.

(d) Provide a proposed governance structure and summary roles and responsibilities required to govern and execute the project up to a successful conclusion.

(3) **Weighting of requirements**: The score for the SOLUTION DUE DILIGENCE evaluation will be calculated as follows:

(a) Each Bidder will be evaluated on each individual requirement as indicated in the tables in section 7.3.2 below.

(4) **Minimum threshold**. These individual scores will be converted to a cumulative percentage and only those bidders that have met or exceeded the minimum threshold of **70%** (cumulative) out of a total of **100%** for the SOLUTION DUE DILIGENCE Evaluation will proceed to the **next evaluation stage**.

(5) SITA will inform the bidders about the logistical arrangements regarding DUE DILIGENCE EVALUATIONS. Bidders must be prepared to PERFORM THE DUE DILIDGENCE either at the premises of SITA (in Pretoria), or at their own premises.

(6) **Note: The Yes/No Answers for the questionnaire below must be attached to Annex B, section 11.4.**

(7) Scoring as per the table below

No.	Due Diligence Requirements	Weighting
1.	High Level Architecture Diagram and a migration approach	50%
2.	Project governance and execution	50%
	TOTAL	**100%**

7.3.2. DUE DILIGENCE REQUIREMENTS

No.	DUE DILIGENCE REQUIREMENT	Substantiating evidence and reference to be completed by bidder. Evaluation per requirement: Each question indicated in the tables below must be completed and will be scored. In column marked Y/N: Mark as Y for "comply" and N for "not-comply", if not marked Y/N it is regarded as N In column marked Evidence: Provide evidence Point will be scored according to relevant evaluation criteria specified for each question per 'Y/N'.			Weight
1.	**High Level Architecture Diagram and a migration approach:** Verify the Bidder can supply a solution to support the business objectives in relation to the required technology infrastructure, the required functional components, express their understanding, technical capabilities and acknowledge the timeline of this project.		Y/N	**Evidence** Provide a high-level logical architecture diagram and supporting catalogue that describes the components and relationships between the architectural components that depicts the design intent, the business objectives, including the technology, functional components and required capabilities (e.g. security, electronic forms, etc.) **Note:** The attached **(Annex B section 11.2)** Bidder architecture and catalogue must be utilised for this purpose. **Note:** The logical solution architecture must clearly indicate whether a fully COTS solution, a fully Bespoke solution or a hybrid COTS/Bespoke solution is proposed. The COTS components and the bespoke components must be clearly identifiable.	50%
		a.		Architecture diagram of the Solution is provided with a supporting catalogue	
		b.		The architecture diagram depicts the various releases with a supporting catalogue.	
		c.		The architecture diagram depicts the various releases with a supporting catalogue. The integration requirements are clearly reflected on the architecture diagram and reflected in the catalogue. The migration approach is described. The COTS/Bespoke attributes, on the architecture is identifiable and fully described on the supporting catalogue.	
		d.		The architecture diagram depicts the various releases with a supporting catalogue. The integration requirements are clearly reflected on the architecture diagram and reflected in the catalogue. The migration approach is described. The architecture components clearly reconcile with the milestones of the project schedule, i.e. the terminology and deliverables are the same. The COTS/Bespoke attributes, on the architecture is identifiable and fully described on the supporting catalogue. The architecture solution must have less dependency on third-party plugins and licenses that creates dependency and bottleneck to only procure from a specific service provider.	
		e.		The architecture diagram depicts the various releases with a supporting catalogue.	

No.	DUE DILIGENCE REQUIREMENT	Substantiating evidence and reference to be completed by bidder. Evaluation per requirement: Each question indicated in the tables below must be completed and will be scored. In column marked Y/N: Mark as Y for "comply" and N for "not-comply", if not marked Y/N it is regarded as N In column marked Evidence: Provide evidence Point will be scored according to relevant evaluation criteria specified for each question per 'Y/N'.			Weight
				The integration requirements are clearly reflected on the architecture diagram and reflected in the catalogue. The migration approach is described. The architecture components clearly reconcile with the milestones of the project schedule, i.e. the terminology and deliverables are the same. The technology stack description is included as part of the high-level architecture diagram. The COTS/Bespoke attributes, on the architecture is identifiable and fully described on the supporting catalogue. The architecture shall be TOGAF compliant and the approved design shall be implemented by a Certified TOGAF Architect with 10 years TOGAF experience. The certified IT Security architect will certify the security architecture to enable a certified Ethical Hacker/CISP/CISA/COMPTIA with a minimum of 10 years' experience. The solution architecture demonstrates the Disaster Recovery approach and solution.	
		Evaluation: Each point will be scored according to the following criteria: 5 = A 10 = B 20 = C 35 = D 50 = E			
2.	**Project governance and execution:** Verify that the Bidder can supply the required solution which fully addresses this SAPS FCS requirement/business objectives in relation to the required technology infrastructure, the required functional components as well as express their understanding, has the technical capabilities and acknowledge the timeline of this project.		Y/N	**<u>Evidence</u>** Provide the project governance structure and high-level project schedule that reconcile to the timelines and scope of this tender specification. The project schedule clearly states the milestones to deliver the architectural perspective. **Note (1):** Attach the Project Governance structure and Project schedule to Annex B, section 11.4. **Note (2):** The Bidder must use the Project milestones, outlined in Par 8.2(4), as the project schedule WBS as the basis of the proposed schedule. **Note (3):** The implementation methodology reflects whether a fully COTS solution, a fully Bespoke solution or a hybrid COTS/Bespoke solution is proposed and reflects the approach and key activities to implement the full scope of the specification.	50%

No.	DUE DILIGENCE REQUIREMENT	Substantiating evidence and reference to be completed by bidder. Evaluation per requirement: Each question indicated in the tables below must be completed and will be scored. In column marked Y/N: Mark as Y for "comply" and N for "not-comply", if not marked Y/N it is regarded as N In column marked Evidence: Provide evidence Point will be scored according to relevant evaluation criteria specified for each question per 'Y/N'.			Weight
	The Bidder demonstrates its ability to establish the required project governance structure to execute the project. The Bidder demonstrates the implementation methodology that fully realises the scope of this specification.	a.		Project schedule and project governance structure are provided.	
		b.		Project schedule and project governance structure are provided. The project schedule clearly reflects the releases with supporting estimation, reconciling to the tender specification.	
		c.		Project schedule and project governance structure are provided. The project schedule clearly reflects the releases with supporting estimation, reconciling to the tender specification. The project reflects the required deliverables as stated in this tender specification. The implementation methodology is clearly identifiable and describes the full scope of this specification. The Project Manager must be PMP or Prince2 certified or certified in a recognised Agile methodology with 10 years or more experience in large project delivery. The Developers must be certified and have 10 years or more experience.	
		d.		Project schedule and project governance structure are provided. The project schedule clearly reflects the releases with supporting estimation, reconciling to the tender specification. The project reflects the required deliverables as stated in this tender specification. The project schedule reflects the contractual requirements in terms of the specified time constraints to comply with the court order. **Refer to Sec 8 regarding the time constraints.** The implementation methodology is clearly identifiable and describes the full scope of this specification.	
		e.		Project schedule and project governance structure are provided. The project schedule clearly reflects the releases with supporting estimation, reconciling to the tender specification. The project reflects the required deliverables as stated in this tender specification. The project schedule reflects the delivery of the requirements in terms of the specified time constraints no later than 6 months prior to the required end date of the product. **Refer to Sec 8 regarding the time constraints.**	

No.	DUE DILIGENCE REQUIREMENT	Substantiating evidence and reference to be completed by bidder. Evaluation per requirement: Each question indicated in the tables below must be completed and will be scored. In column marked Y/N: Mark as Y for "comply" and N for "not-comply", if not marked Y/N it is regarded as N In column marked Evidence: Provide evidence Point will be scored according to relevant evaluation criteria specified for each question per 'Y/N'.			Weight
				The implementation methodology is clearly identifiable and describes the full scope of this specification. The bidder must demonstrate how the solution will be implemented locally with clear modules and milestones aligned to the project phases.	
		Evaluation: Each point will be scored according to the following criteria: 5 = A 10 = B 20 = C 35 = D 50 = E			

ANNEX A.3: SPECIAL CONDITIONS OF CONTRACT (SCC)

8. SPECIAL CONDITIONS OF CONTRACT

8.1. INSTRUCTION

(1) The successful supplier will be bound by Government Procurement: General Conditions of Contract (GCC), as well as this Special Conditions of Contract (SCC), which will form part of the signed contract with the successful Supplier. However, SITA reserves the right to include or waive the condition in the signed contract.

(2) SITA reserves the right to

(i) Negotiate the conditions; or/and
(ii) Automatically disqualify a bidder for not accepting these conditions.

(3) In the event that the bidder qualifies the proposal with own conditions, and does not specifically withdraw such own conditions when called upon to do so, SITA will invoke the rights reserved in accordance with subsection 8.1(2) above.

(4) The bidder must complete the declaration of acceptance, as per section 8.3 below by marking with an "X" either "ACCEPT ALL" or "DO NOT ACCEPT ALL", failing which the declaration will be regarded, as "DO NOT ACCEPT ALL" and the bid will be disqualified.

(5) The bidder must provide the necessary software and equipment for their resources to develop, test and deploy the required products.

8.2. SPECIAL CONDITIONS OF CONTRACT

(1) **CONTRACTING CONDITIONS**

(a) **Formal Contract.** The Supplier must enter into a formal written Contract (Agreement) with SITA.
(b) **Right of Award.** SITA reserves the right to award the contract for required goods or services to multiple Suppliers.
(c) **Right to Audit.** SITA reserves the right, before entering into a contract, to conduct or commission an external service provider to conduct a financial audit or probity to ascertain whether a qualifying bidder has the financial wherewithal or technical capability to provide the goods and services as required by this tender.
(d) **DELIVERY ADDRESS.** The supplier must deliver the required products or services at as indicated in Section 2.4, Delivery Address.

(2) **PERFORMANCE MEASUREMENT**

Refer to par 3.7 for detail.

(3) **PREREQUISITES**

(a) The bidder is required to correctly interpret and apply the FCA for this solution.
(b) The bidder must comply with any required FCA amendments made during the development of the solution/project.
(c) Upon request, the bidder must provide resources CVs to demonstrate that they have a **minimum of ten (10) years' experience in all the roles of the project to deliver the solution in context of the development technology and business environment.**
(d) The business language is English and artefacts are documented using Microsoft Word, Excel, PowerPoint and Visio.
(e) Portable document format (.pdf) can be used as a final product to obtain signatures, but the editable version of the document must accompany the .pdf.
(f) All artefacts must be stored in the shared project repository.
(g) The bidder's resources are English proficient.

(h) The bidder's developers are proficient in the technologies specified in section 2 as well as the technologies added for the solution.
(i) The bidder's resources will be required to participate and function in a team environment which may include remote working environments.
(j) The bidder's resources are required to demonstrate progress on a regular basis.
(k) The bidder's resources must be able to do proper unit level technical testing for all technical conditions.
(l) The bidder's resources must be able to interpret high level designs and user stories/user requirements.

(4) **MILESTONES PER RELEASE**

(a) The work in the table below must be completed in the specified period.

Table 6: Milestones per Release

WBS	Milestones
1.	FCS Phase 1 (Release 1) - Baseline
1.1	Validate Requirements
1.2	New FCS Design
1.3	Solution Architecture
1.4	Data Architecture
1.5	Data Migration
1.6	Security Architecture
1.7	Develop ICDs
1.8	Develop IDDs
1.9	Develop FDSs
1.10	Develop TDSs
1.11	Develop Test Plan
1.12	Development of FCS Functional Baseline:
1.13	Data migration FCS/EFRS components & management
1.14	Register Applicant or Stakeholder (Front-end - enrol for electronic submissions)
1.15	System Security: Portal, 2FA (including biometric for internal users, if applicable), User Profiles, 1st face to face registration
1.16	Capture biometric identification including the scanning of fingerprints
1.17	User Interface (Front end)
1.18	Schedule management
1.19	Sign-off locally based supported solution
1.20	Develop electronic submission form / form capability
1.21	Replace interim eSubmission process for DMG and Official Institution
1.22	Competencies
1.23	System Security
1.24	User Interfaces, User Roles and Profiles
1.25	License printing
1.26	BI Reports, Queries and Dashboard
1.27	Administration Support – Scanning and Indexing of related documents / information
1.28	Integration (External via SiBus)
1.29	SPVS: ID Verification – integration to DHA
1.30	2FA

1.31	HANIS (Deceased) – DHA
1.32	Competency Verification - Accredited Association
1.33	Licence Printing - via IJS hub
1.34	Integration (Internal via SiBus)
1.35	Data migration from EFRS to new FCS
1.36	CRIM to verify applicant's criminal record
1.37	ICDMS/CAS to update firearm status lost/stolen/found
1.38	Profiling to verify and confirm applicant's information
1.39	Circulation (CIR) to verify person status
1.40	NPIS retrieval of images
1.41	POLFIN electronic payment
1.42	PERSAL retrieval of user information
1.43	PAS – firearm detail
1.44	Notification messages (e.g. SMS, email or other) to Applicants and/or other SAPS personnel
1.45	Application Status
1.46	Information Request
1.47	Escalations/Follow-up
1.48	Phase 1 Reports
1.49	Phase 1 Queries and Dashboard
1.50	System Support: Scanning and Indexing
1.51	System Administration: User Roles and Profiles
1.52	Comprehensive Transaction Audit Trail
1.53	User Context Sensitive Guidelines
1.54	Training Material
1.55	Test Procedures
1.56	Unit Test
1.57	Deploy to SIT (SIT Release)
1.58	SIT
1.59	UAT
1.60	Phase 1 Release
1.61	Phase 1 Monitor
1.62	Production Release
2.	FCS Phase 2 (Release 2) – Warrants
2.1	Validate Requirements
2.2	Refine/Enhance Solution Architecture
2.3	Refine/Enhance Data Architecture
2.4	Refine/Enhance Data Migration
2.5	Refine/Enhance Security Architecture
2.6	Develop ICDs
2.7	Develop IDDs
2.8	Develop FDSs
2.9	Develop TDSs
2.10	Develop Test Plans
2.11	Development of Warrants:
2.12	Enhanced/Extended Data migration from EFRS to new FCS for Stage 1 and 2

2.13	Enhance User Interfaces: Additional screens (Front-end) and develop the processes relating to business process requirements per application type
2.14	License to Possess & Additional Licence
2.15	Renewals of all application types
2.16	Accreditations (various as per FCA)
2.17	Import/Export/In-Transit/Transport Permits (x4)
2.18	Temporary Authorisation
2.19	Duplicates of all application types
2.20	Notifications (various)
2.21	Submission of Annual Reports for Accredited Institutions, Accredited Official Institutions and exempted DMGs
2.22	Enhanced Integration (Internal via SiBus)
2.23	Data migration and applicable integration from/with EFRS to new FCS
2.24	CRIM & AFIS to verify applicant's criminal record
2.25	ICDMS/CAS to update firearm status lost/stolen/found
2.26	Profiling to verify and confirm applicant's information
2.27	Circulation (CIR) to verify person status
2.28	NPIS retrieval of images
2.29	SAPS 13 Property Register (handing in of firearms)
2.30	SAPS43 Register of Exhibits
2.31	Registration
2.32	POLFIN electronic payment
2.33	PERSAL retrieval of user information
2.34	PAS – firearm information
2.35	Enhanced Integration (External via SiBus)
2.36	SPVS: ID Verification – integration to DHA
2.37	2FA
2.38	HANIS (Deceased) – DHA
2.39	Competency Verification - Accredited Association
2.40	PSIRA for registered security officials
2.41	Skills transfer to local black-owned company through 30% sub-contracting
2.42	Enhanced Notification messages (e.g. SMS, email or other) to Applicants and/or other SAPS personnel
2.43	Application Status
2.44	Information Request
2.45	Escalations/Follow-up
2.46	Phase 2 Extended Reports
2.47	Phase 2 Extended Queries and Dashboard
2.48	Enhanced Access to the System
2.49	Enhanced / Extended Data Migration from EFRS to New FCS
2.50	Enhanced/Extended Schedule Management, System Administration and Support
2.51	Enhanced/Extended Comprehensive Transaction Audit Trail
2.52	User Context Sensitive Guidelines
2.53	Training Material
2.54	Test Procedures
2.55	Unit Test

2.56	Deploy to SIT (SIT Release)
2.57	SIT
2.58	UAT
2.59	Phase 2 Release
2.60	Phase 2 Monitor
2.61	Production Release
3.	FCS Phase 3 (Release 3) - Firearms Administrative Components
3.1	Validate Requirements
3.2	Refine/Enhance Solution Architecture
3.3	Refine/Enhance Data Architecture
3.4	Refine/Enhance Data Migration
3.5	Refine/Enhance Security Architecture
3.6	Develop ICDs
3.7	Develop IDDs
3.8	Develop FDSs
3.9	Develop TDSs
3.10	Develop Test Plan
3.11	Development of Firearms Administrative Components:
3.12	Estates (including execution of estate executor appointed by High Court)
3.13	Circulations: Lost/Stolen/Found Firearms
3.14	Appeals
3.15	Surrendering
3.16	Disposal: Deactivation and Destruction
3.17	Declaration of Unfitness (including declaration of unfitness by courts)
3.18	Cancellation and Extension
3.19	Firearm Free Zones
3.20	Administrative Fines
3.21	Alteration of Firearms
3.22	Custom Built Firearms
3.23	Manufacturing of Firearms
3.24	Enhanced Notification messages (e.g. SMS, email or other) to Applicants and/or other SAPS personnel
3.25	Application Status
3.26	Information Request
3.27	Escalations/Follow-up
3.28	Phase 3 Enhanced/Extended Integrations (Internal & External where applicable)
3.29	Phase 3 Extended Reports
3.30	Phase 3 Extended Queries and Dashboard
3.31	Enhanced/Extended Security / Access Control
3.32	Enhanced/Extended Schedule Management, System Administration and Support
3.33	Enhanced/Extended Comprehensive Transaction Audit Trail
3.34	User Context Sensitive Guidelines
3.35	Training Material
3.36	Test Procedures
3.37	Unit Test

3.38	Deploy to SIT (SIT Release)
3.39	SIT
3.40	UAT
3.41	Phase 3 Release
3.42	Phase 3 Monitor
3.43	Production Release
4	FCS Phase 4 (Release 4) - System Administrative Components
4.1	Validate Requirements
4.2	Development of System Administrative Components:
4.3	Final Review and Confirmation of Data Migration (end to end)
4.4	Enhance / change relevant processes if required to align with amendments in FCA
4.5	Review and Finalise Audit Trail, Escalations and Reports
4.6	Review and Finalise Enhanced System Administration, User Roles and Access
4.7	Review and Confirm Support Administration, Scanning Indexes and Relationships
4.8	Finalise Manage paper documents
4.9	User Context Sensitive Help Guidelines and Documentation
4.10	User Training Material & Change Management
4.11	Final Review and Confirmation of Refined / Enhanced Queries and Dashboard per Phase
4.12	Final Review and Confirmation of Refined / Enhanced Reports per Phase
4.13	Solution Performance Monitoring & Final Report
4.14	Final Test Procedure
4.15	Unit Test
4.16	Deploy to SIT (SIT Release)
4.17	SIT
4.18	UAT, security testing and IT audit on the solution by a certified expert
4.19	Phase 4 Release
4.20	Phase 4 Monitor
4.21	**Final Production Release**
4.22	Production Monitor and Post Mortem Report
4.23	Hand over

(5) **PAYMENT SCHEDULE REQUIREMENT**

(a) **Do not pay for licence that is not deployed in production;**

(b) **Payments only due when the deliverable was signed by the Client / SAPS.**

(6) **SUPPLIER PERFORMANCE REPORTING**

(a) The supplier will be managed through a project governance structure under leadership of SITA and will be required to attend meetings as and when determined by SITA.

(b) The Supplier will report on a weekly basis to SITA/Client during the design, installation and implementation phase of the project; weekly written reports are to be presented to the SITA/Client on the progress of the preceding week until installation process has been completed.

(c) The Supplier will be required to immediately escalate any risks or issues to through the appropriate channels

(d) Quarterly meetings to be scheduled between SITA/Client and service provider as well as *ad-hoc* meetings scheduled by both parties.

(e) The Supplier is required to generate regular reports as outputs during the maintenance and support cycle within the following service levels (the report type will drive the service level agreement; definition of the content of each report type will be finalised at the time of concluding the contracted service level agreement).

(7) **CERTIFICATION, EXPERTISE AND QUALIFICATION**

(a) The Supplier represents that

(i) it has the necessary expertise, skills, qualifications and ability to competently undertake the work required in terms of the Statement of Work or Service Definition;

(ii) it is committed to provide the Products or Services in full; and

(iii) perform all obligations detailed herein without any interruption to the Customer.

(b) The Supplier must provide the service in a good and workmanlike manner and, in accordance with the practices and high professional standards used in well-managed operations.

(c) The Supplier must perform the services in the most cost-effective manner consistent with the level of quality and performance as defined in Statement of Work or Service Definition; and

(d) The Supplier must confirm that their resource/s have knowledge of the technology that will be approved as part of the Solution Architecture deliverable.

(8) **LOGISTICAL CONDITIONS**

(a) **Hours of work** - 08h00 to 16h30 (**or** as required by the project).

In the event that SITA grants the Supplier permission to access SITA's or SAPS' Environment including hardware, software, internet facilities, data, telecommunication facilities and/or network facilities remotely, the Supplier must adhere to SITA's or SAPS' relevant policies and procedures (which policy and procedures are available to the Supplier on request) or in the absence of such policy and procedures, in terms of, best industry practice.

(b) **Tools of Trade**. The Supplier personnel must provide and utilise their own required tools of trade in order for them to perform their duties adequately. These tools must be all encompassing and include all valid software license requirements.

(c) **Configuration and access to SAPS environment.** The bidder is required to ensure that the network/operating system configuration are applied in compliance with the SAPS security governances.

(d) **On-site** and/or Remote Services - the Supplier must deliver the service on-site at either the SAPS or SITA – decision will form part of the contract negotiations. Services might be able to be rendered remotely; which decision will be finalised during contracting after award.

(9) **SKILLS TRANSFER AND TRAINING**

(a) The Service Provider must provide training on the proposed solution or product to technical staff to enable SITA to operate and support the product or solution after implementation.

(b) The Service Provider must provide training to trainers on the proposed solution or product for further training, by SAPS, to their end-users.

(c) The number of trainers to be trained for all the releases are: 100 (10 per province plus 10 at National level)

(d) The basic and advanced training to be done for SITA technical team.

(e) The training will be conducted on a "train the trainer" basis.

(f) The Service Provider must assist SITA to develop the required end-user training material.

(10) **POST-GO-LIVE SUPPORT DURATION**

(a) Each release requires post-go-live support.

(b) The post-go-live duration for each release is specified within this tender specification.

(11) **APPLICATION MAINTENANCE AND FUNCTIONAL APPLICATION SUPPORT DURATION**

(a) Each release requires HANDOVER FROM THE Service Provider to SITA Application Maintenance and SITA Functional Application Support; during which period, the maintenance and support responsibilities will transfer for the Service Provider to SITA.

(b) The handover duration is depicted within this tender specification.

(12) **REGULATORY, QUALITY AND STANDARDS**

(a) The Supplier must for the duration of the contract ensure that the proposed product or solution conform with the Government Minimum Interoperability Standards (MIOS 6).

(b) Quality Standards.

(c) Microservices/SOA based architecture that enable interoperable solutions.

(d) Project Management Methodology.

(e) Agile Development Methodology.

(f) The Supplier must for the duration of the contract ensure compliance with ISO/IEC General Quality Standards, ISO27001, and Protection of Personal Information Act (POPIA).

(g) The Supplier must for the duration of the contract ensure compliance with General Quality Standards, ISO 9001.

(h) **The solution implementation needs to be POPIA and ISO27001 (IT Security Certified)**.

(13) **PERSONNEL SECURITY CLEARANCE**

(a) The Supplier personnel who are required to work with information related to NATIONAL SECURITY must have a **valid South African security clearance**, or must apply within 30 days of the signed contract for a security clearance to the level of CONFIDENTIAL at the expense of the Supplier from the South African State Security Agency, or duly authorised Personnel Security Vetting entity of SA Government.

(b) The Supplier personnel who are required to work with GOVERNMENT CLASSIFIED information or access government RESTRICTED areas must be a South African Citizen and at the expense of the Supplier be security vetted (pre-employment screening, criminal record screening and credit screening).

(c) The Supplier must ensure that the security clearances of all personnel involved in the Contract remains valid for the period of the contract.

(14) **CONFIDENTIALITY AND NON-DISCLOSURE CONDITIONS**

(a) The Supplier, including its management and staff, must before commencement of the Contract, sign a Non-Disclosure Agreement (NDA) regarding Confidential Information.

(b) Confidential Information means any information or data, irrespective of the form or medium in which it may be stored, which is not in the public domain and which becomes available or accessible to a Party as a consequence of this Contract, including information or data which is prohibited from disclosure by virtue of:

(i) the Promotion of Access to Information Act, 2000 (Act no. 2 of 2000);

(ii) being clearly marked "Confidential" and which is provided by one Party to another Party in terms of this Contract;

(iii) being information or data, which one Party provides to another Party or to which a Party has access because of Services provided in terms of this Contract, and in which a Party would have a reasonable expectation of confidentiality;

(iv) being information provided by one Party to another Party in the course of contractual or other negotiations, which could reasonably be expected to prejudice the right of the non-disclosing Party;

(v) being information, the disclosure of which could reasonably be expected to endanger a life or physical security of a person;

(vi) being technical, scientific, commercial, financial and market-related information, know-how and trade secrets of a Party;

(vii) being financial, commercial, scientific or technical information, other than trade secrets, of a Party, the disclosure of which would be likely to cause harm to the commercial or financial interests of a non-disclosing Party; and

(viii) being information supplied by a Party in confidence, the disclosure of which could reasonably be expected either to put the Party at a disadvantage in contractual or other negotiations or to prejudice the Party in commercial competition; or

(ix) information the disclosure of which would be likely to prejudice or impair the safety and security of a building, structure or System, including, but not limited to, a computer or communication System; a means of transport; or any other property; or a person; methods, Systems, plans or procedures for the protection of an individual in accordance with a witness protection scheme; the safety of the public or any part of the public; or the security of property; information the disclosure of which could reasonably be expected to cause prejudice to the defence of the Republic; security of the Republic; or international relations of the Republic; or plans, designs, drawings, functional and technical requirements and specifications of a Party, but must not include information which has been made automatically available, in terms of the Promotion of Access to Information Act, 2000; and information which a Party has a statutory or common law duty to disclose or in respect of which there is no reasonable expectation of privacy or confidentiality;

(c) Notwithstanding the provisions of this Contract, no Party is entitled to disclose Confidential Information, except where required to do so in terms of a law, without the prior written consent of any other Party having an interest in the disclosure;

(d) Where a Party discloses Confidential Information which materially damages or could materially damage another Party, the disclosing Party must submit all facts related to the disclosure in writing to the other Party, who must submit information related to such actual or potential material damage to be resolved as a dispute;

(e) Parties may not, except to the extent that a Party is legally required to make a public statement, make any public statement or issue a press release which could affect another Party, without first submitting a written copy of the proposed public statement or press release to the other Party and obtaining the other Party's prior written approval for such public statement or press release, which consent must not unreasonably be withheld.

(15) **GUARANTEE AND WARRANTIES**

The Supplier warrants that:

(a) The warranty of goods supplied under this contract remains valid for twelve (12) months after the goods, or any portion thereof as the case may be, have been delivered to and accepted at the final destination indicated in the contract, or for eighteen (18) months after the date of shipment from the port or place of loading in the source country, whichever period concludes earlier;

(b) as at Commencement Date, it has the rights, title and interest in and to the Product or Services to deliver such Product or Services in terms of the Contract and that such rights are free from any encumbrances whatsoever;

(c) the Product is in good working order, free from Defects in material and workmanship, and substantially conforms to the Specifications, for the duration of the Warranty period;

(d) during the Warranty period any defective item or part component of the Product be repaired or replaced within 3 (three) days after receiving a written notice from SITA;

(e) the Products is maintained during its Warranty Period at no expense to SITA;

(f) the Product possesses all material functions and features required for SITA's Operational Requirements;

(g) the Product remains connected or Service is continued during the term of the Contract;

(h) all third-party warranties that the Supplier receives in connection with the Products including the corresponding software and the benefits of all such warranties are ceded to SITA without reducing or limiting the Supplier's obligations under the Contract;

(i) no actions, suits, or proceedings, pending or threatened against it or any of its third-party suppliers or sub-contractors that have a material adverse effect on the Supplier's ability to fulfil its obligations under the Contract exist;

(j) SITA is notified immediately if it becomes aware of any action, suit, or proceeding, pending or threatened to have a material adverse effect on the Supplier's ability to fulfil the obligations under the Contract;

(k) any Product sold to SITA after the Commencement Date of the Contract remains free from any lien, pledge, encumbrance or security interest;

(l) SITA's use of the Product and Manuals supplied in connection with the Contract does not infringe any Intellectual Property Rights of any third party;

(m) the information disclosed to SITA does not contain any trade secrets of any third party, unless disclosure is permitted by such third party;

(n) it is financially capable of fulfilling all requirements of the Contract and that the Supplier is a validly organized entity that has the authority to enter into the Contract;

(o) it is not prohibited by any loan, contract, financing arrangement, trade covenant, or similar restriction from entering into the Contract;

(p) the prices, charges and fees to SITA as contained in the Contract are at least as favourable as those offered by the Supplier to any of its other customers that are of the same or similar standing and situation as SITA; and

(q) any misrepresentation by the Supplier amounts to a breach of Contract.

(r) **The bidder shall provide unconditional performance guarantee for the full value of the contract from reputable financial institution for the duration of the contract.**

(16) **INTELLECTUAL PROPERTY RIGHTS**

(a) SITA retains all Intellectual Property Rights in and to SITA's Intellectual Property. As of the Effective Date, the Supplier is granted a non-exclusive license, for the continued duration of this Contract, to perform any lawful act, including the right to use, copy, maintain, modify, enhance and create derivative works of SITA's Intellectual Property for the sole purpose of providing the Products or Services to SITA pursuant to this Contract; provided that the Supplier must not be permitted to use SITA's Intellectual Property for the benefit of any entities other than SITA without the written consent of SITA, which consent may be withheld in SITA's sole and absolute discretion. Except as

otherwise requested or approved by SITA, which approval is in SITA's sole and absolute discretion, the Supplier must cease all use of SITA's Intellectual Property, at of the earliest of:

(i) termination or expiration date of this Contract;

(ii) the date of completion of the Services; and

(iii) the date of rendering of the last of the Deliverables.

(b) If so required by SITA, the Supplier must certify, in writing to SITA, that it has either returned all SITA Intellectual Property to SITA or destroyed or deleted all other SITA Intellectual Property in its possession or under its control.

(c) SITA, at all times, owns all Intellectual Property Rights in and to all Bespoke Intellectual Property.

(d) Provide SITA with the compliant safety file.

(17) **SOFTWARE LICENSING**

(a) All software that must be procured and licenced must be included separately in the pricing section of this RFB and will be used as part of the evaluation of the response. However, the procurement of software will be handled, as a separate procurement process once the technology stack has been confirmed and approved, as part of the Solution Architecture process.

(b) The Bidder who proposes a fully COTS solution, or a hybrid COTS/Bespoke solution hereby warrants that it has full right to transfer the ownership of the COTS/hybrid solution. The bidder shall transfer the ownership of the COTS/hybrid solution to SITA at no extra cost. The bidder also warrant that the COTS/hybrid solution is free from any encumbrances presently or in future.

(c) Locally developed solution is preferred.

(18) **GENERAL**

(a) The supplier will be bound by Government Procurement: General Conditions of Contract.

(b) (GCC) as well as this Special Conditions of Contract (SCC), which will form part of the signed contract with the Supplier. However, SITA reserves the right to include or waive the condition in the signed contract.

(c) SITA reserves the right to:

(i) Negotiate the conditions, or

(ii) Automatically disqualify a bidder for not accepting these conditions.

(iii) Right to Audit: SITA reserves the right, before entering into a contract, to conduct or commission an external service provider to conduct probity to ascertain whether a qualifying bidder has the technical capability to provide the goods and services as required by this tender.

(d) "The parties in this Agreement agree that the offer price of all the equipment shall be at the wholesale price or below wholesale price as agreed with the OEM. Should, at any time during the existence of the agreement that the offered price which is higher than the wholesale price or as agreed with the OEM, SITA client shall be entitled to such wholesale price with the exclusion of the mark-up which the reseller may have charged".

NOTE: These conditions will form part of the contract obligations and suppliers are expected to comply in order for SITA to conclude an agreement with the potential suppliers. Failure to comply during finalisation of a contract may result to disqualification.

(19) **COUNTER CONDITIONS**

- Bidders' attention is drawn to the fact that amendments to any of the Bid Conditions or setting of counter conditions by bidders may result in the invalidation of such bids.

(20) **FRONTING**

(a) The SITA supports the spirit of Broad Based Black Economic Empowerment and recognizes that real empowerment can only be achieved through individuals and businesses conducting themselves in accordance with the Constitution and in an honest, fair, equitable, transparent and legally compliant manner. Against this background the SITA any form of fronting.

(b) The SITA, in ensuring that bidders conduct themselves in an honest manner will, as part of the bid evaluation processes, conduct or initiate the necessary enquiries/investigations to determine the accuracy of the representation made in bid documents. Should any of the fronting indicators as contained in the Guidelines on Complex Structures and Transactions and Fronting, issued by the Department of Trade and Industry, be established during such enquiry/investigation, the onus will be on the bidder / contractor to prove that fronting does not exist.

(c) Failure to do so within a period of 14 days from date of notification may invalidate the bid / contract and may also result in the restriction of the bidder/contractor to conduct business with the public sector for a period not exceeding ten (10) years, in addition to any other remedies SITA may have against the bidder/contractor concerned.

(21) **BUSINESS CONTINUITY AND DISASTER RECOVERY PLANS**

The bidder confirms that they have written business continuity and disaster recovery plans that define the roles, responsibilities and procedures necessary to ensure that the required services under this bid specification is in place and will be maintained continuously in the event of a disruption to the bidder's operations, regardless of the cause of the disruption. Certified bidder in ISO22201 Business Continuity Management (BCM) system is preferred.

(22) **REGIONAL CAPACITY**

(a) Bidders must have the capacity to render services in all provinces of South Africa and must be prepared to render services in such regions.

(23) **COOPERATION WITH OTHER SUPPLIERS**

Bidders may be required to cooperate with other suppliers to achieve the implementation of a holistically functioning solution, in cases where products from different suppliers have to be integrated or implemented together, while remaining accountable for the quality and functioning of products or components supplied by themselves.

(24) **SPECIAL CONDITIONS OF SERVICE**

(a) The product must be delivered, in full, against the stipulated specifications, within the time and financial constraints.

(b) The agreed upon payment schedule must reconcile with the fully accepted milestone deliverables and pricing schedule.

(c) The Bidder must **confirm compliance** to the following mandatory requirements:

(i) Security.

(ii) Integration and interoperability.

(iii) Reselling the services to SITA's Customers.

(iv) Intellectual property of developed software.

(v) Project management and implementation responsibility.

(d) **System Architecture.**

(i) The FCS must be locally installed and must not have any dependency on any public cloud architecture or other form of dependency requiring a connection to any external ICT infrastructure,

(ii) All modules of the solution must be fully customisable for on-site customisation by technical resources,

(iii) Sub-components of the solution (if applicable) must be interoperable with each other in compliance with MIOS 6 where applicable,

(iv) Provide for a data capturing functionality that will ensure data is captured in data groups and not visible between users of different groups and segregation of duties where applicable,

(v) Security features to enable classification of users,

(vi) Must support a minimum of 1500 concurrent users (SAPS as well as external users). An estimated number of 3500 SAPS users and additional capacity for the public and firearms dealers to perform the online functionalities as per SAPS requirement.

(vii) Data migration will include, but not limited to, the following data entities from the existing SAPS EFRS:

SNO	ITEM	# OF RECORDS
1	Firearms	7030092
2	Individuals (natural persons)	3767183
3	Private institutions (juristic persons) e.g. dealers	2644
4	Government institutions	838
5	Ammunition	2894 types of calibres
6	Imports	160882
7	Exports	87436
8	Firearm components - calibre	2894
9	Firearm components - Makes	3687
10	Payment Information	5989885

(e) The Bidder must **comply with** the Product / Service **Functional requirements** for the Installation and functioning of the deployed solution.

(f) The Bidder must be an **authorised** Reseller, Original Equipment Manufacturer (OEM), or Original Software Manufacturer (OSM), in the Republic of South Africa, in order to participate in this tender.

(g) Any **additional component**, required for the delivery of a minimum viable product, not specified/included by the service provider on the pricing schedule, shall be provided by the service provider at no cost to SITA or SAPS.

(h) **Data Leakage.** The architecture diagram must confirm that no data will be stored or duplicated outside of the SITA Private Cloud infrastructure/SAPS platform, which includes any performance or reporting data to service provider or third-party platforms. SITA will be responsible to monitor

and manage the deployed solution and connected devices with the support/cooperation of the service provider.

(25) **TARGETED PROCUREMENT/TRANSFORMATION**

- SITA in terms of the PPPFA Regulation 2017 section 9(1), has an obligation to advance designated groups which includes black SMMEs (i.e. Exempted Micro Enterprises (EME) and Qualifying Small Enterprises (QSE)) for the supply of certain ICT goods or services where feasible to subcontract for a contract above R30m, an organ of state must apply subcontracting to advance designated groups.
- The bidder is required to subcontract a minimum of 30% of the value of the contract to EMEs, and/or QSEs which is at least 51% owned by black people, black women, youth or people with disability.

(26) **SUPPLIER DUE DILIGENCE**

- SITA reserves the right to conduct supplier due diligence prior to final award or at any time during the Contract period and this may include pre-announced/ non-announced site visits. During the due diligence process the information submitted by the bidder will be verified and any misrepresentation thereof may disqualify the bid or Contract in whole or parts thereof.

(27) **THIRD-PARTY MANAGEMENT RISK ASSESMENT**

a) The Bidder will provide all reasonable supporting documentation for the Third-Party Risk Management Assessment when requested to do so, as well as during contract finalisation as this is a **pre-award condition of this bid**.

b) Any risk identified during the assessment process will have to be mitigated and/or remediated before or during the contract finalisation phase. A detailed mitigation plan, that is acceptable to SITA, may also be required.

c) Supplier due diligence, as contained in the Special Conditions of Contract, is also applicable to this Third-Party Risk Management process.

8.3. DECLARATION OF ACCEPTANCE

No.		ACCEPT ALL	DO NOT ACCEPT ALL
1.	1.1 The bidder declares to ACCEPT ALL the Special Condition of Contract as specified in section 8.2 above by indicating with an "X" in the "ACCEPT ALL" column.		
2.	**Note:** **Failure not to Accept all the Special Conditions of Contract will result in disqualification.**		

ANNEX A.4: COSTING AND PRICING

9. COSTING AND PRICING

9.1. COSTING AND PRICING EVALUATION

(1) In terms of Preferential Procurement Policy Framework Act (PPPFA), the following preference point system is applicable to all Bids:

(a) the 80/20 system (80 Price, 20 B-BBEE) for requirements with a Rand value of up to R50 000 000 (all applicable taxes included); or

(b) the 90/10 system (90 Price and 10 B-BBEE) for requirements with a Rand value above R50 000 000 (all applicable taxes included).

(2) This bid will be evaluated using the preferential point system of **90/10**, subject to the following conditions –

(a) If the lowest acceptable bid price is up to and including R50 000 000 (all applicable taxes included) then the 80/20 preferential point system will apply to all acceptable bids; or

(b) If the lowest acceptable bid price is above R50 000 000 (all applicable taxes included) then the 90/10 preferential point system will apply to all acceptable bids;

(3) The bidder must **complete the declaration of acceptance** as per section 9.3 below by marking with an "X" either "ACCEPT ALL", or "DO NOT ACCEPT ALL", failing which the declaration will be regarded as "DO NOT ACCEPT ALL" and the bid will be disqualified.

(4) Bidder will be bound by the following general costing and pricing conditions and SITA reserves the right to negotiate the conditions or automatically disqualify the bidder for not accepting these conditions. These conditions will form part of the Contract between SITA and the bidder. However, SITA reserves the right to include or waive the condition in the Contract.

9.2. COSTING AND PRICING CONDITIONS

1. **SOUTH AFRICAN PRICING**

The total price must be VAT inclusive and be quoted in South African Rand (ZAR).

2. **TOTAL PRICE**

(a) All quoted prices are the total price for the entire scope of required services and deliverables to be provided by the bidder.

(b) The cost of delivery, labour, S&T, overtime, etc. must be included in this bid.

(c) All additional costs must be clearly specified.

(d) Provide the TOTAL BID PRICE as well as the TOTAL EFFORT in hours to complete the work for the duration of Contract.

SITA reserves the right to negotiate pricing with the successful bidder prior to the award as well as envisaged quantities.

3. **RATE OF EXCHANGE PRICING INFORMATION**

Provide the TOTAL BID PRICE for the duration of Contract and clearly indicate the Local Price and Foreign Price, where –

(a) **Local Price** means the portion of the TOTAL price that is NOT dependent on the Foreign Rate of Exchange (ROE) and;

(b) **Foreign Price** means the portion of the TOTAL price that is dependent on the Foreign Rate of Exchange (ROE).

(c) **Exchange Rate** means the ROE (ZA Rand vs foreign currency) as determined at time of bid.

4. **BID EXCHANGE RATE CONDITIONS**

The bidders must use the exchange rate provided below to enable SITA to compare the prices provided by using the same exchange rate:

Foreign currency	South African Rand (ZAR) exchange rate
1 US Dollar	R16,78
1 Euro	R16,83
1 Pound	R19,71

5. **BID PRICING SCHEDULE**

Note: Bidders must complete the bid pricing schedule in the accompanying Excel spreadsheet format provided and include this as part of their submission.

There are three price response sheets:

(a) **Fully BESPOKE solution** – Complete ONLY this sheet if a fully BESPOKE solution is proposed.

(b) **Fully COTS solution** – Complete ONLY this sheet if a fully COTS solution is proposed.

(c) **Hybrid COTS/BESPOKE solution** – Complete ONLY this sheet if a HYBRID solution is proposed with both COTS and BESPOKE components.

Note:

(a) Bidder must complete/enter YELLOW cells only on the applicable price response sheet.

(b) Unit and Line prices must be VAT EXCLUSIVE and in South African Rand (ZAR) currency.

(c) The price must include all costs to deliver the goods or render the service, including all applicable taxes, duty fees, logistics/delivery, storage, labour, overtime and subsistence and travel.

(d) Prices that are dependent on Rate of Exchange (ROE) must use ROE indicated above, then enter in the applicable price response sheet Column "Forex %" the percentage of the price that is ROE dependent (0% means the price is not ROE dependent).

(e) Refer to the bid specification for the full requirement and time constraint to determine the effort and costing.

(f) The applicable price response sheet must be completed in conjunction with this Bid Specification document.

(g) The Bidder must refer to the Scope of Work (SoW), Technology Stack and time constraints in this Bid Specification to determine the effort and cost associated with a solution of this complexity.

(h) The applicable price response sheet must reflect the COTS and/or BESPOKE Bidder implementation methodology that includes any and all possible customisation.

9.3. DECLARATION OF ACCEPTANCE

No.		ACCEPT ALL	DO NOT ACCEPT ALL
1.	1.1 The bidder declares to ACCEPT ALL the Costing and Pricing conditions, as specified in section 9.2 above by indicating with an "X" in the "ACCEPT ALL" column, OR 1.2 The bidder declares to NOT ACCEPT ALL the Costing and Pricing Conditions as specified in section 9.2 above by (a) Indicating with an "X" in the "DO NOT ACCEPT ALL" column; and (b) Provide reason and proposal for each of the condition not accepted.		
2	**Comments by bidder:** Provide the condition reference, the reasons for not accepting the condition.		

ANNEX A.5: TERMS AND DEFINITIONS

10. TERMS AND CONDITIONS

10.1 DEFINITIONS

Terms and Definitions

No.	Term	Definition
1.	2FA	Two Factor Authentication assists to prevent fraudulent access.
2.	Authentication	A person's identity must be authenticated each time they access a System or resource. The user is asked to re-validate that they are the same person who registered for the service. Verification is usually performed once.
3.	Bidder	Any person/s constituted as, partnership, company, close corporation, or any other form of enterprise which has been invited by SITA to submit a BID.
4.	Service Provider	The awarded Bidder.
5.	Confidential Information	All technical and business information, including, without limiting the generality of the foregoing, all secret knowledge and information (including any and all financial, commercial, market, technical, functional and scientific information, and information relating to a party's strategic objectives and planning and its past, present and future research and development), technical, functional and scientific requirements and specifications, data concerning business relationships, demonstrations, processes, machinery, know-how, architectural information, information contained in a party's software and associated material and documentation, plans, designs and drawings and all material of whatever description, whether subject to or protected by copyright, patent or trademark, registered or unregistered, or otherwise disclosed or communicated.
6.	Digital Transformation initiatives	Shedding paper-laden processes in favour of digitisation and modernisation, to provide self-service options to citizens. Digital Transformations, present new opportunities for process improvement and the creation of new, innovative ways to dispense policing services to citizens. The future of SAPS IS/ICT is not just about technology, but it is also about how the SAPS uses information and technology to deliver better services in a constantly changing environment. Digitised processes (electronic forms and scanned supporting documentation if relevant), secure capability and networks and mobile devices enhance efficiency and effectiveness.
7.	DMG	A registered Dealer or Manufacturer or Gunsmith also known as a Commercial Agent.
8.	e-Government or digital government	Innovative use of communications technologies (including mobile devices), websites, applications and other ICT services and platforms to link citizens and the public sector and facilitate collaborative and efficient governance.
9.	eSubmission	A sub-system providing the capability to submit digitally signed electronic ADOBE XFA forms to SAPS which are processed in an automated process via the Adobe Experience Manager.
10.	EFRS	Electronic Enhanced Firearm Register System. This is the current firearm licencing system utilised by the SAPS.
11.	FCA	The Firearm Control Act (FCA) was promulgated in 2004 to give effect to a comprehensive, structured and effective System for the control of firearms. The Act's intent among others, is to prevent the proliferation of illegally possessed firearms, improve control over legally possessed firearms, and prevent crime

No.	Term	Definition
		involving the use of firearms, thereby contributing to the creation of a safe and secure environment for all the people of South Africa.
12.	FCS Business Processes	All the required FCS business processes are based on the FCA, as per section and must ensure the implementation of the FCA via digitised, secure and efficient processes. Business processes must be engineered to focus on end-to-end service delivery, and where relevant to integrate the new capabilities of modernised and agile technologies.
13.	Identification	Identification is the submission of person biometric data with the aim of determining if the user is enrolled in the database, and if so, finding their identity. The identification request shall contain the following minimum set of data: Biometric information; Biometric test template(s); and Biometric sample acquisition date and time.
14.	Information Sharing Capability	An ability to share information - either on a one-to-one or one-to-many or many-to-many basis. This capability to be used by humans or application systems.
15.	Managed Diary	Calendar scheduling integration to enable applicants to schedule an appointment with relevant responsible DFO on slots/openings made available.
16.	Modern Application Development	The industry definition of Modern Application Development involves incorporation of, as many of the following attributes, as applicable in a given scenario: •Cloud-Backed: Project assets stored in the cloud catalyse collaboration between stakeholders; •Human-Cantered: Focusing on the design and appearance of the application that brings the front-end designer and/or application programmer into the enterprise development process more fully than ever before; •Agile: Software is built via incremental, frequent releases; •Socially-Oriented: Integrating of user-interface patterns borrowed from social networks, such as timelines, event streams, social graphs and other social metadata; •Mobile: Supporting touch interaction and adaptability to a large range of screen sizes and pixel densities; •Lightweight: Less complex software that is less time-consuming to install, learn and use; •Analytics-Infused: Developers get rich intelligence on application usage; •DevOps-Enabled: Developers own deployment or work seamlessly with Ops staff to test, release, test, refine and rerelease applications to users; •Continuously Integrated and Delivered: Applications must be integrated to run continuously; •API Factored and Surfaced: The move to APIs involves a comprehensive movement to componentise and granularize back-end software, in order to achieve composable and easy-to-evolve back-end platforms; •App Store Delivered and Extended: The app is delivered in an app store and/or uses modules or off-the-shelf components and services; and •Model-Driven: Rich use of visual tools to support abstraction in the development toolset, such as for relations in a data model, business logic flows, and process flows.
17.	Non-repudiation	Provide proof of origin of data and the integrity of the data and the assurance in the process that someone cannot deny the validity of a transaction.

No.	Term	Definition
18.	Registered Person	A Registered Person is a person that has been provided 2FA to the New FCS per 2FA and allocated a unique CJS identity number against a number of unique measurable Person Attributes that can be tested to confirm the allocation of a unique CJS identity.
19.	Seamless information to to perform Policing related transactions	The SAPS rely on Information System Information and Communication Technology that is enabled by various technology capabilities, including infrastructure capabilities. In this regard the SAPS is embarking on a transformational journey to modernise and improve efficiency of service delivery through technology and contribute towards the achievement of the National Development Plan (NOP) and vision 2030 aspiration.
20.	Verification	Application: Verification is confirming correctness of the application/warrant details and the related supporting documents that have been submitted or presented. Person: Verify a claim of identity with the aim of authenticating that person. The verification request will contain the following minimum set of data: Biographic information; Name or Alias; Person Identification number, and documentation; Biometric information; Biometric test template(s); and Biometric sample acquisition date and time.

10.2 ABRBREVIATIONS

AFIS	Automated Fingerprint Identification System
AA	Accounting Authority
AO	Accounting Officer
API	Application Programming Interface
ASAP	As Soon As Possible
B-BBEE	Broad-Based Black Economic Empowerment
BI	Business Intelligence
BPMN	Business Process Model and Notation
BUS	Bidirectional Universal Switch
CAS	Crime Administration System
CEO	Chief Executive Officer
CFR	Central Firearms Register
CIR	Circulation System
CJP	Criminal Justice Programme
CJPBRS	Business Requirement Specification
CJS	Criminal Justice System
CP	Criminal Profile
CRC	Criminal Record Centre
CRIM	Criminal Record Systems
CSD	Circuit Switched Data
CSS	Cascading Style Sheets
CV	Curriculum Vitae
DDL	Data Definition Language
DFO	Designated Firearms Officer
DHA	Department of Home Affairs
DMG	Dealers/Manufacturers/Gunsmiths
DMZ	Demilitarized Zone
DTI	Department of Trade Industry
EFRS	Enhanced Firearms Register System
ERP	Enterprise Resource Planning
FCA	Firearms Control Act
FCS	Firearms Control Solution
FDS	Functional Design Specification
FIN	Firearm Identification Number
GCC	General Conditions Contract
HANIS	Home Affairs National Identity System
HTML	Hyper Text Mark-up Language
HTTPS	Hyper Text Transfer Protocol Secure
IBM	International Business Machines Corporation
ICD	Interface Control Document
ICDMS	Investigation Crime Docket Management System
ICT	Information and Communications Technology
ID	Identification Document
IDD	Interface Design Document
IJS	Integrated Justice System
ISO	International Standards Organisation
IT	Information Technology
JCPS	Justice, Crime Prevention and Security Cluster
JEE	Java Enterprise Edition

LC	Large Custom
LSS	Life Scan Solution
MDM	Master Data Management
MIOS	Minimum Interoperability Standards for Information Systems
MQ	Message Queuing
MRI	Master Record Index
MS	Microsoft
NCACC	National Conventional Arms Control Committee
NOP	National Development Plan
NPIS	National Photo Identification System
OSD	On Screen Display
OSM	Original Sales Manager
OTP	One Time Pin
PAS	Provisional Administration System
PDF	Portable Document Format
PERL	Practical Extraction and Report Language
PERSAL	Personnel and Salary System
PFMA	Public Finance Management Act
PID	Project Initiation Document
POLFIN	Police Financial System
PPPFA	Preferential Procurement Policy Framework Act
PSIRA	Private Security Industry Regulatory Authority
PVS	Person Verification Service
QSE	Qualifying Small Enterprise
RAD	Rational Application Developer
RFB	Request for Bid
RFQ	Request for Quotation
S&T	Subsistence and Travel
SA	Solution Architecture
SaaS	Software as a Service
SABS	South African Bureau of Standards
SAPS	South African Police Service
SARP	Standard and Recommended Practice
SATS	Standard Assessment Tests
SBD	Standard Bidding Document
SCC	Special Conditions of Contract
SCM	Supply Chain Management
SDD	Solid State Drive
SI	Service Integration
SiBus	Service Integration Bus
SIT	Service Integration Testing
SITA	State Information Technology Agency
SLA	Service Level Agreement
SMME	Small, Medium and Micro Enterprise
SMS	Short Message Service
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SPVS	SAPS Person Verification Service
SQL	Structured Query Language
TCP/IP	Transmission Control Protocol/Internet Protocol
TBD	To Be Determined

TDS	Technical Design Specification
TMS	Technology Management Services
UAT	User Acceptance Testing
VAT	Value Added Tax
VISPOL	Visible Policing
WAS	WebSphere Application Server
WBS	Work Breakdown Structure
ZAR	South African Rand
XML	Extensible Mark-up Language

ANNEX B: BIDDER SUBSTANTIATING EVIDENCE

11. MANDATORY REQUIREMENT EVIDENCE

11.1 BIDDER EXPERIENCE AND CAPABILITY REQUIREMENTS

Complete table below, noting that:

a) The bidder must have developed information system(s) comparable in size and complexity as stated in this bid specification in section 2.2, section 3.2, prescribed technology stack in section 2.5. as well as time constraints in section 3.6, for at least one (1) customer in the last five (5) years.
b) Project end-date must be current or not older than 5 years from date this bid is advertised.
c) Scope of work must be related.

No	Company name	Reference Person Name, Tel and/or email	Project Scope of work	Project Start and End-date
1	<Company name>	<Person Name> <Tel> <email>	< Provide scope details from a project for the solution design, migration and software development services was delivered in the past five (5) years>	Start Date: End Date:
2*	<Company name>	<Person Name> <Tel> <email>	< Provide scope details from a project for the solution design, migration and software development services was delivered in the past five (5) years>	Start Date: End Date:
3*	<Company name>	<Person Name> <Tel> <email>	< Provide scope details from a project for the solution design, migration and software development services was delivered in the past five (5) years>	Start Date: End Date:

*Note: Please include more rows if required.

11.2 PRODUCT OR SERVICE TECHNICAL AND FUNCTIONAL REQUIREMENTS

Requirement 1:
The bidder **must comply** with the Technical and Product Service Requirements by **completing** ANNEX C: Addendum1 and **attach it here.**

and;

Requirement 2:
The Bidder is required to provide a logical architecture that depicts the proposed solution, conforming to the functional and technical requirements as stated in this specification, with a supporting catalogue that lists and describes the architectural components and related relationships between the components and **attach it here** and complete the table below with the applicable references.

No	Product	Unique Reference to Product
1	Logical Solution Architecture	
2	Catalogue	

11.3 THIRD PARTY RISK MANAGEMENT ASSESMENT

The Bidder **must** comply to the Third-Party Risk Management Assessment requirement by completing All the questions in **ANNEX E and attach it here.**

11.4 TECHNICAL FUNCTIONALITY AND DUE DILIGENCE REQUIREMENTS

The Bidder **must attach** all the Technical Functionality and Due Diligence completed sheets (Yes/No answers) **here.**

No	Product Evidence	Unique Reference to Product Evidence
1	Technical Functionality questionnaire answers Refer to section 7.2 (1, 2, 3, 4 and 5)	
2	Due Diligence questionnaire answers Refer to section 7.3.1(2)(a) and (b)	
3	Project Schedule Refer to section 7.3.2.1	
4	Project Governance structure Refer to section 7.3.2.2	

ANNEX C: ADDENDUM 1

NB: The bidder must declare that they comply with the following Technical Mandatory Requirements as indicated below, as this will be legal contractual binding:

1) PRODUCT OR SERVICE TECHNICAL REQUIREMENTS	2) SUMMARY OF SECTIONS STATED IN THE LEFT COLUMN
The bidder **must declare** compliance to the following: a) **Full Scope of Work of the Functional Product / Service** Functional requirements for the SAPS FCS as indicated in this Specification as per section 2 of the Bid Specification, b) **Technical Requirements** as per section 3 of the Bid Specification. c) **Time Constraint** as indicated in this Specification as per section 3.6 of the Bid Specification, d) **The Approach** as indicated in this Specification as per section 2.2 of the Bid Specification, The bidder must supply a solution that meets the following specification:	(a) fully and exclusively installed, configured and operated from the SAPS's own on-site ICT environment. (b) establish integration between the solution, biometric devices, workflow scheduling, electronic forms, digitised information and digital certificates. (c) connect to and interrogate multiple secure data stores simultaneously, internal and external to the SAPS, without limitation of quantity, size and type. (d) All modules of the solution must be fully customisable for on-SAPS/SITA-site customisation by technical resources. (e) sub-components of the solution (if applicable) must be interoperable with each other in compliance MIOS 6 where applicable. (f) provide integrated security features to establish secure and interoperable processes in the solution and non-repudiation capability for external classified users (g) provide for a data capturing functionality that will ensure data is captured in data groups and not visible between users of different groups and segregation of duties where applicable. (h) must support a minimum of 2000 concurrent users. (i) Integration Technologies: • MQ • IBM-IBUS

DECLARATION

I, the bidder (Full names) …….

representing (company name) …….

Hereby confirm that I comply with the above Technical Mandatory Requirements and understand that it will form part of the contract and is legally binding.

Thus, done and signed at …….. On this……day of……20….

…….

Signature

Designation:

ANNEX D: ADDENDUM 2

NB: The bidder must declare that they comply with the following Technical Functionality Requirements as indicated below, as this will be legal contractual binding:

1) TECHNOLOGY STACK	Product Name	License type
(a) Frontend		
(b) Middleware		
(c) Backend		
(d) Provide list of all the open source licensed components		
(e) Provide a list of all the commercially licensed components		
(f) Integration Technology		

Note 1: License Type must be either commercial, Open Source or a description of the type of license that will enable scoring.

Note 2: In the event that no license type is provided/indicated by the bidder, the declaration must still be completed and signed.

DECLARATION

I, the bidder (Full names) …….

representing (company name) …….

Hereby confirm that I comply with the above Technical Functionality Requirements and understand that it will form part of the contract and is legally binding.

Thus, done and signed at …….. On this……day of……..…20….

…….

Signature

Designation:

ANNEX E: THIRD-PARTY RISK MANAGEMENT (TPRM) ASSESSMENT

1. INSTRUCTIONS

(1) In terms of the approved SITA Third-Party Risk Management Framework, all Bidders responding to this bid **must** complete the following section by answering **ALL** the questions.

(2) By completing the Third-Party Risk Management Assessment, the Bidder agrees to provide all reasonable supporting documentation when requested to do so, as well as during contract finalisation as this is a **pre-award condition of this bid**.

(3) Any risk identified during the assessment process will have to be mitigated and/or remediated before or during the contract finalisation phase. A detailed mitigation plan, that is acceptable to SITA, may also be required.

(4) Supplier due diligence, as contained in the Special Conditions of Contract, is also applicable to this Third-Party Risk Management process.

(5) The following 6 (six) risk elements will be assessed:

(a) Company risk: 10 questions;

(b) Financial risk: 6 questions;

(c) Operational risk: 8 questions;

(d) Governance and compliance risk: 6 questions;

(e) Information security and privacy risk: 7 questions;

(f) Reputational risk: 6 questions.

2. EVALUATION CRITERIA

(1) Company risk

(a) Questions 2, 3, 6, 8, 9, 10:

Evaluation criteria	Score
Yes	0
Partially meet requirements	0.5
No	1

(b) Questions 1, 4, 5:

Evaluation criteria	Score
Yes	1
Partially meet requirements	0.5
No	0

(c) Question 7:

Evaluation criteria	Score
Yes, actively operating for more than 5 years	1
2-5 Years actively operating	0.5
No, actively operating for less than 2 years	0

(2) All questions for all other risk elements:

Evaluation criteria	Score
Yes	1
Partially meet requirements	0.5
No	0

3. THIRD PARTY RISK ASSESSMENT

The assessment of bidders' responses to the questions will be determined by the completeness (i.e. **all** questions answered), undertaking signed (where required) and accuracy of substantiating evidence, when requested. Please note that SITA reserves the right to verify the information provided.

Question to assess each risk element		Bidders response: Mark relevant box with an "X"		
Company Risk				
(1)	Have you listed all related party transactions to be declared between you and SITA or its department in SBD9?	**YES**	**PARTIALLY**	**NO**
(2)	Are you currently involved in litigation against SITA – or do you foresee litigation being instituted within the next 6 months?	**YES**	**PARTIALLY**	**NO**
(3)	Are there any law suits or ongoing litigation that could affect this transaction in any way or the bidder as an ongoing concern?	**YES**	**PARTIALLY**	**NO**
(4)	Is customer service delivery or contract performance actively monitored by you?	**YES**	**PARTIALLY**	**NO**
(5)	Do you have formal strategic planning processes in place?	**YES**	**PARTIALLY**	**NO**
(6)	Are any of your directors or shareholders Prominent Influential People (PIP) or Politically Exposed Persons (PEP)?	**YES**	**PARTIALLY**	**NO**
(7)	Has your company been actively operating as a going concern for more than 5 years?	**YES**	**2-5 YEARS**	**LESS THAN 2 YEARS**
(8)	Is the company busy with a re-organisational/restructuring process that may impact this transaction?	**YES**	**PARTIALLY**	**NO**
(9)	Are any of your suppliers located in a region where geopolitical risk exposure is high?	**YES**	**PARTIALLY**	**NO**
(10)	Has any current director of the bidder ever served as a director of a company during a period where a Government contract was cancelled?	**YES**	**PARTIALLY**	**NO**
Financial Risk				
(1)	Did you have positive revenue growth in the past three years?	**YES**	**PARTIALLY**	**NO**
(2)	Is the proposed bid price going to be **less than 40%** of your total annual revenue for the previous financial year?	**YES**	**PARTIALLY**	**NO**
(3)	Is the financial health of your company in good standing?	**YES**	**PARTIALLY**	**NO**
(4)	Were your Annual Financial Statement (AFS) unqualified in the last financial year?	**YES**	**PARTIALLY**	**NO**
(5)	Do you have sufficient cash in the bank (2 or more months' worth of operating cost) to operate under restricted conditions for at least 2 months?	**YES**	**PARTIALLY**	**NO**
(6)	Do you have a clean credit record: No current or pending judgement, adverse listing, business rescue or principal sequestration listing?	**YES**	**PARTIALLY**	**NO**
Operational Risk				
(1)	Do you have operational redundancy (resilience) in terms of technology and energy resources to ensure high availability of services?	**YES**	**PARTIALLY**	**NO**

Question to assess each risk element		Bidders response: Mark relevant box with an "X"		
(2)	Are your dependencies for logistics either fully under your own control **or** managed through supplier performance management contracts? (Choose "Yes" if fully under your own control and "No" for supplier contracts)	**YES**	**PARTIALLY**	**NO**
(3)	Do you have operational procedure standards in place across the organisation, such as change control, release management, access control, incident management, back-up regimes and restore tests, etc?	**YES**	**PARTIALLY**	**NO**
(4)	Do you have human resources management in place, including succession planning and mitigation against key reliance on single individuals?	**YES**	**PARTIALLY**	**NO**
(5)	Do you have sound supply chain processes in place?	**YES**	**PARTIALLY**	**NO**
(6)	Do you have sound third party risk management processes in place (fourth party for SITA)?	**YES**	**PARTIALLY**	**NO**
(7)	Do you have a fully-fledged research and development (R&D) department to ensure continuous improvement?	**YES**	**PARTIALLY**	**NO**
(8)	Do you rely on locally manufactured components or have actively managed the risk relating to lead times or delivery delays? (Choose "Yes" is you rely on locally manufactured components or can actively manage lead times and prevent delivery delays where manufacturing is not local i.e. not in South Africa)	**YES**	**PARTIALLY**	**NO**
Governance and Compliance Risk				
(1)	Do you comply with all legislation, including labour, health and safety regulations?	**YES**	**PARTIALLY**	**NO**
(2)	Do you have the appropriate governance frameworks (COBIT, ITIL, King) in place with due monitoring against set standards?	**YES**	**PARTIALLY**	**NO**
(3)	Do you have an internal audit function compliant with IIA standards (insourced, outsourced or co-sourced) in place?	**YES**	**PARTIALLY**	**NO**
(4)	Do you follow formally documented enterprise risk management processes?	**YES**	**PARTIALLY**	**NO**
(5)	Are all statutory requirements of the entity up to date? Specifically, the following: CIPC Returns, Tax returns, UIF and COIDA.	**YES**	**PARTIALLY**	**NO**
(6)	Do you have comprehensive insurance in place, including cover for assets, business disruption and liability?	**YES**	**PARTIALLY**	**NO**
Information Security and Privacy Risk				
(1)	Are your physical security perimeters appropriately safeguarded?	**YES**	**PARTIALLY**	**NO**
(2)	Do you have video surveillance of areas that will contain SITA information/products?	**YES**	**PARTIALLY**	**NO**
(3)	Do you conduct security and suitability verification of all employees prior to employment?	**YES**	**PARTIALLY**	**NO**
(4)	Do you have identification verification controls in place in all your buildings?	**YES**	**PARTIALLY**	**NO**
(5)	Are your access control protocols verified to be effective by Internal and/or External Auditors?	**YES**	**PARTIALLY**	**NO**

Question to assess each risk element		Bidders response: Mark relevant box with an "X"		
(6)	Do you have Security Information and Events Management (SIEM) processes in place?	**YES**	**PARTIALLY**	**NO**
(7)	Do you have sufficient information security and cyber arrangements in place for employees working from home?	**YES**	**PARTIALLY**	**NO**
Reputational Risk				
(1)	Do you have anti-bribery and corruption, anti-money laundering and fraud prevention practices in place?	**YES**	**PARTIALLY**	**NO**
(2)	Please confirm that neither the company, nor any of its directors has been named in any corruption scandal (choose "Yes" to confirm **not being named** in a corruption scandal)	**YES**	**PARTIALLY**	**NO**
(3)	Do you have a social responsibility programme in place?	**YES**	**PARTIALLY**	**NO**
(4)	Do you have an environmental protection policy, including potential harmful emission or hazardous waste management?	**YES**	**PARTIALLY**	**NO**
(5)	Do you actively manage your organisation's energy consumption?	**YES**	**PARTIALLY**	**NO**
(6)	Is your employment equity plan up to date and actively managed?	**YES**	**PARTIALLY**	**NO**

4. THIRD PARTY RISK MANAGEMENT DECLARATION

The bidder hereby makes the following declaration and confirm the following information (mark with a "X" in the corresponding column):

STATEMENT OF DECLARATION		ACCEPT AND CONFIRM	DO NO ACCEPT AND CONFIRM
(1)	All questions in this assessment were answered accurately.		
(2)	SITA can request additional supporting documentation, within reason, to confirm the accuracy and completeness of the information provided in this self-assessment.		

DECLARATION OF ACCEPTANCE

		ACCEPT ALL	DO NOT ACCEPT ALL
(1)	The bidder declares that all information provided in this assessment is accurate.		
(2)	The bidder understands that any false information may constitute misrepresentation.		
	(a) SITA reserves the right to verify the information provided.		
(3)	By completing the Third-Party Risk Management Assessment, the Bidder agrees to provide all reasonable supporting documentation when requested to do so, as well as during contract finalisation as this is a **pre-award condition of this bid**.		
(4)	The bidders understand and agrees that this section will form part of the contract and is legally binding.		

Any additional comments by bidder pertaining to the third-party risk assessment:		

NOTE: Failing to complete all the questions, or not Accepting the Declaration of Acceptance above will result in disqualification.