8 Hardware and Infrastructure Requirements

All PhilSys applications that will be developed by the SI MUST run on commodity-first hardware and MUST be capable of horizontal and vertical scaling without changing major components. The hardware and peripherals to be provided MUST have in-country presence, service, and support for all components proposed in this project (e.g. compute, storage, security, network, and other peripherals). The SI shall provide a detailed Summary of Costs using **FPF 2 of PBD Volume 1**. The Summary of Costs shall specify each hardware, software, and peripherals to be provided indicating their brand, models and specifications under the description column, quantities, country of origin, unit price, and cost related to taxes, transportation, etc.

8.1 Guidelines and Instructions

8.1.1 Component Specifications

a. SI shall offer latest and proven technologies that are available in-country and with local support and parts for the offered items. The SI shall secure from the OEM or its authorized resellers/distributors that these conditions are met. Any component that does not meet this requirement shall be rejected. .

b. The SI is responsible for provisioning all the equipment along with associated peripherals, accessories, cables, sub-components, etc.

c. Any additional components, sub-components, assemblies, sub-assemblies that would be required to meet the desired performance requirements and configuration of proposed solution under **"live"** conditions will have to be provisioned by the SI at no additional cost to PSA and without any project delays.

d. It is expected that the SI shall provide an integrated solution after due consideration to the compatibility issues between various components. If there is a problem with compatibility between components, the SI shall replace the components with an equivalent or better component that is acceptable to PSA at no additional cost to PSA and without any project delays.

e. The OEM(s) whose components are proposed should be established industry players in their respective domains such as Servers, Storage, Network, Security etc. and should figure in reports published at any time in last three years from leading and widely recognized international IT publications.

f. The OEMs whose products are offered must have their own Technical Assistance Centers. The SI is responsible for coordinating with all Technical Assistance Centers for all issues.

g. The SI shall obtain a certification from the OEM that the quoted products are not End of Support (EoS) and not End of Life (EoL). Further, for the duration of the contract the SI is responsible for securing the Annual Maintenance Contract (AMC) from the OEM and for ensuring availability of spare units and/or parts.

h. The SI must factor the standard warranty of product and AMC in such a manner that the PSA has the benefit of AMC for the duration of the contract.

8.1.2 Software License Guidelines

a. All proposed software licenses by the SI must be perpetual licenses on behalf of the PSA with maintenance, upgrades and updates during the contract period. Software licenses must not be restricted by location and the PSA will have the opportunity to use software licenses for its needs at any time and any place in relation to this project. The SI must provide, with the offer, OEM standard licensing policies for each software.

b. The SI licensing model based will be subject to the following conditions:

   1) The license MUST be in the name of the PSA,

   2) For Subscription Licenses, coverage MUST be for the entire duration of the contract,

   3) That PSA shall have the right to renewal of software licenses at the end of the contract.

8.1.3 Server Specifications

a. At the time of bid submission, SI shall propose the latest (within the last 1 year) server model with proof from OEM.

b. The proposed server models should support redundant power supplies.

8.1.4 Storage Specifications

The SI must propose Software Defined Storage (SDS) or any other compatible storage system along with enterprise support for the duration of the contract.

8.1.5 Network Specifications

The network components forming part of the Summary of Costs should be from the same OEM for all phases of deployment. In the event that the OEM is no longer able to provide device upgrades, updates or refresh, the SI shall propose to PSA equivalent or better replacements.

8.1.6 Security Specifications

The OEM(s) whose security components are proposed should be from reputable and established industry leaders in the security domain and should figure in reports published at any time in last three years from leading and widely recognized international IT publications. The SI MUST provide materials to support the OEM's experience and expertise.

8.1.7 Virtualization Specifications

a. SI shall include the virtualization license costs into the BOM.

b. The OEM(s) whose virtualization components are proposed should be available in publicly available information materials published within the last three years from leading and widely recognized international IT publications. The SI MUST provide materials to support the OEM's experience and expertise.

8.1.8 Backup and Recovery Specifications

a. SI shall provide enterprise-grade backup and recovery solution.

b. Backup and recovery solution shall provide for backup of host file systems, VMs, Software Defined Storage, Databases, and Log/Audit Files.

8.1.9 Replication Specifications

a. Replication solution shall provide for replication of data in file systems, Software Defined Storage, Applicatios, Databases and Log/Audit Files.

The replication solution shall use established standards and protocols. Proprietary components for replication shall be disclosed and subject to PSAs review and approval. PSA reserves the right to require the SI to propose alternatives for a replication solution during the negotiation stage.

8.2 HSM Module

a. Encryption keys must remain high availability with multiple HSM executed in active-active mode.

b. Backup to be performed only on compatible HSM stations

c. Backup to be performed whenever a new key pair is generated

d. The SI, at the minimum shall provide HSM boxes for the following sites:

   1) For production environment for Primary DC

   2) For production environment for Secondary DC

   3) For production environment for DR

   4) For testing/staging environment

8.3 Network Architecture

8.3.1 Network Operations Center (NOC)

SI shall undertake a requirement analysis and provide requirements for set up of NOC facility and to integrate PhilSys network monitoring to the NOC. The NOC requirement analysis is part of the detailed functional and technical specification under the Project Initiation deliverables. The NOC requirements analysis MUST be further enhanced as succeeding versions of PhilSys Infomration System are implemented.

a. The SI shall:
    1) Setup and provide network infrastructure for PhilSys Network Operations Center (NOC).
    2) Provide the detailed Summary of Costs (**FPF 2 of SI PBD Vol. 1**) for NOC.
    3) Define objectives, key activities, technical and physical requirements of NOC for integration with PhilSys.
    4) Undertake integration of tools and network architecture and prepare a process for reporting requirement for PhilSys and share it with PSA for generation of necessary reports

b. PSA shall provide physical space for hosting of NOC.

8.3.2 Network and Connectivity

This section describes the network requirements for the PhilSys solution. The requirements of connectivity, WAN, LAN, DC-DR, internet is described in the section.

The PhilSys network consists of four different type of networks, namely WAN, Data Center to Data Center (P2PLinks) Network, Internet Network, and DC Local Intranet.

The network connectivity encompasses the following:

a. Partner Network
    1) Relying Parties Connectivity
    2) Trusted Service Providers – Authentication Services to DC/DR
b. PhilSys WAN
    1) Card Production to DC/DR

2) PhilSys Fixed Registrations Centers to DC/DR
3) DC-DR Replication Links
4) Primary DC-DR – Secondary DC Links
5) Contact Center – CRMS to DC/DR
6) IT Operations
    i. NOC to DC/DR
    ii. SOC to DC/DR

c. Internet
    1) PhilSys Web Portal Access
d. DC/DR LAN and Intranet
    1) DMZ
    2) MZ

8.3.3 Standards and Guiding Principles

a. Use Open Standards like TCP/IP (V4/V6) for Network / Transport Layer
b. All data in transit and at rest to be encrypted
c. All external network connectivity should be via multiple ISPs
d. All Network links should be highly available – with redundant paths
e. All Network devices should be highly available with no single point of failure and should support redundant network interfaces
f. External Network Links to be provisioned from two different ISPs with different network paths
g. All ingress traffic to be routed via Firewalls, NIPS, Deep packet inspection devices
h. All incoming packets to be subjected to AV Checks
i. Network MUST be designed to handle Microservices, Virtualization, Software Defined Storage requirements
j. Network to be segregated into multiple Physical, Logical Zones for security & isolation
k. Access Control at every layer, MAC / Network / Transport / Application
l. All network devices, links, ports should be monitored and managed via the management tools as defined in the EMS section.
m. Separate network for data and management.

8.3.4 Network Architecture

WAN	P2P Links	Internet
Data Center – DMZ, MZ/DC LAN		

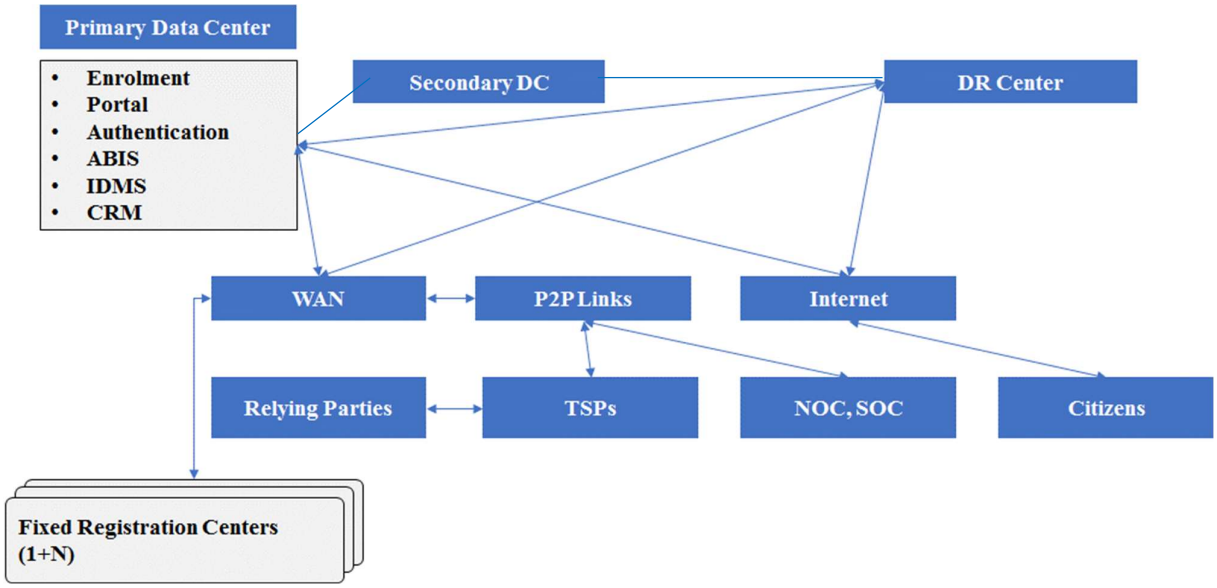

Figure 15. PhilSys Indicative High Level Network Architecture

The above figure shows the indicative PhilSys WAN network connecting the Data Centers, Relying Parties and other entities in the ecosystem. Various entities in the PhilSys network are the Primary Data Center, Secondary Data Center, DR site, Fixed Registration Centers, Relying Parties, Trusted Service Partners, the NOC and SOC of the PhilSys Operations. The end users or the public connect via internet. The SI shall finalize this design and request for approval from PSA during Project Initiation.

8.3.5 PhilSys DC Network

The PhilSys DC network shall have a multiple tiered architecture with multiple zones protected by firewalls, intrusion prevention devices. The SI shall finalize this design and request for approval from PSA during Project Initiation.

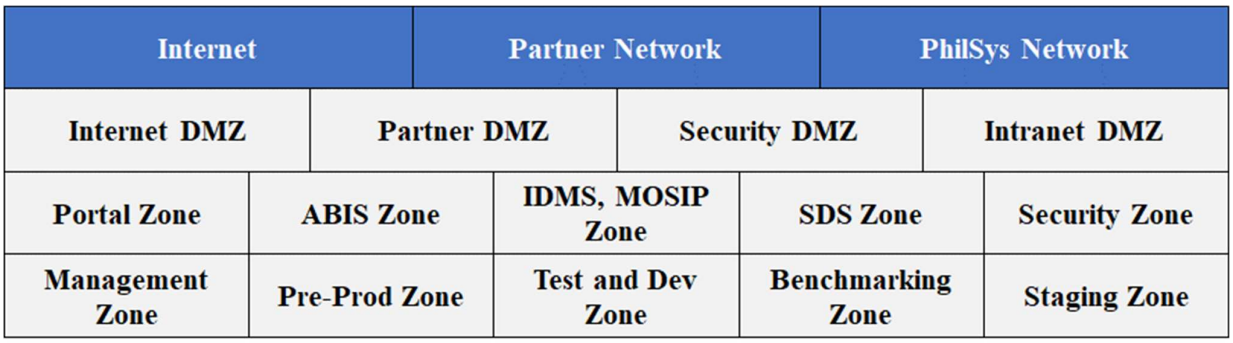

Figure 16. Data Center Network Zones

As shown in Fig.16, the Data Center (DC) network is divided into multiple zones. This is to enable enhanced security and isolation of each subsystem. At the edge lies the connectivity to the external network via Internet, Partner Network and the PhilSys Network. The external network is followed by a corresponding DMZ. There is also a corresponding MZ for each of the external entities to connect to the MZ which is further divided into multiple zones, each zone is completely isolated from another zone via intrusion prevention devices and firewalls.

Figure 17. External Network Zones

8.3.6 PhilSys Fixed Registration Centers Network

The SI shall provide the networking devices to protect and maintain the secured networking connectivity of the 250 PhilSys Fixed Registration Centers.

8.4 Storage Architecture

a. The SI shall use Software Defined Storage (SDS) approach or technology for PhilSys solution.

b. The propose SDS shall support Bare Metal hosts, Hypervisors, virtual machines and containers to access the storage across all leading operating systems, databases, data stores used by the PhilSys and MOSIP applications.

c. The SI shall finalize the storage architecture and request for approval from PSA during Project Initiation.

8.4.1 Open Standards

The SDS solution shall be based on open standards, preferably open source with and safeguards against vendor lock-in.

8.4.2 Storage Security

8.4.2.1 Authentication & Authorization

The SDS solution shall allow only authorized hosts or VMs or containers or applications to access the relevant storage object. All communications between the SDS user/client and the SDS cluster shall be secure.

8.4.2.2 Data Encryption

The SDS solution shall support strong encryption using client supported keys and also integration with HSM.

8.4.3 Capacity, Performance and Scalability

The SDS solution shall support increased storage capacity and throughput by addition of memory, disks to a node or by addition of new nodes. The upgrades shall be done without downtime and zero data loss. The SDS solution shall support addition of data nodes of different capacities (Storage, Performance) to

the cluster. The solution shall also support migration of data, metadata from an existing node to a new node (in case of hardware failure, obsolescence or migration to a higher capacity node).

9 Services

This section provides the scope of work that must be delivered by the SI. The scope covers the software to be developed and services to be delivered for the PhilSys Information System. The SI shall also provision the hardware needed related to the development of the software and services to be delivered for the PhilSys Information System.

An overview of the scope of work for the System Integrator is given below.

9.1 Software Development Life Cycle

This section provides the key activities to be performed by the SI in implementing the software development life cycle for the PhilSys.

9.1.1 PhilSys Application Development & Implementation

As implementation of PhilSys Application is critical and complex, PSA envisages a Phased implementation approach for a successful implementation. It is understood that pre-registration and registration of Citizens and residents are important functionalities of the application and hence has to be implemented first. The detailed implementation schedule of PhilSys is provided in *Section 13* Implementation Schedule.

The development of PhilSys Information System has been envisaged in 4 phases. It would be the responsibility of the SI to prioritize the roll out of all PhilSys Application modules. Please refer to Section 13.3 SI Implementation Timeline.

9.1.2 Implementation and Customization (Provision of Software Tools and Licenses)

In the development of PhilSys applications, SI should ensure that the following is adhered to:

a. SI will be responsible for supplying the application and licenses of related software products and installing the same so as to meet PhilSys requirements.

b. SI will be responsible for supplying tools, accessories, documentation required to make the integrated solution complete as per the requirements. Tools and accessories shall be part of the solution at no additional cost to PSA.

c. SI shall have to provision for procurement of licenses for all phases of implementation.

d. The SI shall perform periodic audits to measure license compliance against the number of valid end user software licenses consistent with the terms and conditions of license agreements, volume purchase agreements, and other mutually agreed upon licensed software terms and conditions. The SI shall report any exceptions to license terms and conditions at the right time to the PSA. However, the responsibility of license compliance solely lies with

the SI. Any financial penalty imposed on PSA during the contract period due to license non-compliance shall be borne by SI.

9.1.2.1 Maintenance of PhilSys Information System

a. The SI will be responsible for Operations and Maintenance of the PhilSys Information System for the duration of the contract. PhilSys maintenance and management support includes, but not limited to, troubleshooting and addressing functionality/availability and performance issues and also implementing change requests etc.

b. For the purpose of operation and maintenance support, the SI shall provide a team of full-time resources as given in *Section 11 Manpower Requirement*. Maintenance and management support shall be undertaken whenever any maintenance and enhancement activity need to be carried out as per the mutually agreed plan or change request. SI shall plan upgrades/major changes to the software s while ensuring that the SLA requirements are met at no additional cost to the PSA.

c. The SI shall be responsible for maintaining all the master data for the PhilSys.

Key activities to be performed by the SI shall include the following:

9.1.2.2 Application Software Support

a. The SI shall provide continuous support through on-site team / telephone / email / Video Conferencing / installation visits as required.

b. The SI shall address all the errors / bugs / gaps in the functionalities of the solution vis-à-vis the approved FRS and SRS at no additional cost during the maintenance and management phase.

c. All patches and upgrades from OEMs shall be implemented by the SI. Technical updates/ upgrades relating to new version, as and when required, shall be done by the SI. Any version upgrades of the software / tool / application will be done by the SI after seeking prior approval from the PSA and submitting the impact assessment of any upgrade.

d. Any changes/upgrades to the software performed during the support phase shall be subject to comprehensive and integrated testing by the SI in order to ensure that the changes implemented in the system meet the specified requirements and do not impact any other existing functions of the system. A detailed process in this regard will be finalized by the SI in consultation with the PSA.

e. An issue log shall be maintained by the SI for the errors and bugs identified in the solution as well as any changes implemented in the solution. Issue log shall be submitted to the PSA monthly.

f. The SI will inform the PSA, as per the agreed plan, about any new updates/upgrades available for all software components of the solution along with a detailed action report. In case of critical security patches / alerts, the SI shall inform the PSA immediately along with any relevant recommendations. The report shall also contain the SI's recommendations on update/upgrade, benefits, impact analysis etc. The SI needs to execute updates/upgrades and update all documentations and Knowledge databases etc. The SI will carry out all required updates/upgrades by following a defined process at no additional cost.

9.1.2.3 Change and Version Control

a. All planned or emergency changes to any component of the system shall be carried out through the approved Change Control Management process. The SI must always follow standard industry process. For any change, SI shall ensure:
   1) Detailed impact analysis is conducted
   2) All change plans are backed by roll back plans
   3) Appropriate communication on change required has taken place
   4) Requisite approvals have been received
   5) Schedules have been adjusted to minimize impact on the Production environment
   6) All associated documentation is updated after stabilization of the implemented change
   7) Version control is maintained for all software changes

b. The SI shall define the version control process through version control process software. For any changes to the solution, the SI must prepare detailed documentation including proposed changes and impact to the system in terms of functional outcomes/additional features added to the system etc. The SI shall ensure that software and hardware version control is carried out for the entire contract duration.

9.1.2.4 Release Management

a. Release Management is used for the release of software of software, upgrades and patches. This ensures the availability of licensed, tested, and version-certified software, which will function as intended when introduced into the production environment.

b. In the context of PhilSys Information System, release management is required to be handled at two levels.

c. The SI is responsible for development and maintenance of all other support applications. Level-3 software incidents related to support application or other enhancements would require change in the respective modules. It is the responsibility of the SI to test the

modified software (including UAT, if required) and then deploy in the product environment. The SI should use automated tools like CI/CD for release and deployment into production. These automated tools and release processes should ensure near zero downtime for deployment of new releases

d. The overall release management and version control of the PhilSys will be the responsibility of SI.

e. The SI shall carry out the following activities in the release management process:

   1) Plan releases as per the requirements for the approved changes.

   2) Build release packages for the deployment for approved changes (one /many) into QA/Staging /Production.

   3) Design, test and implement procedures (mechanisms) for the distribution of approved changes to QA / Staging / Production environment.

   4) Effectively communicate and manage expectations of the customer/internal stakeholders / end-users during the planning and rollout of new releases

   5) Monitor, Control, and Report the distribution and installation of changes to all concerned stakeholders.

   6) Deploy the release as per guidelines.

9.1.2.5 Maintain System Documentation

a. The SI shall maintain at least the following minimum documentation with respect to the PhilSys Information system:

   1) High level design of whole system

   2) Low level design for whole system/module design level

   3) Updated System Requirements Specifications (SRS)

   4) Any other explanatory notes about system

   5) Traceability matrix

   6) Compilation environment

b. The SI shall also ensure that any software system documentation is updated with regard to the following:

   1) Source code is documented

   2) Functional specifications are documented

   3) Application documentation is updated to reflect on-going maintenance and enhancements including FRS and SRS in accordance with the defined standards

4) User manuals and training manuals are updated to reflect on-going changes / enhancements

5) Standard practices of version control and management are adopted and followed

9.1.2.6 Issue Identification and Resolution

a. Errors and bugs that persist for a long time, impact a wider range of users and are difficult to resolve in turn lead to application hindrances. The SI shall resolve all the application problems through implementation of the identified solution (e.g. system malfunctions, performance problems and data corruption etc.)

b. Monthly Issue Logs on problems identified and resolved would be submitted to the PSA along with recommended solutions.

9.1.2.7 Support During System Audits

a. The PSA may get the system audited by third party auditors. The SI shall provide necessary support and cooperation for the audit and close the findings of the audit.

b. The PSA may arrange for the ISO 27001 audit to be conducted for the PhilSys. The SI shall cooperate, provide necessary support and close the findings of the audit.

9.2 MOSIP Application Suite

a. The SI shall use MOSIP applications suites to satisfy the requirements for the PhilSys Information System.

b. The SI shall be responsible to configure the MOSIP application suites to comply with PhilSys requirements and SI shall be responsible for the first level and second level (L1 and L2) maintenance and management of the MOSIP application suite. PSA and its appointed party will assist in resolving the third level (L3) maintenance and management of the MOSIP application suite.

9.2.1 MOSIP and COTS Implementation and Customization

a. The SI shall be responsible for the first level and second level (L1 and L2) maintenance and management of the MOSIP application suite. Assistance to resolve L3 tickets will be provided by IIIT-B India or its nominated agency for one year after Go Live. (Refer Annex D for MOSIP Underlying Tools and Technology)

b. IIT-B India or its nominated agency will also provide maintenance and management support of MOSIP application suite at Level 3 which can be utilized by the SI on need basis for a period of one year or end of MOSIP mandate, whichever is earlier.

c. The Process for escalation of L3 support tickets will be specified in consultation with PSA

In case of development of a COTS/ OTS applications, SI should ensure that the following is adhered:

d. The SI will be responsible for supplying the application and licenses of related software products and installing the same to meet PhilSys requirements.

e. The SI will be responsible for supplying tools, accessories, documentation required to make the integrated solution complete as per the requirements. Tools and accessories shall be part of the solution at no additional cost to PSA.

f. The SI shall have to provision for procurement of licenses for all phases of implementation of the PhilSys.

g. The SI shall perform periodic audits to measure license compliance against the number of valid end user software licenses consistent with the terms and conditions of license agreements, volume purchase agreements, and other mutually agreed upon licensed software terms and conditions. The SI shall report any exceptions to license terms and conditions at the right time to the PSA. However, the responsibility of license compliance solely lies with the SI. Any financial penalty imposed on PSA during the contract period due to license non-compliance shall be borne by SI.

9.3 Setting up of Fixed Registration Centers

PSA is planning to set up Fixed Registration Centers as per the given schedule. (Refer Annex E for list of PFRCs)

Table 46. List of Tentative PFRCs

Year	List of Tentative PFRCs
2020	1. Laoag, Ilocos Norte 2. Lipa City, Batangas 3. Calapan City, Oriental Mindoro 4. Legazpi City, Albay 5. Bacolod City, Negros Occidental 6. Dumaguete City, Negros Oriental 7. Maasin City, Southern Leyte 8. Davao City, Davao del Sur 9. Cotabato City, Cotabato 10. Butuan City, Agusan del Norte

Year	List of Tentative PFRCs
2021	PSA to establish additional 93 PFRCs
2022	PSA to establish additional 25 PFRCs

The role and responsibility of SI in set up and preparation of PFRCs is given below:

a. The SI shall assist PSA in the setup of the PFRCs. The list of tentative locations of PFRCs are given in *Annex E.*

b. The SI shall provide 1 desktop and 1 printer for each PFRC (for a total of 250 desktops and 250 printers) for use in providing other PhilSys Services.

c. The SI shall perform the following activities before commencement of Registration:

   1) Upload the PFRCs location plan into the PhilSys Web Portal

   2) Install and setup ICT system and resources in the PFRCs including connections to PhilSys Data Center.

   3) Prepare readiness checklist for PFRCs to be approved by PSA

   4) Ensure that only PhilSys Registered devices are deployed in PFRCs

   5) Prepare a coordination and escalation procedure for problems encountered in PFRCs

   6) A coding system should be defined and notified for the identification of PFRCs, registration officer before capture of citizen/resident data.

   7) Location code should be assigned for each kit by the PSA and the same should be incorporated in the registration kit before commencement of registration.

9.4 Technical Services to be provided by SI

9.4.1 Warranty & Annual Technical Support

a. The SI shall be responsible for providing annual technology support for the COTS/OTS products supplied by respective OEMs during the entire maintenance and management phase. It is mandatory for the SI to take enterprise level annual support over the entire contract duration, at a minimum, for the software(s) as mentioned in the Summary of Costs provided by the SI.

b. It is mandatory for the SI to take enterprise level annual support over the entire contract duration, at a minimum, for the MOSIP underlying tools and components software(s). The SI should also refer to the MOSIP documentation at https://github.com/mosip/ on MOSIP underlying tools and technologies

c. The SI shall provide a comprehensive OEM warranty applicable on all goods supplied under this contract.

d. The SI shall be responsible for ensuring that the total period of coverage of the warranty and AMC proposed shall be for the duration of the contract.

e. The SI shall provide Technical Support for Software or the respective OEM for the duration of the contract.

f. The SI shall ensure that AMC and warranty support for the server and storage components proposed are provided directly by the OEM or by OEM certified engineers.

g. The warranty and AMC arrangements of SI should ensure that technical resources of the OEM and/ or OEM certified engineers are available for handling L3 incidents facilities whenever required.

h. The SI shall be responsible for creating an asset register with full log of Warranty and AMC provisions of each of the existing assets and providing a half yearly report of the Warranty / AMC position of each asset.

i. For assets whose AMC / Warranty is due for expiry, intimation to PSA shall be provided at least 6 months prior to the expiry of the current contract of SI.

9.4.2 Warranties, AMCs and Spares Management

a. The SI is expected to keep track of all warranties / AMCs in the Asset Management system and invoke the same for maintenance after following predefined processes.

b. The SI is required to make all due payments for warranties / AMCs on time to the OEMs and ensure that the necessary agreements are provisioned and in force always during the tenure of the contract.

c. Adequate number of hardware and spare parts must be maintained to ensure uninterrupted operations.

d. The SI is required to submit a Quarterly Report (Monthly report for the last year of the contract) on AMC / Warranty status, compliance of due payments to OEMs for AMC or Warranties as well as availability and utilization of spares.

9.4.3 Manage Multiple Environments

In addition to the PhilSys production environment, the SI is also required to set up and manage multiple environments for development, testing and training purposes. These will include:

a. **Development environment** – Virtual Infrastructure for source code control, compile, build including appropriate compute, OS, storage, network as required by each of the vendors appointed by PSA.

b. **Testing environments** – Virtual Infrastructure for functional and acceptance testing of applications.

c. **Staging and pre-production environments** – Virtual Infrastructure for testing and validation of the applications prior to production deployment.

d. **Benchmarking environment** – Virtual Infrastructure for performance testing and baselining of the various PhilSys applications. The benchmarking environment is a scaled down version of the production environment. The test results and data from the performance tests in the benchmarking environment will be used to baseline the performance parameters of the system (Throughput, Response Time, System Resource Utilization) including benchmarking of biometric systems (1:1 and 1:N) accuracy.

e. **Production environment** – The SI will be responsible for setting up and managing the production environment, deployment of applications and services to the production environment and will be responsible for coordinating with other service providers for managing releases to the production environment. The SI will be responsible for performing vulnerability assessment for all applications and services prior to their deployment in production environment.

   The SI MUST design and run a periodic (Monthly) accuracy testing of the biometric matching systems. This periodic testing MUST reliably test the accuracy of automated matching for all biometric modalities of both the ABIS (1:N) and the ABAS (1:1). This periodic accuracy testing MUST be done on the production environment and be silent: the BioSP MUST not be able to distinguish testing-related transactions from real ones.

   The SI MUST brief PSA and share report(s) generated after each accuracy testing.

9.4.4 Asset Management

Asset management is a web-based application accessible by PSA.

9.4.4.1 Asset Lifecycle Management

The SI must manage the lifecycle of all hardware and software assets from acquiring, installing, configuration, maintaining and decommission as per PSA policies in force from time to time.

9.4.4.2 Asset Install, Move, Add, Change (IMAC)

The SI shall perform on a need basis asset moves, add, change ("IMAC") for all equipment supplied by it as a part of this contract. The scope of services to be provided shall be as follows:

a. Implement automated digital workflows for end to end IT Asset and its lifecycle management, including real-time usage monitoring

b. SI shall place emphasis on minimal disruption to the business of the PSA during asset IMAC activity scheduling. SI shall provide a single-point-of-contact for all IMAC requests.

c. SI shall:

   1) Implement digital workflows to provide approval for all IMAC requests.

2) All approval processes should be an automated workflow with appropriate levels of approvals by the relevant stakeholders.

3) Ensure that all IMAC requirements are clearly defined in each request;

4) Coordinate any 'Third Party Vendor' activity required to affect an IMAC;

5) Be responsible for the completion of site preparation requirements, prior to the scheduled IMAC date;

6) Establish and communicate to the PSA the escalation procedures for situations where site preparation requirements have not been completed within the defined time frames or in accordance with specifications;

7) Provide required host, server, and network connectivity;

8) Provide the necessary addressing standards and allocations;

9) Provide a designated staging area for displaced hardware and software;

10) Define the procedures for disposal of displaced hardware and software;

11) Be responsible for all regulatory requirements associated with the disposal of displaced hardware and software;

12) Automate logging and tracking of all IMAC activity from receipt of request through completion;

13) Schedule and coordinate IMAC and Refresh activity with End Users and the appropriate business organizations at the PSA (e.g., network operations, facility services, LAN administration, etc.)

14) Automatically backup data on End User Machines prior to relocation, if required;

15) Automate reload of all software and data from an existing Machine to the new Machine and purge existing data from the de-installed machine, if required;

16) Conduct Power on Self-Test;

17) Run additional diagnostics if any if the Power On Self-Test fails to execute;

18) Test network connectivity to a defined logon screen, if required;

19) Obtain End User sign-off that the IMAC activity has been performed in accordance with the requirements specified in the IMAC request;

20) Move all displaced hardware and software and excess packing materials to designated staging area

21) Automatically update the information necessary in the asset management system following any IMAC activity.

22) The IMAC status should be available for real-time viewing, reporting in the EMS portal

9.4.4.3 Asset Tracking

Asset tracking will be one of the key responsibilities of the SI. As part of this, the SI shall automate the asset tracking, asset configuration by real-time monitoring of the physical, virtual devices and software systems.

9.4.4.4 Software Asset Management

Management of software licenses procured by PSA shall be one of the key responsibilities of the SI. The SI shall ensure that all measures are undertaken to ensure compliance that PhilSys operations comply with the terms of licenses and associated usage rights. This shall cover open source software, free software and proprietary software deployed as part of PhilSys operations. The scope of SI's services shall include the following:

a. Implement digital workflows for automated software license management

b. Automate and streamline the process of software inventory and license management. The tool implemented should feature the following functionalities:

    1) Support and manage software license of all types including OEM, node locked, server based, floating, time bound, CAL, Enterprise, concurrent, Volume Licensing, trail, free, open source, etc.

    2) Provide software license utilization dashboard.

    3) Automate tracking of license validity, renewal state and support.

    4) Enable real-time dashboard for compliance status.

    5) Automated tracking of licenses which are active/inactive and thus help manage costs by eliminating renewal of subscription or AMC of unused licenses.

    6) Map dependencies and define relationships as necessary to support complex licensing requirements.

    7) Create a complete picture of application deployment and software asset usage across environments.

    8) Establish linkages between assets and software license, leases, warranty, and support contracts to optimize entitlements and ensure compliance.

c. In addition, the SI shall:

    1) Manage vendor software contracts and relations

    2) Ensure that usage of all trial, open source, freeware licenses are done after approval of the licensing by PSA.

    3) Manage license upgrades, product downgrade rights, and user/device entitlements

4) Manage unusual or customized license agreements through proper exception approval procedures in consultation with PSA. Automate the approval processes.

d. Following will be the deliverables of the SI in this regard:

1) Digital workflows for software asset management

2) Real time dashboard for viewing, monitoring of software asset and license usage across the PhilSys network

3) Identify under-utilized assets, unused assets or licenses and provide an action plan for de-commissioning or shutdown of unused assets.

4) Recommendations on improving utilization of licenses and cost optimization, if any.

9.4.5 IP Address Management

The SI Shall be responsible for IP Address Management for the PhilSys Information System including, but not limited to, the following activities:

a. Planning for IP Address Management

b. Automated IP address tracking

c. Monitoring of traffic flow per IP address

d. Integrated DHCP, DNS, and IP address management

e. IP alerting, troubleshooting, and reporting

f. Provide API Support for IP Address Management

9.4.6 Migration of Pilot Registration Data

The SI shall migrate pilot registration data (approximately one million records including demographic and biometric data) into the PhilSys Registry.

9.5 Services Related to Registration and Authentication

9.5.1 Development of Registration Manuals

The SI shall develop and update PhilSys registration manuals as described below:

a. Create a manual of PhilSys Handbook for Registration officers

b. Develop Technical Manual for on boarding of registration officers

c. Provide one-time creation, enhancement, validation, updating and modification of Technical manual for on-boarding of Registration office

d. Perform continuous updating and modification of the Technical manual to align it with the PhilSys decision on releases on Software System.

e. Provide recommendations for improvement of Registration software, quality checks, manual de-duplication and fraud management functions.

9.5.2 PhilSys Authentication Implementation Framework ("PAIF")

a. The SI shall develop the PAIF which will be an overarching set of standards, protocols, risk models, privacy and liability policies, trust models, and enforcement mechanisms that govern the PhilSys identity authentication ecosystem.

b. Manage the authentication activation requests from respective Relying Partners. The SI shall be responsible for performing all necessary coordination with the respective RP to ensure that the authentication activation request is completed in a timely fashion.

c. To begin with the Government verification and authentication services shall be free of charge. However, in case PSA decides to make authentication services a paid service, the revenue generated from such services shall be electronically collected by SI through a payment gateway.

d. The trigger for deploying authentication services in the distributed mode at the Regional Center level would be provided by SI based on the predictive analytics tools deployed by SI and recommend the same to PSA.

e. Create a Technical manual for authentication on boarding with the approval of PSA.

9.6 Primary Data Center, Secondary Data Center and Disaster Recovery

PSA shall provide the physical space for hosting IT Infrastructure in Primary Data Center, Secondary Data Center, and Disaster Recovery sites. The SI shall be required to take over the sites for hosting infrastructure. The SI shall undertake assessment of the sites, prepare a site plan and rack plan.

9.6.1 Data Center Strategy of Project

a. The core of PhilSys IT Infrastructure shall be hosted in three-way data center setup comprising of Primary DC, Secondary DC and DR sites with the following features:

   1) The Primary DC and DR sites will be in 1:1 configuration i.e. exact replica of each other.

   2) The Primary Data Center will be replicated to Secondary Data Center on real-time basis for all critical application except raw registration packets whose replication frequency will be decided at the time of implementation.

   3) The data at the Secondary Data Center will be replicated to Disaster Recovery Site on a frequency such that the RTO and RPO requirements are met.

   4) For entire duration of the contract, a mechanism for storage and safekeeping of backup media at a remote site will be utilized. The details of these sites will be shared with the winning bidder.

b. The PSA will establish and maintain the network connectivity of sufficient quality and capacity to ensure data replication between data centers.

c. The following table provides the location and capacity by data center type:

Table 47. Hosting sites in Long Run

Data Center Type	Name of Data Center Site	Capacity (in Racks)
Primary Data Center	Subic Bay , Freeport Zone, Zambales	21
Secondary Data Center	Location to be disclosed to winning bidder only	To be shared with winning bidder
Disaster Recovery Site	Location Makati area, Metro Manila	21
Backup Media Storage Site	Location to be disclosed to winning bidder only	To be shared with winning bidder

The details of the scope are provided below in subsequent sections.

9.6.2 Site Set-up

a. The PSA shall provide the physical space for hosting IT Infrastructure in Primary Data Center, Secondary DC and Disaster Recovery Site.

b. The PSA shall be responsible for civil works including provision of cooling and power facilities in these sites.

9.6.3 Primary Data Center and Secondary Data Center Set-up

a. The SI shall take over the Primary Data Center, Secondary Data Center and Disaster Recovery Site from the PSA and set-up the site for hosting of PhilSys Information System.

b. For setting up of site, the SI shall:

1) Undertake a site survey to highlight the positioning of racks, power and backup systems and chart the appropriate and necessary changes, if any.

2) Prepare a site survey report capturing desired changes and submit it to the PSA.

3) Prepare a detailed plan for site set-up and obtain approval from the PSA.

4) Prepare a rack plan positioning and infrastructure set up within the racks.

5) The proposed solution should be optimized for power, rack space while ensuring high availability and no single point of failure.

6) SI needs to provide the requirement for rack space and power for the suggested infrastructure as part of the proposal. SI will need to provide the required air flow, power outlets placement etc. to the PSA so as to align the establishment of Primary Data Center and Secondary Data Center as per the requirements of the infrastructure.

9.6.4 Disaster Recovery Site Set-up

a. For setting up of the DR site, the SI shall:

1) Undertake a site survey to highlight the positioning of racks, power and backup systems and chart the appropriate and necessary changes, if any

2) Prepare a site survey report capturing desired changes and submit it to the PSA

3) Prepare a detailed plan for site set-up and obtain approval from the PSA

4) Prepare a rack plan positioning infrastructure set up within the racks

5) The proposed solution should be optimized for power, rack space while ensuring high availability and no single point of failure

6) SI needs to provide the requirement for rack space and power for the suggested infrastructure as part of the proposal.

9.6.5 Business Continuity and Disaster Recovery (BCP/DR)

a. The main features of the BCP/DR policy to be considered in designing solution are given below:

   1) DR solution to provide with a comprehensive IT infrastructure offering core services such as virtual environment, computing, network and connectivity, and other supporting services.

   2) Replication built-in feature, virtualization manager replication, storage replications, third-party tools etc. will be defined for each service and application during the design phase.

   3) The Primary DC and DR sites will be configured in an Active-Passive Mode while the Primary DC and Secondary DC will be configured Active-Active Mode (For Front-End applications).

b. The SI shall design, document, implement, and maintain all processes under BCP/DR such as backup media recovery, data backup, HSM backup, data replication, remote working, infrastructure recovery, data and technology recovery, people recovery, emergency response procedures etc. for PhilSys Operation.

9.6.5.1 Process/Component-wise Recovery Strategy

An indicative list of recovery strategy of processes and components is given below. The SI is expected to validate the list and finalize the recovery strategy in consultation with PSA.

Table 48. Recovery Strategy

Responsibility	Scope of Work
Registration	• Active – Passive (DC – DR), offline backup • 100% data backup in Secondary DC
Authentication	• Active – Active (DC – DR), offline backup • 100% data backup in Secondary DC
PhilSys portal(s)	• Active – Active (DC – DR), offline backup • 100% data backup in Secondary DC
Email	• Active – Active (DC – DR), offline backup • 100% data backup in Secondary DC
CRMS	• Active – Active (DC – DR), offline backup • 100% data backup in Secondary DC
SOC	• Active – Active (DC – DR), offline backup • 100% data backup in Secondary DC
Admin offices	• Active – Passive (DC – DR), offline backup

Responsibility	Scope of Work
	• 100% data backup in Secondary DC
EMS	• Active – Passive in DC DR

9.6.6 Recovery Time Objective (RTO) and Recovery Point Objective (RPO)

The following table provides the RTO and RPO of various PhilSys business processes:

Table 49. RTO and RPO Business Rationale

#	Process	Criticality	RTO	RPO	Business Rationale for RPO and RTO
1	Registration	High	24 hours	30 minutes	RTO: Registration is an offline process and officers are required to upload packets once a day hence 24 hrs. is affordable RPO (Registration Databases): It is a business requirement that no data shall be lost in the ecosystem (IDMS and PFRCs)
2	Authentication	High	30 minutes	5 minutes	RTO: Authentication is an online process and it is anticipated that the majority of government and private organizations in the Philippines will use this service to be able to provide further services. Hence RTO is 30 RPO (Authentication databases including logs): It is a business requirement that no authentication data shall be lost
3	Critical Portals	High	30 minutes	5 minutes	RTO: These portals could be public-facing and any downtime could have a major reputational impact RPO (Logs databases and Registration, Authentication databases): It is a business requirement that no data is lost from the logs database.
4	CRMS	High	5 minutes	5 minutes	RTO: CRMS is a customer-facing service and any downtime could have a major reputational impact

#	Process	Criticality	RTO	RPO	Business Rationale for RPO and RTO
					RPO (CRMS database, call recordings, etc.): It is a business requirement that no data is lost from the CRMS databases and maintenance of the databases also may be necessary for compliance to legal requirements.
5	SOC	High	5 minutes	5 minutes	RTO: SOC is a very important security operation for IDMS. SOC should never be down as logs from various devices are collected by SOC tool and it is important that logs are always available for investigation purposes RPO (Logs file system, SOC configuration, etc.): It is a business and legal requirement that logs are always available
6	Email	High	5 minutes	5 minutes	RTO: Email is very critical service as a lot of other services depend upon email such as email to applicants when PSN is generated or when registered person authenticates RPO (Emails): Email is a very critical service and a lot of internal and partner communications take place on email hence it is a critical service.
7	Other Portals	Medium	5 minutes	5 minutes if data other than logs ~24 hrs if only logs	RTO: It is understood that these portals are not public facing and criticality RPO (Logs databases and Registration, Authentication databases): It is a business requirement to ensure there is no data loss in case data other than logs is present.
8	NOC	Medium	30 minutes	~24 hrs.	RTO: It is understood that NOC is an important process to monitor the availability of service RPO (Ticketing database etc.): Ticketing database is not a critical database and hence loss of 24 hrs. of tickets can be afforded

#	Process	Criticality	RTO	RPO	Business Rationale for RPO and RTO
9	Office	Medium	24 - 48 hours	N/A (No data is stored)	

9.6.7 HSM Recovery

The SI shall ensure HSM encryption keys (encryption keys and master keys) are backed up every time a new key pair is generated, and the keys are stored securely in HSM backup docks in biometric lockers. The following table provides the frequency, media and storage specifications for each type of HSM data:

Table 50. HSM Recovery

S.No.	Data	Frequency	Media	Storage
1.	Encryption Keys	Every time a new key pair is generated	HSM Backup Docks	Offsite location (other than Primary DC and DR Site) in fire proof safe
2.	Master Key			Offsite location (other than Primary DC and DR Site) in biometric enabled locker with dual access control

9.6.7.1 VPN Access

The SI shall enable remote working of Data Center staff via VPN in case the sites are physically inaccessible. The following guidelines governs the use of VPN access:

a. Enable VPN facility for key staff.

b. Key staff to run the operations from home if site is physically inaccessible.

c. Minimal staff may be present in the Data Centers as far as feasible for on ground support.

9.6.7.2 Disaster Recovery Strategy and Procedures

The SI shall enable recovery strategies in case of any natural or man-made disasters, including but not limited to the following:

Table 51. Disaster Recovery Strategy and Procedures

S.No.	Issue	Recovery Strategy
1.	One Data Center facility is down	• Alternate Data Center with 100% capacity capability • Active-Active or Active-Passive based on criticality of operations and feasibility
2.	Any system component is down	• Redundancy at component level in DC • Redundancy for critical components in DR • Failover to DR in case DC is completely down or vice versa
3.	Data unavailable	• Real time replication (near zero) of all critical data in DR site and vice versa • Worst case scenario if data is lost from both DC and DR, recovery shall be done from backup media stored in a third offsite location
4.	Any telecommunication link is down	• Dual path telecom connectivity • Dual Service providers • Different Telecom service providers for DC and DR • Failover to DR in case DC is completely down or vice versa
5.	People unavailable	• Critical Operations run in automated mode and will continue to run till resolution • VPN facility shall be provided for key staff to enable work from home

9.6.7.3 Testing of BCP/ DR

The SI shall perform the following testing exercises, ensuring simulation of all possible failures:

Table 52. Testing of BCP-DR

#	Test Type	Frequency	Details
1.	Power Source and UPS maintenance	Quarterly	Quarterly maintenance of Power Source and UPS as per manufacturer specifications
2.	Full load power testing	Monthly	Shut down the power from the main electricity switch and test the auto start of Power Source and UPS battery support
3.	Primary Data Center, Disaster Recovery and Secondary Data Center failover for all services	Half yearly	Power shut down in one of the DCs and running the entire operations from the other Data Center
4.	Primary Data Center, Disaster Recovery and Secondary Data Center failover tests for Registration	Half yearly	Registration services down in one Data Center and entire registration operations are run from the alternate Data Center

#	Test Type	Frequency	Details
5.	Primary Data Center, Disaster Recovery and Secondary Data Center failover tests for Authentication	Half yearly	Authentication services down in one Data Center and entire Authentication operations are run from the alternate Data Center
6.	Primary Data Center, Disaster Recovery and Secondary Data Center failover tests for portals	Half yearly	Portal services down in one Data Center and entire portals operations are run from the alternate Data Center
7.	Primary Data Center, Disaster Recovery and Secondary Data Center failover tests for CRMS	Half yearly	CRMS services down in one Data Center and entire CRMS operations are run from the alternate Data Center (DR)
8.	Fire drill	Half yearly	Building evacuation
9.	VPN	Half yearly	Specific staffs operate from home through VPN
10.	Sample restoration of data from backup media	Monthly	Good sampling method shall be used to select random backup media and attempt recovery. Also testing to be done for time taken to bring the backup media from offsite to Data Centers
11.	Full Data backup from backup media	Half yearly for 2 years and then yearly	Full data restoration and reconstruction of the database shall be carried out from the backup media. Initially half yearly activity and once activity is stabilized, frequency can be changed to yearly

9.7 Information Security

This section provides a detailed description of the various Information Security services to be provided by the SI. The scope includes entire PSA security landscape containing LAN, WAN, Wireless, Remote Access, Private Cloud and their accesses and management. The SI shall prepare and maintain proper documentation for each process carried out as a part of their scope of work. These documents have to be approved by PSA for each version update.

The Information Security for PhilSys solution should be comprehensive and should cover all aspects of the information lifecycle across all stakeholders in the ecosystem. The security solution should encompass all hardware, software, processes, governance, procedures, policies, risks and training needs. Following are the indicative list of activities to be carried out by the SI with respect to Information Security.

9.7.1 Security Framework

a. The PhilSys Security framework should cover:

1) Solutions required to secure the core information assets of PhilSys

2) Solutions, capabilities required to secure all interactions with the PhilSys Information System. This includes managing the complete lifecycle of registration centers (fixed and mobile), TSPs, eKYC providers, third parties interacting with PhilSys, PSA Staff, SI and other Vendor staff managing the Data Centers Infrastructure/Applications and managing their access to the systems and how the trust is established in managing these entities.

3) Governance, Compliance and Risks of the PhilSys solution

4) Infrastructure Capabilities required securing these infrastructure assets – Network, Servers, Storage, registration & authentication stations / devices.

5) Surveillance, Thread Models to foresee events, threats that can impact security and reputation of the PhilSys system, identity of users, security of the IDs etc.

b. The following table provides an overview of the security tools required for the solution. The SI is encouraged to enrich the security of the solution by complementing the tools if found necessary.

Table 53. Overview of Security Tools

Level	Services
Security Information and Event Management (SIEM) Security Orchestration, Automation and Response (SOAR)	• The SIEM is used for collecting the security logs from all the perimeter devices, servers, VMs, Containers, Databases etc. Information collected from these devices is used for creating correlation rules and perform investigation for security incidents, troubleshooting the issues, etc. • In SOAR, the security processes and security solutions are mapped together using automation. SOAR will lower down the manual efforts for security analyst in the SOC and improves the efficiency and overall response time for any incident. The SOAR should be integrated with the SIEM solution.
IAMS	IAMS tool is used for user access provisioning and de-provisioning for PhilSys systems. It ensures that right people have access to right resources. The privilege Identity management module is used to provide secure access to servers. IAMS tool helps to provide role-based access to privileged users.
GRC	This solution is used for managing the Governance, Risk and Compliance (GRC) program across the IT infrastructure of PhilSys. Services which must enabled by GRC are: Vulnerability Management, Incident Management,

Level	Services
	Risk Management, Vendor Management, Audit Management, Business Continuity Management and Audit modules policies. GRC tool should receive inputs from Technical Help Desk for incidents.
Vulnerability Assessment	This tool should perform the vulnerability assessments of all IPs in the PhilSys Network. This tool should integrate with the GRC tool. The vulnerabilities assessments may be carried out periodically by this tool as per the information security polices of PhilSys
Penetration Testing	The penetration testing tool is used for performing penetration testing of all external facing applications, portals of PhilSys.
Application Scanner	The Application scanner should perform secure code review of all applications before they are moved into production. The tool should be integrated with CI/CD release management process
Firewalls	There should be two sets of firewalls at the perimeter level and internally. These two sets should be from two different OEMs.
NIPS	Network Intrusion Prevention boxes should run in Inline mode and all the packets should be scanned against the enabled signature. Signature update should happen automatically on daily basis.
Web Gateways	Web Gateway should perform content filtering in the PhilSys Network. Filtering is used on the basis of categories defined in web gateway like social networking, pornography, job portal etc. Whitelisting for any specific access is done only after approval from the Security Team of PhilSys. It should integrate with advanced persistent threat solution.
Mail Gateways	All the incoming and outgoing mails should be scanned against the rules deployed at Mail Gateways. It should protect PhilSys from both Spam and phishing mails. It should integrate with advanced persistent threat solution.
WAF	It should protect the web infrastructure of PhilSys from any kind of web attacks like defacement, injection, broken authentication etc. It can also function as a load balancer.
HSM	HSM devices should be used for managing and providing security to encryption keys generating during registration / update of resident data or any other key management in the solution.
DDoS	Protection against attack like DDoS can be catered by ISP providers securing PhilSys network from such attacks at off-premises locations.

Level	Services
	During an attack, ISP reroute the DDOS traffic destined for the victim's network to the mitigation center where it is scrubbed, and legitimate traffic is then forwarded to the organization. ISP should provide daily traffic reports. It should also generate alerts in the event of suspected DDoS attacks.
Patch Management	The patch management solution should provide automated patches of the Operating System, Firmware, Virtual Machines, Hypervisors and Applications
Antivirus/Endpoint Protection	The Antivirus solution should be deployed on all endpoints
HIPS	The Host Intrusion Prevention should be installed on Servers
Data Loss Prevention (DLP)	Data Loss Prevention system is used for monitoring any kind of data leakage. Rules should be put in place as a checkpoint against which data is checked before leaving the PhilSys system. The DLP solution should manage the host level and network level data.
Security Feeds	The solution should obtain automatic feeds, emails on threats and new vulnerabilities from leading security authorities.
Policy Compliance	The policy compliance tools should check the systems against the defined hardening policy and alert if there is any vulnerability.
F2F	The dual factor authentication solution should support app-based key generators, OTP, email-based authentication.
DAMS	The access to databases should be secure and all accesses changes to be logged and tracked (including applications, administrators, DBAs etc.).
User Behavior Analytics (UBA)	A standalone UBA tool should be deployed in the PhilSys Infrastructure for monitoring user behavior against any kind of suspicious activity occurred using a PhilSys resource (desktop, laptop, devices etc.). UBA focuses on what the user is doing: apps launched, network activity, and files accessed (when the file or email was accessed, who accessed it, what was done with it and how frequently). UBA solution should make it easier for security personnel to create controls around these policies.
Attack Surface Reduction (ASR)	The goal of ASR is to close all but the required doors to the technical infrastructure and limit access to those doors through monitoring, vulnerability assessment/mitigation, and access control. The Network and Security Team shall perform quarterly audits for the configuration of their

Level	Services
	owned devices and validate for any unnecessary services, ports or assets present in the network.
Application Security and SDLC	The application security should be built into the software development process by using tools, technology and processes. The security solution should manage the Open Web Application Security Project (OWASP) top 10 vulnerabilities and risks in the applications. • A1 Injection • A2 Broken Authentication and Session Management • A3 Cross-Site Scripting (XSS) • A4 Insecure Direct Object References • A5 Security Misconfiguration • A6 Sensitive Data Exposure • A7 Missing Function Level Access Control • A8 Cross-Site Request Forgery (CSRF) • A9 Using Components with Known Vulnerabilities • A10 Unvalidated Redirects and Forwards In addition, the following tools/processes aid in the secure development and testing: • Vulnerability Assessment • App Scan – with Inspection of Critical Code/Potential Vulnerabilities • PT/VT – Automated Testing, Manual Testing/Injection These should be supplemented with the GRC framework.

9.7.2 Design Information Security Architecture

a. The SI is required to carry out detailed assessment of information security needs of PhilSys

b. Based on the overall PhilSys architecture being designed, develop the information security architecture incorporating the required security features/products.

c. Develop detailed deployment architecture for the information security products (LAN, WAN, Physical, Virtual, Wireless, Remote Access, Device Access, etc.) including detailed deployment plan, integration requirements and product configurations.

d. The SI shall develop detailed deployment architecture for cloud information security architecture including detailed deployment plan for virtual and containerized environment.

e. The SI should develop security architecture for securing the Virtual Private Network, Virtual Network Functions, Software Defined network

f. The SI should review and update all ITSM policies and procedures associated information security

g. The SI should update all information security documentation according to the requirements of the design.

h. The SI shall provide fully automated real-time security management and monitoring of entire private cloud infrastructure.

9.7.3 Provide Information Security Products

a. The SI is required to provide the requisite number of licenses and subscriptions of the various information security products (DLP, Anti-Virus, etc.) as per the detailed design.

b. The products should be provided within the timelines determined in the overall implementation plan for PhilSys infrastructure.

9.7.4 Deployment, integration and ongoing support

a. SI will be responsible for deployment of the security products, their integration with rest of PhilSys infrastructure, middleware and software applications and ensuring their successful go-live.

b. SI shall also provision the support for the execution of existing system and services.

c. SI will be required to coordinate with other vendors appointed by PSA in ensuring successful integration and go-live of the information security products.

d. On an ongoing basis, SI will be required to support, update and upgrade (to N-1 version or latest stable version) the tools and devices currently deployed as well as the tools/devices that will be used in the PhilSys infrastructure.

e. Based on issues identified through periodic audits, reviews by PSA or PSA appointed agencies, update and upgrade or fine-tune the deployments of products/solutions.

f. Any new or existing vulnerability/vulnerabilities reported through external system or through vulnerability assessment shall be closed appropriately by update and upgrading the respected system. The vulnerability closure shall be validated by VA test.

9.7.5 Information Security Automation

The SI's Security Automation should cover the following activities/processes:

a. Incident Management and response

   1) Fully Automate the process of collection of incidents from all eligible devices;

   2) Automate the incident qualification process based on intelligence sourced;

3) Dispatch incidents automatically to respective service tracking tools with appropriate priority to service owners;

b. Audit, Verification and Compliance

1) Automation of Vulnerability and Penetration testing process for all eligible resources with little or no manual intervention;

2) Automation of analyses of vulnerabilities and penetration of results with intelligence received from security knowledge source;

3) Automate the creation of service requests with appropriate priorities in service request tools for tracking of incidents;

4) Automation of syslog analysis and creation of service requests with appropriate priorities;

c. Access Control

1) Authentication and Authorization and Single-Sign On;

2) Automate the process for creating reports to all respective stakeholders of PSA;

d. Service Request Automation

1) Study and understand the workflows required for security operations center for managing the service requests;

2) Automation of the workflows and routing service requests;

3) Automation of escalation procedures;

4) Automate the allocation of incidents from various tools to respective queues and service request agents;

5) Automate the Escalation and prioritization process;

6) Publish automated dashboard for SLA monitoring

e. Security Infrastructure Monitoring: Availability, performance and throughput monitoring using automated dashboards for GRC, SIEM, Syslog Servers, Anti-virus / HIPS / DLP / Firewall / Load Balancer and other security devices

f. Enable Log File Monitoring using automated dashboards

g. Provisioning using automation scripts

1) Provisioning of security to all IaaS, PaaS, Bare Metal Services (HIPS, Antivirus, Patch, Virtual Firewall, Virtual LB etc.);

2) All approvals required for provisioning security services workflow;

3) Provisioning of any other services;

h. Reports – All reports to be available in Real-time on the EMS Portal;

i. BCP-DR (switchover, drills, data verification / validation)

j. Performance and Capacity Management – including analysis, prediction and automated capacity provisioning / de-provisioning

9.7.6 Asset Classification and Control Standards

The SI shall perform the following services:

a. Establishing processes for identifying assets and assigning classification levels based on the Confidentiality, Integrity and Availability (CIA) ratings to these assets. The SI should update all asset details in the Asset Management System.

b. Establishing procedures in support of decision-making regarding controls, access privileges of users, and ongoing information management;

c. Ensuring that the information is regularly reviewed for value and updated to manage changes to risks due to new threats, vulnerabilities or changes in the environment;

d. Establishing practices for periodic reclassification, declassification, and destruction based on business impact analysis / risk assessment, changing business priorities or new laws, regulations and security standards;

e. Enforcing archive document retention rules regarding proper disposition all assets; and

f. Protection of the asset and for implementing the controls (as identified and approved by the owner of the asset) and ensuring that protection mechanisms are in place for the classified assets as per PSA's standards.

9.7.7 Vendor Management, AMCs, Subscription and Warranties

The SI will be responsible for managing the vendors of the information security products and will be responsible for timely provision of AMCs, subscriptions, warranties as the case may be.

9.7.8 Ongoing Updates, Upgrades and Patch Management of Products/Solutions

The SI shall be responsible for management of automation scripts timely updates, upgrades, and patch management of the various information security products deployed. The SI should pro-actively identify information security issues and threats and carry out timely countermeasures to protect the PhilSys infrastructure.

9.7.9 Network / Security Access

The SI shall be responsible for management of PhilSys network security. As part of network security, the SI shall ensure the following:

a. PhilSys network shall be used for valid operation purposes only. The protection of information contained on the networks is therefore the responsibility of the SI and the activity and content of user information on the computer networks is within the scope of review by management.

b. The SI shall manage the existing network security systems and procedures, and work for transitioning the existing system and procedure to its proposed version by providing required network security resources in order to protect all PhilSys data, related application systems and operating systems software from unauthorized or illegal access at a level that is appropriate for the information and computing resources.

c. The SI shall ensure that access to network and network resources must made available on need to know basis and authorizations must be obtained from appropriate authorities before providing access.

d. The SI shall conduct access reconciliation audit exercise quarterly to ensure the defined process is being followed.

e. All network and network services in PhilSys shall be identified and documented by the SI.

f. Network and network services required for every job function and role shall be identified and documented by the SI.

g. The SI, for providing access to network and network services shall follow policies detailed in PSA's ISMS Policy manual like Access Controls Policy – User Account Management.

h. The SI shall ensure that the networks shall be logically or physically divided based on the criticality of the information stored in the networks.

i. The SI should ensure that PhilSys networks should not be used for personal and/or private information unrelated to business activities.

9.7.10 Secure Data and Media Handling

a. The SI ensure security of data while transmitting confidential information over public networks to other government agencies.

b. Confidential information not being actively used, when stored or transported in computer-readable storage media (such as disks), shall be stored securely under lock and key.

c. Media shall be protected from physical damages like fire, moisture, and magnetic interference.

d. All media shall be handled with care and shall be ensured that they are not kept near magnetic material and are not exposed to any extreme heat or pollution.

e. A stock or inventory of all the media shall be maintained.

f. Media shall be disposed-off securely and safely when no longer required.

g. Formal procedures for the secure disposal of media shall be established to minimize the risk of sensitive and confidential information being disclosed to unauthorized persons.

h. Special controls shall be adopted, wherever necessary, to protect sensitive information from unauthorized disclosure or modification e.g. use of locked containers, tamper – evident packaging.

9.7.11 Network Security Assessment

a. The SI shall perform network vulnerability assessments on an ongoing basis to protect against compromise and attacks.

b. Assessment report shall be submitted to PSA on a quarterly basis.

c. The SI shall coordinate / assist PSA in independent Third-party information security/network assessment audits performed by PSA empaneled bodies that shall be carried out annually in order to provide assurance to the management.

d.

9.7.12 User and Machine Security for PSA Offices and Inside PhilSys Network

There are likely to be several users and machines (laptops, desktops, Mobile etc.) within PhilSys offices and facilities that connect to the network and some of the servers. As part of network and security management, the SI should ensure appropriate access control is enforced and ensure all machines comply with standard software (OS patch level, Anti-virus versions, etc.) stack. Network security and access control systems should also ensure unwanted programs (bit-torrent, etc.) are prevented from running within the network.

9.7.13 Business Continuity and Disaster Recovery

The SI is required to carry out the following activities with respect to Business Continuity and Disaster Recovery:

a. Develop BCP/DR plan and Business Impact Analysis for BCP/DR.

b. Identify critical systems and dependencies between them.

c. Review the risks and also identify any gaps created by disruptive events created that might impact PhilSys.

d. Form a cross functional BCP/DR Team.

e. Include all the services (Authentication, Registration, CRMS, SOC, NOC, Portals) while managing and periodically updating the BCP/DR plan.

f. Review the data replication strategy between the Primary DC, Secondary DC and DR site; and DC-DR connectivity and failover procedures and perform the necessary upgrade as per the identified gaps.

g. Execute the processes and procedures as per BCP/DR procedures and conduct yearly BCP/DR drills. In doing so, the SI should coordinate with other vendors appointed by PSA to ensure successful completion of the BCP/DR activities.

h. Update existing procedures to address any issues/gaps based on findings of ongoing BCP/DR drills,

i. Implement the DR solution with necessary automation scripts to minimize the need for manual interventions in case of any disaster.

j. Review and validate the disaster recovery procedures, disaster recovery preparedness plan and mitigation procedures, as well as the crisis communication plan implemented in the DR solution.

k. Create the following functional Business Continuity working plans for PSA approval:

   1) Authentication business continuity;

   2) CRMS business continuity;

   3) Registration business continuity;

   4) NOC and SOC business continuity;

   5) PhilSys Web Portal business continuity;

l. Create the following Disaster Recovery working plans for PSA approval:

   1) Information Security Disaster Recovery Plan;

   2) CRMS Disaster Recovery Plan;

   3) Registration Disaster Recovery Plan;

   4) NOC and SOC Disaster Recovery Plan;

   5) Portal Disaster Recovery Plan;

9.7.14 Security Operations Center

This section provides details of SI's scope of work with respect to setting up and operation of the Security Operations Center. The SI shall:

a. Perform 24x7x365 continuous monitoring using automated dashboards of the cyber security posture by analyzing, detecting, preventing and responding to cyber security threats and incidents. For achieving efficiency and accuracy, automate the processes for handling security incident and decreasing false positive.

b. SOC administration services will provide Level 1 (L1), Level 2 (L2), and Level 3 (L3) support services for security monitoring of the PhilSys infrastructure. L1 services will comprise of monitoring, L2 services will comprise of validation of incidents and SIEM management and L3 activities will cover supervision of the SOC team.

c. SIEM must be a single point of collation / convergence of logs from SOC technologies

d. Work on creating SOC environment that must be able to detect attacks emanating from emerging technologies.

e. Carry out continuous threat analysis and create business related use cases, correlation rules by developing the parsers to handle new threats proactively by utilizing the available security resources.

f. Carry out a mechanism for performing automated/manual malware analysis/re-engineering and Sandboxing capabilities.

g. Implement mechanisms for anti-phishing, anti-malware, anti-rogue mobile application, brand abuse across PhilSys ecosystem.

h. Perform advanced threat hunting

i. Monitor, detect and perform root cause analysis of intrusions.

j. Respond to confirmed incidents by coordinating with PSA stakeholders and other vendors appointed by PSA, as necessary.

k. Deploy required tools and devices to automate processes and for faster response to issues.

l. Administer the information security tools and devices deployed in PhilSys landscape on an ongoing basis.

m. Provide real-time view of the PhilSys landscape's security status at the centralized dashboard.

n. SOC team shall be responsible for closure of the issues/incident that are triggered through SOC monitoring (like AV, brute force, spam mail, application attack etc.). SOC should assist the affected team whose tool, device, application, workstation, server has been attacked or is the source of attack.

o. All security issues/incidents shall be managed only by ticketing tools and shall be monitored using automated dashboards for closure as per the defined SLAs

p. Analyze security threat intelligence and vulnerability feeds from various vendors and threat feed sources for security advisory and protecting PhilSys environment from new security challenges.

9.7.14.1 Security Operation Center (SOC) Requirements

The SI's attention is invited to Section 9, which provides a list of security components required for implementing security solution and security operations centers. The SI is required to setup the SOC for PhilSys. The SI shall:

a. Provide 24x7x365 local security operations and support.
b. Provide display unit (television / monitor) and local network connectivity.
c. Define and deliver technical and physical controls of SOC.
d. Design security operations model including detailed technical design.
e. Implement SOC infrastructure, security tools and integrate with network.
f. Manage events log, events, incidents and operations of SOC
g. Provide manpower to PSA for SOC services for duration of the contract. PSA shall deploy its manpower mirroring the SI manpower. The SOC operations and services shall be transitioned to PSA at the completion of the SI contract
h. Develop and implement formal security event reporting and escalation processes, distinct roles and responsibilities for the management of security events, and a continual improvement process.
i. Ensure management of security incidents, inclusive of incident classification, Business Impact Analysis (BIA), and incident closure.
j. Establish a security exception management process.
k. Identify and report information security exceptions based on PhilSys security policies and processes.
l. Provide monthly technical and service reporting capabilities such as:
    1) Service Level Agreement (SLA) Reports
    2) Incident, Problem, and Change Reports
    3) Technical Performance Reports

9.8 Operations and Maintenance

The O&M phase would start from the launching of PhilSys Application Version_4. A summary of O&M operations, Roles and Responsibilities are given below for reference. An indicative scope of major O&M activities is provided in subsequent sections.

This section provides an overview of the activities of the PhilSys project relating to two broad areas: (1) Designing to manage the entire infrastructure, application and (2) Operations & Maintenance of the same.

As part of the overall Operations and Maintenance, the following are the activities and relevant guidelines/details:

a. Comprehensive and onsite manufacturer's warranty should be available in respect of proper design, quality and workmanship of all hardware, equipment, accessories etc. for all the components mentioned above. There should be warranty for all hardware, equipment, accessories, spare parts, software, etc. procured and implemented against any manufacturing defects during the warranty period.

b. Any equipment, having a hardware failure on four or more occasions in a period of less than three months, should have a replace ability assessment and agreement with the hardware supplier.

c. In case of any hard disk drive of any server, SAN, or client machine is replaced during warranty/AMC, the unserviceable HDD should be maintained by the PSA team.

d. Preventive Maintenance (PM) should be carried out of all hardware and testing for virus, if any, and proper records should be maintained at both DC and DR site for such PM.

e. Corrective Maintenance may be carried out for maintenance/troubleshooting of supplied hardware/software and support infrastructure problem including network (active/passive) equipment, security and rectification of the same. There should be complete documentation of problems, isolation, cause and rectification procedures for building knowledge base for the known problems in centralized repository.

f. Warranties should be monitored to check adherence to preventive and repair maintenance terms and conditions. These warranties should comply with the agreed technical standards, security requirements, operating procedures, and recovery procedures.

g. 24x7 monitoring and management of availability and security of the infrastructure and assets

h. Perform regular hardening, patch management, testing and installation of software updates issued by OEM/vendors from time to time after following agreed process.

i. Ensure overall security - ensure installation and management of every security component at every layer including physical security.

j. Prepare documentation/policies required for certifications included in the scope of work.

k. Preventive maintenance plan for every quarter.

l. Performance tuning of system as required.

m. Design and maintain Policies and Standard Operating Procedures.

n. User access management.

9.8.1 Benchmarking, Acceptance and Go-Live

Prior to Go-Live of the PhilSys Information System, SI shall be responsible for undertaking a benchmarking exercise, commission the PhilSys Information System and support the PSA in User Acceptance testing as shown in the Fig.18.

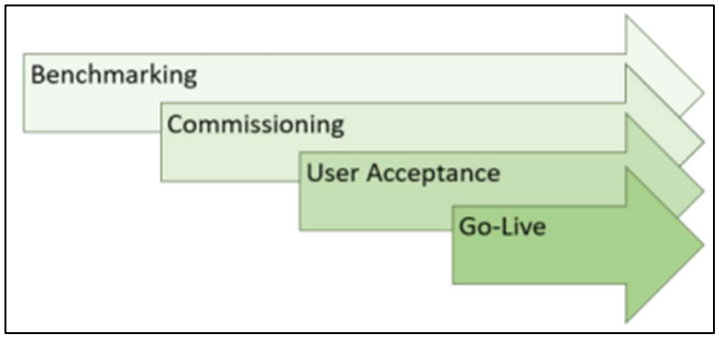

Figure 18. Benchmarking, Acceptance and Go-Live

9.8.1.1 Benchmarking

a. The Benchmarking exercise is intended to evaluate the ability of the proposed PhilSys Information System to scale to the intended usage. It is envisaged to cover the entire PhilSys Information System, including but not limited to its applications/software, other component solutions, PHILSYS Data Store and all related interfaces. The Benchmarking process does not intend to simulate all the aspects of PhilSys Information System however all design parameters, components and related interfaces shall be considered.

b. Benchmarking shall be in accordance with the production deployment and solution architecture proposed in the Technical Proposal of the SI.

c. SI shall be responsible to undertake the benchmarking of the PhilSys Solution. The SI shall:

   1) Prepare benchmarking test cases and obtain sign-off on the test cases from the PSA
   2) Supply, build, commission, configure, tune and execute the benchmarks of the Disaster Recovery Set-up
   3) Provide the tools (load generator), scripts for etc. for benchmarking.
   4) Create test data
   5) Demonstrate at least one successful (live) run
   6) Undertake benchmarking of the PhilSys Information System as per the parameter shown in the table below:

Table 54. ABIS Test Scenarios

Gallery Size Test Scenario (ABIS)	Test Description	Gallery Size	Deduplication Rate	Test Duration
0 to 10 Million	Basic Performance Test with proposed sizing of associated IT Hardware	10 million	125,000	24 Hours
10 to 25 Million	Scalability and proposed sizing for associated IT Hardware	25 million	200,000	24 Hours

Where:

- **Deduplication Rate** – Successful biometric deduplication of resident within 24 hours of receipt of request, subject to a maximum of 125,000 and 200,000 biometric deduplication requests
- **Test Duration** – Duration in which 1: N deduplication of each registration packet should get completed in 24 hours' time cycle

Table 55. Authentication Test Scenarios

(SDK)	Description	Rate	Duration	Concurrency	Response
Auth_1	Basic Performance Test	0.083 Million per Hour	8 Hours	1,000	0.5 seconds
Auth_2	Advanced Performance Test	0.25 Million per Hour	8 Hours	1,000	0.5 seconds

Where:

- **Authentication Request Rate (Basic Performance Test)** – 0.083 million Authentication Requests are expected per hour with a response service time of 0.5 seconds with 1,000 concurrent users during basic performance test.
- **Authentication Request Rate (Advanced Performance Test)** – 0.25 million Authentication Requests are expected per hour with a response service time of 0.5 seconds with 1,000 concurrent users during advanced performance test.
- **Test Duration** – Duration in which 1:1 matching authentication completes as per expected SLA of 0.5 seconds for SDK matching in the entire test cycle.
- **Modes** – Fingerprint (1 or multiple), Iris (both), Face.

- **Basic Test** – OTP based.
- **Advanced Test** – eKYC including biometric authentication.

d. Report the benchmarking output in the format specified by PSA or its appointed party. Key guidelines for reporting benchmarking output are as follows:

   1) Resource usage should have graphs with a sampling interval of 5 minutes for all resources (all servers, routers, switches, disk arrays, firewalls etc.)
   2) Response Time Reports should include minimum, maximum, average and 90 percentile response times. Response Time should be shown as a function of time for the duration of the test.
   3) The test results should also include the iterative configuration changes / tuning required to achieve the benchmark results.
   4) The equipment used for the test shall be the same as proposed by the BioSP, if however, there is a shortfall in the quantity of the equipment proposed, the BioSP should provide the required quantity of equipment/licenses, as the case may-be to achieve the benchmark results and SLA.

e. PSA shall witness the benchmark or appoint an agency at its own cost to verify and validate the benchmarking tests and certify the results of the benchmarking. Benchmark test report provided by the BioSP shall be approved by the PSA.

f. In the event the solution and the corresponding Bill of Materials proposed by the BioSP fails to meet the benchmarking performance criteria, the BioSP shall enhance/augment and supply additional components (including server, storage, networking equipment, etc.) without any additional cost to the PSA.

g. The SI is expected to define parameters to measure performance of PhilSys in consultation with PSA and/or the BioSP.

9.8.1.2 Commissioning

After successful benchmarking of PhilSys Information system, the SI shall commission the entire system in the PSA Primary Data Center, Secondary Data Center and Disaster Recovery Site. The following shall be the key responsibilities of SI for completion of commissioning:

a. Configuration of all the components of the hardware, software, devices, accessories, etc.
b. Integrated testing of all components
c. Tuning and testing of application at the Primary Data Center, Disaster Recovery and Secondary Data Center site.

d. Successful testing of the integrated solution.

9.8.1.3 Acceptance

After successful commission of the PhilSys Information System, the PSA shall undertake a user acceptance of the entire system. Acceptance for PhilSys Information System can be divided into the following phases:

9.8.1.3.1 Pre-Acceptance Phase

9.8.1.3.1.1 Creation of Acceptance Plan

a. The SI shall first identify areas of acceptance of the PhilSys Information System. The SI shall then prepare a draft acceptance plan comprising of acceptance methodology for identified areas, test schedule, timeline of acceptance testing activities and deliverable due dates. The test schedule prepared should identify major test areas, test execution, and test reporting activities. As a part of acceptance plan, SI will also identify roles and responsibilities of the individuals to carry out the acceptance.

b. Acceptance plan should be in alignment with the overall project plan. It will enable SI and PSA to plan the overall project timelines and resource requirements for acceptance phase.

9.8.1.3.1.2 Assistance in Formulating Detailed Acceptance Criteria

The SI shall prepare draft acceptance criteria for each of the above-mentioned areas of acceptance. Acceptance criteria's prepared should be in accordance with the system specifications and functional specifications of the products/service.

9.8.1.3.1.3 Preparation of Detailed Pre-Acceptance and Acceptance Checklists

a. SI shall prepare a detailed checklist of the activities and pre-requisites that are required to be completed before and during the phase of acceptance by PSA. This shall include, but are not limited to:

    1) Required approvals

    2) Availability of testing tools, monitoring tool and test management tools

    3) Preparation of acceptance test scenarios, test cases and test data

    4) Setup of hardware and software etc.

b. The test cases and scenarios developed should be well documented in the format approved by the PSA.

9.8.1.3.1.4 Preparation of Required Environment and Facilities

The SI shall be responsible for setting up the test environment. The test environment, including hardware/software to be tested and support hardware/software, should be as per the planned configuration.

9.8.1.3.2 Acceptance Phase

9.8.1.3.2.1 Execution of Tests

a. SI shall assist the PSA's acceptance test team in executing the defined test cases and scenarios. In the event of unexpected test results/bugs, SI shall log tickets according to the severity of the issue.

b. The PSA may take assistance from an Agency for support in activities related to acceptance of PhilSys Information System. The SI must provide all necessary support to the agency for undertaking the acceptance including sharing of system specifications, functional specifications, acceptance plan, and test cases.

9.8.1.3.2.2 Resolution of Issues Identified During the Acceptance Testing

a. All issues and defects identified by PSA's acceptance test team will be recorded in defined template. For each incident, the SI's defect tracking system should document each issue/defect identified, how it occurred, when it occurred, the tester who discovered it, what system baseline was being used, and a preliminary assessment of the severity

b. The SI should track and report on open defects until they are closed.

c. The SI shall undertake following activities for root cause analysis and take preventive measures:

    1) For every defect reported, the SI team shall carry out root cause analysis and document the same.

    2) At agreed upon intervals, the PSA's acceptance team and SI's team should meet to review the identified defects and decide upon their prioritization and disposition.

    3) SI shall undertake remedial actions for resolution of the defect

    4) SI shall work out the preventive measures so that the incident does not occur in the future.

d. A sample template for reporting the defects shall be prepared by SI:

e. Upon resolution of defects and internal testing, for a maximum of three iterations, the SI shall be responsible for retesting of the issues at no additional cost. The SI shall support the PSA's acceptance test team in re-executing the acceptance test procedures and retest each corrected defect. PSA's acceptance test team can also undertake additional testing if required. If the incident does not re-occur the PSA's acceptance test team shall recommend

closure of the defect. In case incident continues to occur, the PSA's acceptance test team shall inform the SI and the defect shall remain open.

9.8.1.3.3 Post Acceptance Phase

9.8.1.3.3.1 Acceptance Documentation and Signoff

a. The SI shall assist PSA's acceptance test team in creating the reports for acceptance testing. The reports shall summarize the test activities and identify outstanding deficiencies and issues.

b. The Acceptance Test Final Report shall be the detailed record of the acceptance test activities. It shall record which tests were performed, the pass/fail status of each test, and the discrepancies or issues found.

c. The SI shall be responsible for the following deliverables at the end of acceptance testing:

   1) Acceptance Test Plan

   2) Acceptance Test Schedule

   3) Acceptance Test Environment Inventory

   4) Acceptance Test Summary Report

   5) Acceptance Test Final Report

d. Post completion of required documentation and due diligence, the SI shall obtain signoff from the PSAs acceptance test team. **This will constitute Go-Live.**

9.8.2 Network Services

This section describes the network managed services and the scope of work to be performed by the SI.

9.8.2.1 Initial Build

a. Prepare the Network Design and Rack Layout, Cabling Diagram and get it approved by PSA before implementation.

b. Prepare Network Addressing, IP Address management policy document.

c. Prepare Network Connectivity and On boarding of Partners, Network Access and Controls Document.

d. Prepare Network Policies and Procedures Document.

e. Prepare detailed network deployment architecture indicating all network devices, VLANs, subnets, firewalls, NIPS, cabling etc.

f. Create an Acceptance Test plan for testing and validating the network implementation and have it approved by PSA.

g. Create the Wireless Access Policy, SSID, Password Management Policies document for provisioning the wireless networks at the PhilSys fixed registration centers.

h. Create a network rollout plan for connecting external networks, partners, PhilSys fixed registration centers to the Data Centers.

i. Update the Asset management system with all the network asset details (hardware, software).

j. Train the PSA staff on the network setup and operations.

9.8.2.2 Supply and Commissioning of Network Devices

a. The SI shall supply all the required network devices, cables, connectors to the Data Centers and the Remote Offices (PhilSys fixed registration centers).

b. As per the approved design install racks, patch panels and connect the cables, label all the network ports at the patch-panels and the cable ends.

c. Test network physical connectivity across the DC network.

d. Install Network Racks, Routers, Firewalls, Modems, and MUXs for connectivity to external providers. Perform the required cabling to connect to the network service providers (internet, DC-DC p2p links, WAN Links for partner connectivity).

e. Setup the firewall, VLANs, network zones, access controls at the MAC, and network, transport and application layers according to PhilSys policies.

f. Setup and commission the network at PhilSys fixed registration centers.

9.8.2.3 Network Integration

a. Integrate the network elements with the end devices – physical/virtual services.

b. Integrate ABIS network and all the elements in the ABIS network.

c. Integrate the PhilSys Fixed Registration Center Network Devices with EMS.

d. Integrate all the devices for Network Monitoring, management, Trouble Ticketing, Technical Help Desk, SLA Management with the EMS.

e. Integrate the EMS with NOC.

f. Integrate SOC.

9.8.2.4 Network Testing and Go Live

a. Test the LAN connectivity for access, latency and throughput before moving to production
b. Provision the WAN connectivity for
    1) DC To DC Links (replication)
    2) Internet
    3) WAN Connectivity for TPS and other external entities
    4) PhilSys Fixed Registration Services
c. Complete the Acceptance tests as per the acceptance test plan and resolve any open issues as per SLA.

9.8.2.5 Operations and Maintenance

The SI shall perform the continuous monitoring and management of the network 24/7 to maintain the network and overall SLAs. Operations and maintenance activities include:

a. Provision the required manpower as per plan.
b. Monitor and Resolve network issues.
c. Prepare Root Cause Analysis Reports for all critical incidents.
d. Monitor and Track all SLAs.
e. Coordinate with the Network/Telecom Service Providers for resolving any network issues affecting the SLAs.
f. Support PSA in resolving connectivity issues with any TSPs or external entities.
g. Support the ABIS and application teams for resolving any network issues.
h. Continuously Monitor the network bandwidth and capacity for any limitations.
i. Provide a monthly network usage, capacity, errors and SLA report to PSA.
j. Request for provisioning additional bandwidth via the Change request mechanism across any of the WAN networks if the bandwidth becomes a limitation.
k. Coordinate with network OEMs for resolving issues.
l. Backup all the network device configuration after the initial setup and after every configuration change.
m. Update Network Device Firmware based on OEM recommendations after due testing and validation while maintaining the SLAs.

9.8.3 Data Backup

The SI is required to finalize the data back-up strategy in consultation with the PSA's archival policy. An indicative strategy for Data backup is given below for reference.

a. Data Backup Strategy: Key strategy aspects

   1) On the last day of every month, a full backup shall be performed and labelled "Grandfather". The backup media shall be stored permanently offsite.

   2) On the last day of every week, a full backup shall be taken called the "father" and stored offsite.

   3) Daily incremental backup shall be done called the "son". Son backup media can be stored onsite or offsite depending on the volume of data changes. Onsite backup media shall be kept in fireproof cabinet.

   4) Move backup media to offsite location on Daily basis at a geographically separate location with appropriate physical security controls.

   5) For a 5-day working week, there are 4 son backup media, 3 father backup media, and a new grandfather backup media every month.

   6) Backup media shall be encrypted with symmetric key algorithm with highest key strength (such as AES 256).

b. Type of data to be backed up shall include:

Table 56. Types of Data to be Backed-up

#	Data Systems	Types of Data	Frequency	Storage
1.	Data in Databases	• Encrypted raw registration packets • Encrypted Registration Databases • Authentication Databases • Authentication logs databases • Supporting documents databases • ABIS galleries • Encryption Keys databases (if any) • EMS Data Store	Daily, Weekly, and Monthly	Offsite location (other than Primary DC, Secondary DC, and DR Site) in fireproof safe
2.	Applications	• Application databases • Application logs • Application configurations	Daily, Weekly, and Monthly	Offsite location (other than Primary DC, Secondary DC, and DR Site) in fireproof safe

#	Data Systems	Types of Data	Frequency	Storage
		• Application software version repository		
3.	Configurations	• Latest Server configuration images • Latest network configurations	Daily, Weekly, and Monthly	Offsite location (other than Primary DC, Secondary DC, and DR Site) in fireproof safe
4.	Documentation	• Policy, process documents • Standard Operating procedures • Any other important documents	Daily, Weekly, and Monthly	Offsite location (other than Primary DC, Secondary DC, and DR Site) in fireproof safe
5.	Encryption keys (HSM)	• HSM encryption keys	Every time a new key pair generated	HSM backup docks in biometric lockers

c. The SI shall perform back up of all types of PhilSys data based on approved backup strategy for the duration of the contract.

9.8.4 Storage Services

The following is the scope of work of SI for Storage Services:

9.8.4.1 Storage Supply

a. The SI shall supply all the components of the storage, including hardware, software (with all necessary licenses) to install, commission, provision, use and manage the software defined storage solution.

b. The SI shall prepare a storage architecture and deployment architecture, detailed design documents and shall implement the solution after the due approval of the documents from PSA. The design should ensure high availability, reliability and no single point of failure, while meeting the overall SLAs.

9.8.4.2 Storage Design, Policies and Procedures

The SI shall perform the following activities.

a. The SI shall discuss with all the stakeholders and confirm the actual storage capacity and type of storage (block, file, object) and create a detailed design for each of the clusters as follows:
    1) Archival Cluster - 700 TB, 2 replica copies, Raw Capacity – 1500 TB
    2) Log Cluster – 120 TB, 2 replica copies, Raw Capacity – 264 TB
    3) ODS Store – 130 TB, 2 replica copies, Raw Capacity – 273 TB
    4) Authentication Data Store – 20 TB, 3 replica copies, Raw Capacity – 66 TB
    5) Test & Dev Store – 100 TB, 2 replica copies – Raw Capacity – 220 TB
b. The SI shall prepare a storage architecture, detailed design and deployment architecture document. The deployment architecture should include the rack layout, cabling etc.
c. The SI shall prepare a storage access control policy document based on the requirements of the project
d. The SI shall prepare a storage allocation, provisioning and storage-reclaim policy.
e. The SI shall prepare a storage SLA management document.
f. These documents must be approved by PSA.
g. The SI shall ensure that these documents are updated periodically and submitted to PSA for review and approval.

9.8.4.3 Installation and Commissioning

The SI shall perform the following activities.

a. Install the storage servers, network switches and interconnect them based on the approved design and deployment diagram. Ensure that the power limitations per rack, weight distribution/limitations of the data center are followed while installing the storage equipment. Follow the due installation procedure as recommended by the respective OEMs.
b. Ensure that all the equipment is power on self-tested in the staging area before it is moved to the production environment in the data center.
c. Perform the network cabling, iPDU integration in each of the racks.
d. Connect the Storage Servers and the Network Switches as per design, ensure that the end to end connectivity works seamlessly (no packet loss, latency as per the specification) by checking the physical layer, data link and network layers.
e. Complete the installation for all the storage clusters as per design following the guidelines mentioned above.

9.8.4.4 Firewalls and Storage Security

The SI shall perform the following activities:

a. Setup MAC Level, Firewall/Network level access control for all the storage servers to the corresponding clients / users of storage.

b. Ensure that no client or application should have connectivity / access to the storage server or cluster other than what it is permitted to.

c. Integrate the storage node/cluster with the appropriate key management – for managing the encryption/decryption of data

d. Integration the storage solution with the Single Sign-on Solution, setup role-based access to different applications, administrations based on the design and access policy

e. Ensure that the PhilSys Security policies and procedures are followed.

9.8.4.5 Storage Integration

The SI shall perform the following activities.

a. Integrate the storage with the relevant servers and applications

b. Setup MAC Level, Firewall/Network level access control for all the storage servers to the corresponding clients/users of storage.

c. Integrate with the Asset Management System/ITAM tool – via agent or agentless mechanism

d. Integrate with the ITIL tool – via agent or agentless mechanism

e. Integrate with Single-Sign on Server - via agent or agentless mechanism

f. Integrate with SLA Monitoring/Management tool via agent or agentless mechanism

g. Integrate with Storage Provisioning tool - via agent or agentless mechanism

h. Integrate with all the clients, applications, databases which need access to the storage as per the storage policy

9.8.4.6 Storage Capacity, Performance and Scalability

a. Support the storage users (MOSIP application, as applicable, other applications or users) in troubleshooting, resolving issues, rolling out new applications into production and archiving old data as per the archiving policy.

b. Monitor the storage usage by each of the applications and allocate or de-allocate storage necessary based on the usage and policy

c. Monitor the storage performance in terms of IOPS (reads/writes), Network Traffics, Storage Growth, tune/optimize the storage performance to meet the SLAs

9.8.4.7 Patch Management

a. Update the relevant system, OS, Firmware patches after qualifying the same in the test/pre-production environment before moving to production. Notify all storage users of an impact on their applications and assist them in testing their applications with new patches or upgrades.

b. Security and Vulnerability patches should be accorded a higher priority than other patches.

9.8.4.8 Storage Monitoring and Management

The SDS solution should be integrated with the proposed EMS solution for monitoring availability, performance, capacity, configuration management and provisioning. The SDS solution should provide rest API for integration with the EMS. The monitoring shall be 24/7. The SI shall update the CRMS ticketing system with the relevant tickets and resolve the same as per the SLA.

9.8.4.9 Storage Availability and BCP/DR

a. Ensure that the storage is available 24/7 as per SLA.

b. Perform full and incremental backup as per SLA

c. Monitor the storage replication across data centers and ensure that the replication lag is as per SLA.

d. Monitor the replication network and its bandwidth usage, if the lag is due to low bandwidth, coordinate with the network service provider and PSA to increase the bandwidth so that the replication lag is as per SLA.

9.8.5 Technical Helpdesk

a. The PhilSys Information System will require the SI to setup and operate the Technical Helpdesk. The objective of Technical Helpdesk is to provide issue log and issue resolution pertaining to PhilSys Software System, Field Hardware and PhilSys Registry, Security Operations, Network Operations, BioSP team, PSA application users/ System Administrators and database administrators.

b. The PSA shall provide physical space for the Technical Helpdesk along with necessary Electrical and Physical Infrastructure as follows:

1) Premises & Furniture

2) Required floor space

3) Lighting

4) Basic amenities e.g. water facilities
5) Power connection
6) Standard fire-fighting systems
7) Cubicles, chairs, cabinets, etc. constructed
8) Network Connectivity between National Call Center and DC, and National Call Center and DR

c. The SI shall:

1) Provide supervisors and staff to operate the Technical Helpdesk for the duration of the contract.
2) Maintain the IT infrastructure at the Technical Helpdesk for a period of entire contract.
3) Ensure that the Technical Helpdesk is operational 24/7.
4) Enable the Technical Helpdesk to provide support in both **English and Filipino languages.**
5) Leverage the CRMS software / Incident Management module of EMS (supplied by SI as part of this engagement) to achieve the intended objective.

9.8.5.1 Helpdesk Setup and Operations

a. The SI shall be responsible for setting up an IT helpdesk operation to support IT issue resolution
b. The SI shall prepare a detailed plan for implementation of IT Helpdesk in line with overall project timelines. Plan shall be prepared in coordination with the PSA.
c. The SI shall be responsible to prepare standard operating procedures (SOP) for the IT helpdesk. The SOP should include detailed process flow for issue logging, issue prioritization guidelines, problem security codes and escalation procedures, issue resolution etc.
d. The SOP should also include predetermined restoration/resolution targets based upon Service Level Agreements
e. The SI shall deploy CRMS software/ Incident Management module of EMS for the helpdesk which shall be accessible to all users through the PhilSys portal (Intranet) for logging issues
f. The SI should make arrangements for imparting proper training in soft skills, call handling, exposure to related application, required technical skills etc. so as to prepare PSA staff at the IT Helpdesk to answer and resolve issues/ incidents when PSA takes over the helpdesk operation after the contract.

9.8.5.2 Set up IT Infrastructure for Technical Helpdesk Operations

a. The SI shall arrange for the associated hardware, Technical Helpdesk application, other software and network components for operationalizing the Technical Helpdesk.

b. The SI would provide and implement a comprehensive Technical Helpdesk application using the CRMS or Incident Management module of the EMS solution. PSA officials would be using this application. License of the Helpdesk application shall be in the name of the PSA

c. The Technical Helpdesk application should be interfaced with the CRMS solution or EMS solution as the case may be

9.8.5.3 Technical Helpdesk Operations

The Technical Helpdesk would have following major activities and tasks:

a. Log incidents/issues as service requests and provide a unique service request number. Acknowledgement should be sent to user along with service ticket number through an email immediately on issue logging. All issues logged should be assigned a severity level (L1/L2 or L3). Indicative severity level definitions shall be discussed and finalized in consultation with PSA.

b. The Technical Helpdesk application should provide workflow and hierarchy through which each incident should move based on Incident severity, classification and owner.

c. The Technical Helpdesk staff should have a provision to increase the severity levels, if required.

d. The Helpdesk staff shall have provisions through the application for coordinating with concerned vendor in case issues are pertaining to any external entity product/support like:

   1) Respective OEM team
   2) DC/DR Support Team
   3) Network Provider
   4) End User Devices support provider
   5) Any Other

e. The SI shall analyze all the incidents and provide a root cause analysis report on a periodic basis for all the recurring incidents. SI shall ensure that resolution is provided for these problems by respective technical teams/vendors to prevent further issues due to the same cause. The report for the same should be submitted to PSA

f. Track and route incidents/service requests and to assist end users in answering questions and resolving problems. Assign severity level to each ticket as per the SOPs.

g. Issues which cannot be resolved by the Technical Helpdesk should be routed to the concerned team of the SI for resolution

h. Escalate the issues/complaints, if necessary, as per the escalation matrix.

i. Notifying users, the problem status and resolution through the tickets over email or SMS or both.

j. Each service request would have a unique service request number.

k. It is the responsibility of the SI to ensure quality of the Technical Helpdesk.

l. All incidents should be recorded. These records shall be retained on hard disk for 30 days for easy retrieval.

m. Incidents which are not meeting SLAs, and which are exceptional in nature (highly critical, wider spread etc.) shall be escalated as per defined escalation matrix.

n. The Technical Helpdesk should comply with SLAs applicable to them as mentioned in this RFB. Non-adherence to SLAs shall lead to imposition of liquidated damages.

o. Continuous Improvement: The SI shall ensure continuous improvement in the Technical Helpdesk Operations. The SI shall:

    1) Prepare Knowledge base for frequently reported problems along with the resolution steps/solutions and publish on the portal.
    2) On a quarterly basis, carry out the analysis of help desk tickets (open and closed) to identify the recurring incidents and conduct a root cause analysis on the same. The SI shall submit a report to PSA with the analysis and provide inputs to PSA on user training requirements, awareness messages to be posted on the portal, redesign recommendations and/or application enhancements (functional/design) based on help desk ticket analysis. The objective of the analysis should be to address the repeat incidents and enhance the delivery of services to the end users.

p. The SI shall prepare and submit reports to PSA as per the mutually agreed reporting structure. These reports shall include but not limited to the following:

    1) Incident logs (category, severity and status of call etc.)
    2) Incidents escalated
    3) SLA compliance/non-compliance report with reasons for non-compliance
    4) Detailed analysis of the calls containing opportunities of automation, trainings, FAQs, etc.
    5) Technical Helpdesk utilization reports benchmarked against industry standards for similar application/environment.

9.8.6 Enterprise Management

The SI shall manage the PhilSys Information System for the duration of the contract. This includes provision of an Enterprise Management System (EMS) for the PhilSys project. The EMS is intended to enable seamless management of the entire IT Infrastructure, all hardware and software, including network (LAN, WAN) and remote office infrastructure used for the solution. The SI should use open standards and ensure that there is no vendor lock-in in the EMS solution.

The EMS requirements can be broadly classified into the following:

a. Network Management (LAN, WAN)
b. Server Management, Hypervisor, VM Management
c. Storage Management
d. Asset Management
e. Patch Management
f. Backup and Recovery
g. Incident Management, Problem Management, Service Desk
h. DevOps, Release Management
i. Database/Data Store Access Monitoring/Management
j. Application Performance Management
k. Log File Management
l. Infrastructure Service Management
m. SLA Management
n. Portal, Dashboards and Reporting
o. Network Operations Center (NOC)

9.8.6.1 Network Management

The following are the requirements of the Network Management Solution. The SI is expected to provide these functionalities as a part of the overall EMS portal with seamless integration and automation.

9.8.6.1.1 Monitor each network device and port (physical and logical / virtual)

Monitoring for:

a. Availability
b. Uptime
c. Network Latency
d. Usage/Throughput, Bandwidth
e. Errors, Failures (packet losses, interface failures, network failures etc.)

9.8.6.1.2 Configure Network Devices (Routers, Firewalls, L3/L2 Switches, Load Balancers, VPN Gateways / Routers)

a. Access Control (MAC level, device level, port level, protocol level, logical level)

b. Configuration of Virtual Networks, Access Control Policies, Admission Control Policies

c. End to End configuration of physical and virtual network paths

9.8.6.1.3 Network Provisioning

a. Provision Access to required servers, applications, virtual machines, containers/micro services

b. Provision Bandwidth for servers', applications, virtual machines, containers/micro services

c. Network Addresses

9.8.6.1.4 Configuration Management

a. Manage Configuration of each device

b. Backup/Restore Device Configuration

c. Manage firmware updates / Rollbacks

9.8.6.1.5 EMS Integration

a. Support integration with incident management, service desk, help desk

b. Auto generation of tickets during errors/failures, down times or SLA violations

c. Integration with NOC

d. Integration with Single Sign on and Role based access control

e. Unified view of the network across multiple DCs, network zones and sites

9.8.6.2 Server Management

The following are the requirements of the Server Management Solution. The SI is expected to provide these functionalities as a part of the overall EMS portal with seamless integration and automation.

9.8.6.2.1 Monitor each physical, hypervisor and virtual server

Monitoring for:

a. Availability

b. Uptime

c. Utilization (CPU, Memory, Network, I/O), Workload

d. Usage / Throughput, Bandwidth

e. Log files (OS, VM)

f. Errors, Failures (hardware errors, OS errors, system errors)

9.8.6.2.2 Configure Servers (Physical Servers, Virtual Machines)

a. Access Control (MAC level, device level, port level, protocol level, logical level)

b. Network Interfaces

c. Access to Storage (local or networked)

d. Configuration of Virtual Machines, Virtual Networks, Host Level Firewalls, Access Control Policies, Admission Control Policies

9.8.6.2.3 Server Provisioning

a. Installation of Operating Systems for BareMetal servers, Virtual Machines

b. Instantiate/Spin on/off Physical or Virtual Server based on end user requests or automatically based on load/demand/SLA

c. Provision Storage for servers (local or networked)

d. Provision Access to required servers, applications, virtual machines, containers/micro services

e. Provision Bandwidth for servers', applications, virtual machines, containers/micro services on the connected virtual/physical networks

f. Provision virtual/physical interfaces, firewalls, access control policies

9.8.6.2.4 Configuration Management

a. Manage Configuration of each BareMetal, Hypervisor or Virtual servers – including OS configuration

b. Manage Backup and Restoration of Images of Physical and Virtual Servers

c. Manage firmware updates / rollbacks

9.8.6.2.5 Server Integration

Support Integration with other components via agents/agentless

a. Antivirus Solution

b. Endpoint Security, Host Intrusion Detection

c. Data Loss Prevention (DLP)

d. Backup and Recovery

e. Log File Monitoring

f. Application Monitoring

g. Server Monitoring

h. Incident Management, Asset Management, Trouble ticketing

i. SLA Management

9.8.6.2.6 EMS Integration

a. Support integration with incident management, technical help desk

b. Auto generation of tickets during errors/failures, down times or SLA violations

c. Integration with NOC

d. Integration with Single Sign on and Role based access control

e. Unified view of the physical, virtual servers across the DCs and across zones

9.8.6.3 Storage Management

The following are the requirements of the Storage Management Solution. The SI is expected to provide these functionalities as a part of the overall EMS portal with seamless integration and automation.

9.8.6.3.1 Monitor each storage cluster, device/node (data and control) and port (physical and logical / virtual) for:

a. Availability

b. Uptime

c. Capacity

d. Storage Performance - IOPS (Reads, Writes)

e. Usage / Throughput, Bandwidth

f. Errors, Failures (disk failures, packet losses, node failures, interface failures, network failures etc.)

9.8.6.3.2 Configure Storage Clusters

a. Monitoring and Data Nodes

b. Data Replication/Redundancy, Data Striping

c. Access Control (MAC level, device level, port level, protocol level, logical level)

d. Configuration of Storage Partitions, types of storage (block, file, object etc.)

9.8.6.3.3 Storage Provisioning

a. Provision required quantity and type of storage for all applications

b. Provision Access to required clients, applications, virtual machines, containers / micro services

9.8.6.3.4 Configuration Management

a. Manage Configuration of each storage cluster

b. Add, Remove Nodes, Disks in the Cluster

c. Manage Configuration of storage partitions, logical units

d. Backup/Restore storage Configuration

e. Manage firmware/storage software updates / rollbacks

9.8.6.3.5 EMS Integration

a. Support integration with incident management, technical help desk

b. Auto generation of tickets during errors/failures, down times or SLA violations

c. Integration with NOC

d. Integration with Single Sign on and Role based access control

e. Unified view of the network across multiple DCs, network zones and sites

9.8.6.4 Asset Management

The following are the requirements of the Asset Management Solution. The SI is expected to provide these functionalities as a part of the overall EMS portal with seamless integration and automation.

9.8.6.4.1 Asset Lifecycle Management

a. Track the lifecycle of the asset from arrival to disposal (purchase, arrival, provisioning, Warranty, AMC, Repair/Maintenance, Renewal Dates)

b. Track hardware and software assets

c. Support customized meta data for the asset management system

9.8.6.4.2 Track Software License Compliance and Usage

a. Support integration with RFID, Barcode Readers
b. Asset Reporting
c. Detailed Asset Reports – by vendor/manufacturer, by supplier, by brand/model, location (DC location, site)
d. Search by Asset Name, Brand, Model, Serial No, Vendor, Date of Purchase, Location etc.
e. Reports by Warranty Due, AMC Due
f. Provide alerts / notification on Warranty Due Dates / Renewals, AMC Due Dates/Renewals
g. Export reports in PDF, CSV formats

9.8.6.4.3 EMS Integration

a. Support integration with incident management, technical help desk
b. Integration with NOC
c. Integration with Single Sign on and Role based access control

9.8.6.5 Patch Management

The following are the requirements of the Patch Management Solution. The SI is expected to provide these functionalities as a part of the overall EMS portal with seamless integration and automation.

9.8.6.5.1 Patch Repository

a. Repository to Store OS, Middleware, Application Patches
b. Support RPM, MSI, ZIP, EXE and all standard Patch formats
c. Provide facility to pull patches from external repositories

9.8.6.5.2 Patch Management

a. Support Scheduling of Patches across Physical, Virtual Machines, applications, containers by date time, location
b. Optimize the bandwidth usage for patching
c. Support dependencies across patches
d. Scripting engine to create custom packages with composite patches
e. Support multiple patch distribution points
f. Integrate with Continuous Integration/Continuous Delivery (CI/CD) DevOps tools

g. Support Push and Pull of patches to/from the destination

9.8.6.5.3 Reporting

a. Tracking Patch Progress
b. Provide Patch Compliance Reports by OS, Location
c. Provide Patch history reports

9.8.6.6 Backup and Restore System

The following are the requirements of the Backup and Restore System. The SI is expected to provide these functionalities as a part of the overall EMS portal with seamless integration and automation.

9.8.6.6.1 Backup

a. Backup of File System, Databases, Object Stores
b. Backup and cloning of Bare Metal OS, Hypervisors, Virtual Machines and Containers, email storage, CRMS data stores and EMS data stores
c. Full and Incremental Backups
d. Support backup with compression
e. Support secure backup with encryption and user provided keys
f. Support Integration with backup media libraries, software defined storage

9.8.6.6.2 Scheduling and Management

a. Scheduled Backup (full, incremental)
b. Support Disk to backup media and Disk to Disk Backups
c. Support Scheduling with multiplexing multiple streams to manage the SLAs

9.8.6.6.3 Offsite Backup

a. Support Offsite Backup and Recovery

9.8.6.6.4 Automation Support

a. Support SDK, scripting to automate backup/recovery operations

9.8.6.6.5 Recovery / Restore

a. Scheduled Recovery from Backup Media to Disk and from Disk to Disk
b. Recovery from remote sites

9.8.6.7 Incident Management, Problem Management, Technical Help Desk

The following are the requirements of the Incident Management Problem Management and Technical Help Desk. The SI is expected to provide these functionalities as a part of the overall EMS portal with seamless integration and automation.

9.8.6.7.1 Trouble Ticketing

a. User Interface to log tickets and complete the process
b. Customizable workflow for the Incident management process with escalation mechanism (escalation hierarchy) and approval processes
c. Define SLA for resolving tickets and support auto escalation of the tickets based on priority and SLA
d. Support integration with other EMS tools for auto generation of tickets and either automated or manual resolution of tickets
e. Provide role-based access
f. Support multi-vendor workflow
g. Support integration with e-mail, SMS
h. Integrated with SLA management tool for real time monitoring of tickets and SLA adherence / violations

9.8.6.7.2 Technical Help Desk

a. User Interface to log technical help desk requests
b. Customizable workflow for the technical helpdesk request process with escalation mechanism (escalation hierarchy) and approval processes
c. Define SLA for resolving technical helpdesk request and support auto escalation of the requests based on priority
d. Support integration with other EMS tools for auto generation of technical helpdesk request and either automated or manual resolution of technical helpdesk request
e. Provide role-based access
f. Support multi-vendor workflow

g. Support integration with e-mail, SMS

h. Integrated with SLA management tool for real time monitoring of technical helpdesk requests

9.8.6.7.3 Reporting

a. Provide Customizable Reports

b. Provide PDF, CVS report formats

c. Provide Real-time Dashboard for reports

d. Reports Classification by SLA, Priority, Incident Type, Application, Vendor etc.

9.8.6.8 DevOps, Release Management

The following are the requirements of the DevOps, CI/CD and release management tools.

9.8.6.8.1 Release and Build

a. Integrate with the Source Code Control System

b. Provide mechanism to script the release

c. Build the relevant package (container or VM image or executable) via command line or automated process

d. Auto deploy the build in the test, pre-production environment

e. Provision release package from pre-prod to production based on the release criteria (and test criteria)

f. Should be fully integrated with the patch management solution

g. Provide for auto labelling of releases and tracking of the release train

h. Provide user interface for deploying builds/packages

i. Provide workflow or orchestration for customizing the release process

j. Provide scripting tools to script and automate build, test and deploy processes

k. Support Canary and Blue-Green Deployment processes

l. Provide a Dashboard for tracking and managing the release build process

m. Integrate with security, code scanning, vulnerability assessment tools to secure the build

n. Provide digitally signed builds/executables – integrate with the external keys

o. Provide role-based access to the system for different stakeholders

9.8.6.9 Database Activity Monitoring System (DAMS)

The following are the requirements of the Database Activity Monitoring System (DAMS). The SI is expected to provide these functionalities as a part of the overall EMS portal with seamless integration and automation.

9.8.6.9.1 Database Monitoring

a. Monitor and audit all database activities independently including SELECT transactions and privileged users' activities, without any performance impact
b. Provide customizable policy definitions
c. Securely store the database activity logs/data outside the monitored database/data store preferably in a secure, reliable isolated data store
d. Generate alerts/notifications whenever policy violations are detected, integrate with SOC and the incident management system
e. Aggregate and correlate database activities from multiple heterogeneous database management systems
f. Enforce separation of duties of database administrators, monitor the administrators' activities and prevent the manipulation or tampering of recorded activities or logs

9.8.6.9.2 Integration

a. Integrate the DAMS with all the applications accessing the corresponding databases in the solution

9.8.6.10 Application Performance Management

The following are the requirements of the Application Performance Solution. The SI is expected to provide these functionalities as a part of the overall EMS portal with seamless integration and automation.

9.8.6.10.1 Application Monitoring

a. Support non-intrusive monitoring of applications
b. Support monitoring of response times of important calls/transactions
c. For Java Virtual Machine (JVM), monitor heap usage and Garbage Collection (GC) time

d. The application monitoring should not cause any degradation in performance of the application

e. Provide visual call graphs of key transactions along with execution time of all sub transactions

f. Provide transaction correlation across multiple application instances and across multiple applications (on the same or different physical/logical machines) in the call chain

g. Provide option to enable/disable application monitoring during run time without restarting the applications

h. Support monitoring of only selective sessions for a given set of service/function calls

i. Support concurrent tracking of transaction response times of multiple applications or application instances

j. The run time libraries required for the solution should be integrated with the DevOps process

9.8.6.10.2 Dashboard and Reporting

a. Provide a visual dashboard to display call graphs of multiple applications/instances

b. Allow multiple users to track and analyse their applications concurrently in the dashboard

c. Provide role-based access to applications.

9.8.6.11 Log File Management

The following are the requirements of the Log File Management Solution. The SI is expected to provide these functionalities as a part of the overall EMS portal with seamless integration and automation.

9.8.6.11.1 Log File Management

a. Support collection of system logs, application logs across devices, applications, servers, virtual machines and containers

b. Support filtering of log levels (critical, error, warning, information) during collection

c. Support centralized collection of logs

d. Should support customizable log formats

e. Support log rotation and configurable log file sizes for rotation

f. No log data should be lost during rotation

g. Support archival of logs at the log management servers

h. Support multiple transports/protocols for moving logs from the source to the destination

9.8.6.11.2 Log Server

a. Support one or more centralized log server in a highly available mode
b. The log servers should be horizontally scalable
c. Should support correlation of data across log files and data sources
d. Support search across log files
e. Log server should support indexing for fast searches
f. Log server should support customizable analytics on log data
g. Support integration with the dashboard for displaying analytical data

9.8.6.12 Infrastructure Service Management

The following are the requirements of the Infrastructure Services Management in terms of IaaS, PaaS and SaaS services. The SI is expected to provide these functionalities as a part of the overall EMS portal with seamless integration and automation.

9.8.6.12.1 Infrastructure Provisioning

a. Support automatic provisioning of the Virtual machines, Containers based on user request via a portal or API
b. Support a configurable workflow for provisioning all the required elements for the service like storage, network, firewalls load balancers, backup, security etc.
c. Support IaaS, PaaS and SaaS Services as required

9.8.6.12.2 Service Metering

a. Support metering of service usage in terms of compute, storage, network
b. Provide Usage report service wise, businesswise and application wise (hourly, daily, weekly, monthly, quarterly)

9.8.6.13 SLA Management

The following are the requirements of the SLA Management solution. The SI is expected to provide these services as a part of the overall EMS portal with seamless integration and automation.

9.8.6.13.1 SLA Monitoring

a. Support monitoring of all SLAs defined in the RFP

b. Integrate SLA monitoring with the Dashboard

c. Support definition of thresholds of multiple levels for each SLA

d. Show SLA violations by application, services

9.8.6.13.2 SLA Dashboard Reporting

a. The dashboard should be customizable to show the required SLAs

b. The SLA dashboard should be Real time

c. The SLA dashboard should provide alerts via emails, SMS

d. The alert definition should be configurable for each SLA

e. The dashboard should indicate the service impact due to breach of any SLAs

9.8.6.13.3 Integration with Incident Management System

a. The solution shall be integrated with the Incident Management System for auto generation of tickets whenever there is an SLA violation and closure of tickets when the SLAs are back to normal

9.8.6.14 Portal, Dashboards and Reporting

9.8.6.14.1 Portal

a. The portal should provide a single sign on for all EMS services

b. The portal should provide role-based access to different users and administrators

c. The portal should support multiple EMS users concurrently

d. The portal should be highly available and should not have any single point of failure

e. The portal should provide a unified view of multiple DCs, Sites

9.8.6.14.2 Dashboard

a. The dashboard shall provide an intuitive user interface which is customizable by the end user

b. The dashboard shall provide multiple types of data visualizations like graphs (multiple types of graphs), charts (multiple types of charts), Tables with drill downs for each data set

c. The dashboard shall support search functionality by any of the common keywords relevant to the metric

9.8.6.15 Network Operations Center (NOC)

The following are the requirements of the NOC:

a. The SI shall integrate the EMS solution, dashboard with the NOC.

b. The NOC should provide a Video Wall with ability to display SLAs, Key metrics and Data from the EMS Dashboard

c. The access to the NOC should be fully secured

d. The NOC should provide a unified view of all the DC operations, IT Infrastructure and Services

e. The SI MUST provide hardware and software, install, configure, maintain and provide support of all network devices related to NOC. This also covers the connectivity of PhilSys Fixed Registration Centers to Data Centers (Primary DC, Secondary DC and DR sites). The end-to-end connectivity must always be available and reliable.

f. The SI MUST provide 24x7 infrastructure availability (up, down) and performance monitoring (utilization and health) on network components.

g. The SI MUST provide 24x7 infrastructure availability (up, down) and performance monitoring (utilization and health) on telco links and WAN connectivity for PhilSys command Center and PFRCs.

9.8.7 Transition and Migration of Data Center

The SI shall provide up to One (1) Migration services for each of the PhilSys Data Centers, namely, Primary Data Center, Secondary Data Center and Disaster Recovery Site as part of this contract.

The SI shall be responsible for the migration of the ICT equipment/rack, including but not limited to transportation, coordination, manpower, from current location to a new data center location at no additional cost, with supervision from the PSA.

The SI shall perform the following activities:

a. Prepare a detailed strategy and approach for migration including a detailed plan for migration for each of Primary Data Center, Secondary Data Center and DR Site. SI must ensure that there is minimal downtime of PhilSys Information System during migration. The detailed strategy and approach should also include potential risks during migration and steps which the SI shall take to mitigate those risks.

b. Obtain approval on the strategy and approach from the PSA.

c. Undertake transition and migration as per the approved strategy and approach.

d. Once migration is complete, the SI shall test the success of migration.

e. The SI shall prepare a report detailing the migration activities including testing and its results and submit it to the PSA.

f. The SI shall ensure no physical damage is done to the systems during the physical migration activity from one site to other.

g. The SI shall ensure there's no data loss during the migration activity.

h. The SI shall set up the complete architecture, post migration to the new facilities including inclusion of the Secondary Data Center as part of the architecture.

i. The SI shall to conduct DR drill as part of successful completion of the site set up.

10 Project Management & Governance

10.1 PhilSys Overall Governance and Program Management

While the PhilSys Registry Office (PRO) of PSA is responsible for implementation of the PhilSys, under the leadership of the National Statistician and Civil Registrar General (as the head of PSA), the overall governance and program management is summarized in Table 59.

Table 57. Summary of overall governance and program management of the PhilSys

Entity	Responsibility
PhilSys Policy and Coordination Council (PSPCC)	The PSPCC formulate policies and guidelines to ensure effective coordination and implementation of the PhilSys
Inter-Agency Committees (IAC) of the PSPCC	The IACs facilitate coordination, collaboration and consultation with members of the PSCC, specifically: • IAC on Technology: support the procurement and development of technology infrastructure, including software and hardware • IAC on Communications: support the design and implementation of the PhilSys Information and Education Campaign (IEC) to ensure sufficient awareness and approval among the public • IAC on Registration and Validation: support the development of standards, processes, guidelines and plans for registration including mass registration and steady-state • IAC on Legal Affairs: support analysis and development of laws, IRRs, and related policies • IAC on Use Cases and Authentication: support the identification and development of use cases and standards, processes, guidelines, and PhilSys credentials
PhilSys Program Management Unit (PMU)	The PMU is a special temporary unit established inside PSA to carry out and coordinate project management office functions for the overall PhilSys program (technology, operations, policies etc.), including planning, budgeting, tracking, monitoring, and advising PSA management.
Technical Working Groups (TWG) and **Special Working Groups (SWG)**	Ad-hoc TWGs and SWGs are established on an ad-hoc basis to address specific topics. They may be internal to PSA or involving other stakeholders.

10.2 SI Project Management

SI shall be responsible managing the engagement and ensure that the scope of work for the SI is met to the satisfaction of the PSA.

The Project Team of the SI shall be responsible for overall project management and monitoring.

The SI will work on a day-to-day basis with the PRO (on implementation), PMU (on project management), PSA management (on escalated issues) and, where relevant, with TWGs and SWGs (on specific technical issues). The SI may also be requested by PSA to participate and present in meetings of the PSPCC, IACs and PSA management on issues and concerns relevant to this engagement.

Bidders are expected to propose how they will be responsible for, but not limited to, the following project management and governance activities:

a. Maintaining a project management office (PMO) specific to the SI implementation
b. Preparation of a tool based detailed project plan including key project activities and milestones
c. Project Status Monitoring and Reporting
d. Defining an Escalation Matrix
e. Change Control Management
f. Project and Technical SLA Monitoring and Reporting
g. Risk and Issue Management
h. Project and Technical Governance Committees

10.2.1 Maintaining a project management office (PMO)

The SI shall set-up a Project Management Office (PMO) during the start of the project. The PMO shall remain functional until the completion or termination of the project.

The PMO shall consist of the Project Manager and other SI team members designated by the SI and representatives of the PSA (including from PRO and the PMU). Changes in the membership and composition from the SI shall undergo an approval process through the PSA.

PMO shall formally meet each week to discuss topics such as:

a. Project Progress
b. Activities undertaken and planned by the SI
c. Delays, if any – Reasons thereof and ways to make-up lost time
d. Issues and concerns
e. Performance and SLA compliance reports

f. Unresolved and escalated issues

g. Change Management - Proposed changes, if any

h. Project risks and their proposed mitigation plan

i. Discussion on submitted deliverable

j. Timelines and anticipated delay in deliverable, if any

k. Any other issues that either party wishes to add to the agenda

The SI is responsible in the operational aspects of the PMO, specifically in providing/submitting weekly statuses, minutes of the meetings, weekly/monthly/project plans and other project management instruments agreed between the SI and PSA.
The SI shall recommend PMO structure for the project implementation phase and operations and maintenance phase.

10.2.2 Preparation of a Tool-based Detailed Project plan

Upon inception of the project, the SI shall prepare a tool based detailed project plan for the engagement. The project plan shall include detailed project activities for all phases of the project, timelines for those activities, key project milestones, key resources that shall undertake the activity, etc.

A sign-off from the PSA on the project plan shall be undertaken by the SI during the Project Initiation Phase. The approved project plan shall act as a baseline for this engagement. Project status for the entire engagement shall be measured based from the project plan prepared by approved by PSA.

The project plan should include, but not limited to, the following:

a. The project breaks up into logical phases and sub-phases aligned the overall implementation timelines (see volume 1)

b. Activities making up the sub-phases and phases

c. Components in each phase with milestones

d. The milestone dates are decided by PSA in this RFP. SI cannot change any of the milestone completion dates. SI can only propose the internal task deadlines while keeping the overall end dates the same as indicated in the implementation timelines (see Section 13). SI may suggest improvement in project dates without changing the end dates of each activity

e. Key milestones and deliverables along with their dates including those related to delivery and installation of hardware and software

f. Start date and end date for each activity

g. The dependencies among activities (including dependencies on PSA)

h. Resources to be assigned to each activity

10.2.3 Project Status Monitoring and Reporting

The SI shall circulate written progress reports each week to PSA and other stakeholders.

Project status report shall include Progress against the Project Plan, status of all risks and issues, exceptions and issues along with recommended resolution etc. This project status report shall be discussed each week by during the weekly project status meeting.

Other than the planned meetings, in exceptional cases, project status meeting may be called with prior notice to the SI.

PSA reserves the right to ask the SI for the project review reports other than the weekly status review reports.

The SI shall not, without the PSA's prior written consent, divulge (directly or indirectly) any documents, data, or other confidential/sensitive information (including progress/implementation reports) to any third party.

10.2.4 Defining an Escalation Matrix

The SI will define an escalation matrix for technical and operational issues that may arise over the course of the contract implementation, with the aim of ensuring that issues are resolved efficiently and effectively, the highest escalation point being the Steering Committee (see below) or the National Statistician and Civil Registrar General. The escalation matrix will be signed off by PSA.

The SI, with sign off and approval from PSA, may enhance the escalation matrix with proper justification.

10.2.5 Change Control Management

Due to the evolving nature of the project requirements and the complexity of the project, changes may be required before, during and after rollout of the PhilSys Information System. These changes may require modification to the software, infrastructure and underlying processes and may thus have a financial impact.

The SI is required to work with the PSA to ensure that all changes are discussed, managed, and implemented in a controlled manner.

One of the requirements from the SI is to ensure that the system performs in accordance to the defined service levels. This responsibility may include the implementation of upgrades, enhancements, extensions and other changes to the software application in order to maintain and extend reliable information systems, services and service delivery mechanism. It is important that changes to the computing environment and underlying infrastructure are executed in a standardized and controlled manner in order to mitigate the risk of outages and interruptions to the services. The SI is also required to maintain a repository of knowledge (Knowledge Base) about the current and changed configurations to the system. Full documentation of system configurations is required and must be made accessible to PSA at all times.

This section describes the procedure to be followed in the event of any proposed change to the scope of work and SLAs. Such change shall, inter alia, include:

a. Requests for requirements changes (additions, deletions, modifications, deferrals) in Scope of Work (including software)

b. Requests for resolving the problems in current production systems

c. Requests for enhancements in current production systems

d. Requests for new development projects

The Change Control procedure applies to all base-lined work and activities (including development, staging, and production environments) defined in the Project Plan.

10.2.6 SLA Monitoring and Reporting

The SI shall be responsible for delivering the services described in the scope of work, as per the SLAs required from this RFP. The SI should submit an SLA compliance report defined by the implementation timelines (see volume 1). The SI shall also be responsible for providing early warning of any organizational, functional or technical changes that might affect the SI's ability to deliver the services described in the SLA. Immediate actions should be taken to mitigate the risks or issues, if any.

SLA reporting should be undertaken using automated tools. SLA reporting should be extracted from the automated logs without manual intervention. The SI shall prepare the reporting templates for SLA compliance reports and obtain sign-off from the PSA. These reports should include "actual versus target" SLA performance, a variance analysis and discussion of appropriate issues or significant events, if any.

10.2.7 Risk and Issue Management

The SI shall develop a Risk Management Plan and a risk register for the engagement. The SI shall identify project risks, analyze and prioritize the risk, identify mitigation plans and document the risks and their mitigation strategy in the risk register.

The SI must also prepare an issue management procedure to identify, track, and resolve all issues confronting the project.

The SI must prepare an issue register to document all key project issues, their impact on the engagement and their resolution plans.

The SI should periodically update the risk and issue register and present them as part of the weekly project review reports. The project risks and issues shall also be discussed with the PSA weekly PMO meetings in order to discuss and identify mitigation plans.

10.2.8 Project Governance Committees

Bidders are expected to propose the most effective and efficient project governance structure between PSA and the SI for smooth coordination, project management and implementation of the engagement, including for dispute resolution. The highest escalation/decision-making point will be the National

Statistician and Civil Registrar General. The lead technical representative of PSA will either be an Assistant National Statistician or Product Manager.

At a minimum, the proposal should include an **Architecture and Information Security Committee**. This committee will be headed by the lead technical representative of the PSA and involve equivalent-level representatives of the SI and BioSP (e.g. the principal architect and information security leads) and other relevant representatives of the Government of the Philippines (e.g. DICT and BSP), meeting every month or as decided by PSA. This committee will be tasked with the discussion and agreement of major architectural changes and decisions during the course of the implementation. An Architecture Decision Record should be maintained by this group as a minimum this record should include the following for each decision: Design decision, Context, Rationale, Implications.

11 Manpower Requirement

11.1 Guidelines for Staffing and Provisioning of Manpower

a. Implementation of PhilSys Information System is envisaged onsite at PSA premises wherein, a dedicated core team of the SI shall be stationed at the PSA's premises while the development of the system will happen in SI premises.

b. The SI shall provide a detailed staffing schedule in their Technical Proposal as per the format provided as part of this **TPF 7 of SI PBD Vol 1.**

c. The staffing schedule should also include an Organization Chart showing the proposed organization to be established by the SI for execution of the scope of work. The organization chart should clearly bring out variations to the Organization structure if any envisaged by the SI for various phases/stages of the project.

d. Detailed CVs should be provided for key profiles that will be subject to evaluation. CVs should be as per the CV format given in **TPF 6 of SI PBD Vol. 1**. Area of expertise, role and tasks assigned should be clearly identified for each of the key profiles. PSA might interact with the said resources and this interaction shall be considered in technical evaluation.

e. Key roles in the SI's team should be held only by employees of the SI at the time of the issuance of Notice to Proceed for this Project.

f. The Staffing Schedule should contain the schedule of deployment of the Key personnel (see **TPF 7 of SI PBD Vol 1.)**. It should also clearly highlight onsite and offsite effort of each profile.

g. The SI or its Sub-Contractors should provide to its employees assigned to this Project the infrastructure or other facilities required for the efficient execution of work for the Project.

11.2 Replacement of Personnel

a. The SI should to the best of its efforts, avoid any change in the organization structure and proposed manpower for execution of the scope of services or replacement of any manpower resource.

b. If the same is however unavoidable, due to circumstances such as the resource leaving the SI's organization, the SI shall promptly inform the PSA in writing, and the same shall require subsequent approval by the PSA. The SI should ensure that they adhere to the SLA for replacement of manpower as defined in this PBD.

c. In case of replacement of any manpower resource, the SI should ensure efficient knowledge transfer from the outgoing resource to the incoming resource and adequate hand-holding period and training for the incoming resource in order to maintain the continued level of service.

11.3 Removal of Personnel

a. PSA may at any time object to and request the SI to remove from the Sites any of SI's authorized representative including any employee of the SI or any person(s) deployed by SI. This may be due to for professional incompetence or negligence or for being deployed for work for which he is not suited.

b. PSA's Representative shall state to the SI in writing his reasons for any request for removal of personnel. The SI shall promptly replace any person removed with a competent substitute, and at no extra cost to the PSA.

11.4 Logistics Requirements of the Personnel

The SI shall be responsible for the deployment, transportation, accommodation and other requirements of all its employees required for the execution of the work and provision of services for all costs/charges in connection thereof.

11.5 Escalation Matrix

a. As part of the technical proposal, the SI shall provide a detailed Escalation Matrix mapping back to the SI's organizational structure proposed.

b. The Escalation Matrix should include a steering committee for expedited decision making with PSA as the head of the committee.

c. The Escalation Matrix should address key requirements stated in the Service Level Agreements for various service delivery activities and cover all major service delivery activities.

d. The triggers for escalation should be clearly identified and stated for each category of service in the Technical Proposal.

11.6 Manpower Qualification and Experience Requirement

a. The SI shall deploy well-qualified and experienced resources having in-depth knowledge and experience of the position for which they are deployed. The resources shall have to carry out the scope work in order to implement the PhilSys Information System and meet the service levels as defined in this PBD.

b. A minimum qualification and experience requirements of the key resources to be deployed along with the indicative high-level roles and responsibilities of the resources that they are expected to carry out objectively while meeting the SLA requirements. **The details of manpower profile are provided in Annex F.**

11.7 PSA's Role and Responsibility

During project duration, the PSA shall have following roles and responsibilities:

a. PSA will provide basic office amenities to the SI's personnel at its office locations for performing their part of the obligations.

b. All the facilities provided by PSA are promised to be available only for the time as agreed upon by SI and PSA as the official work time and workdays.

c. Beyond the time frame contractually agreed upon, SI will not be entitled to any of these facilities.

d. PSA will provide the following infrastructure and no other facilities beyond this scope mentioned.

   1) SI Operations Room with network connectivity

   2) WAN/LAN Connectivity, Electrical Connectivity.

e. Coordination between all the divisions/departments for providing necessary information for the study and development/customization of the necessary solution.

f. Provide necessary support such as provision of list of participants, coordination with stakeholders' participants, etc. to the SI for conducting workshops for the Stakeholder departments, if any.

g. Monitoring of overall timelines, SLAs and calculation of penalties accordingly.

h. Conducting UAT for the application solution deployed.

i. Issuing the Acceptance Certificate on successful deployment of the software application and for other components of the Scope of Work (wherever required).

j. Ensuring the PSA staff members and other stakeholders attend the training programs as per the schedule defined by SI and agreed upon by the PSA.

k. Provide approval on the deliverables of the project within agreed timelines.

12 Training

During implementation and operation of PhilSys Information System, SI shall be required to train key resources to ensure successful implementation and operations of PhilSys Information System. Following shall be responsibilities of the SI for training.

12.1 Training Needs Assessment

SI in consultation with the PSA shall identify the training required to be imparted to PSA team/ different stakeholders for successful implementation and operations of PhilSys. Both technical and support function training shall be identified by the SI and approved by the PSA. Manpower to be trained shall be identified by the PSA in consultation with the SI. For every training type the SI will provide a maximum of one batch of training with maximum of 25 participants.

Training Course Design and Pre-requisites: The SI shall conduct an onsite type of training covering both theory and practical approach. Minimum modules must include the following training needs:

Table 58. Training Needs

Test Type	Domain	Duration	Outcome
Technical Training	Biometrics Solution (To be provided in partnership with Biometric Solution Provider)	2 weeks	Hands-on understanding of the ABIS and IDMS, Software Development Kits
	Authentication (To be provided in partnership with Biometric Solution Provider)	2 weeks	Hands-on understanding of the Authentication Services, Software Development Kits and authentication Services
	Security	2 days	Understanding of security guidelines, risk, reporting and compliance. Understanding of access rights and policies, DOs and DONTs, and general awareness about cybersecurity and cyber-threats
	Security	4 weeks	Advanced knowledge of network security architecture, data Center security, threats and situation management, software security, etc.

Test Type	Domain	Duration	Outcome
	Technology	2 days	Database management, network management, server storage management, backup and replication management
	BCP	1 day	Awareness on disaster policy, disaster management and BCP
	BCP	2 weeks	Detailed knowledge about the Business Continuity Planning, Disaster Drill Management, Testing of Biometric Solution at DC Site, RTO & RPO Management and Backup & Replication Management
	Application	2 days	Understanding of application development and maintenance, testing, portals management, user acceptance, release management
	PhilSys Core Components	2 days	Understanding PhilSys Core Components, Functionalities and Features, Support Mechanism, Service Levels, etc.
	PhilSys Support Systems	3 days	Understanding PhilSys Support Systems (EMS, CPMS, PhilSys Web Portal, Mobile App, Dashboard and Analytics, etc.) Functionalities and Features, Support Mechanism, Service Levels, etc.
	SOC / NOC and Data Center Operations	5 days	Understanding SOC/NOC and Data Center operations includes hands-on activities.
Support Functions	Registration Operations	2 days	Monitoring of the continuous registration process, upkeep and maintenance of the Registration Software, maintenance of the Registration Kits, coordination with and supervision of the PFRCs, etc.
	Manual Verification	2 days	Understanding of Manual Verification, Manual Verification and Quality Checks with relevant processes, procedures, systems, etc.
	Card Management System and Card Personalization Management System	1 day	Understanding of CMS and CPMS Functionalities and Features, Support Mechanism, Service Levels, etc.
	Technical Helpdesk Support	3 days	Understanding of Call Logging, Call Forwarding, Call Resolution mechanisms, FAQs, etc.

12.2 Preparation of Training Plan

After identification of the training needs, SI shall prepare a training plan that highlights training type, target trainees, date of training, venue for training, trainer details, agenda of training etc. and the final course outline.

The SI shall cover all expenses related to the training including the venue, accommodation of trainers/resource speakers, participants, and other identified personnel, training tools and materials. If the training is outside Metro Manila, the SI shall also cover the transportation expenses.

12.3 Impart Trainings

a. The SI shall be responsible for imparting the identified training in accordance with the training plan. The SI shall also be responsible for preparation of training materials, certificates, training aids (document, audio or video), and venues (including meals) that are required for successful completion of the training. During the training, SI needs to provide copies of the relevant training material.

b. The SI has to ensure that the personnel deployed for training are properly qualified and understand the area of their training in-depth.

12.4 Ensure Training Effectiveness

a. The SI has to ensure that the training sessions held are effective and that the attendees would be able to carry on with their work efficiently. For this purpose, it is necessary that the effectiveness of training sessions is measured. The SI shall prepare a feedback form that will capture necessary parameters on measuring effectiveness of the training sessions. This form will be discussed and finalized with PSA.

b. After each training session, feedback will be sought from each of the attendees either on printed feedback forms or through a link available on the web portal. The feedback received would be reported to PSA for each training session.

c. For each training session, the SI shall categorize the feedback on a scale of 1 to 10, where 10 will denote excellent and 1 will denote unsatisfactory.

d. The training session would be considered effective only after the cumulative score of the feedback [sum of all feedback divided by number of attendees] is more than 7. In case the cumulative score of the feedback is less than seven, the SI shall undertake re-training at no additional cost.

12.5 Transition and Exit Management

a. The transition phase starts one month prior to the contractual period and total duration of the transition phase shall be two months. Knowledge transfer and transition will happen at leadership and track level.

b. The SI needs to update the Transition and Exit management on a yearly basis or earlier in case of major changes during the entire contract duration. This plan needs to be discussed and approved by the PSA.

c. The SI must undertake the following activities to ensure a successful transition:

   1) Submit a structured and detailed Transition and Exit Management plan for approval by the PSA.

   2) Update the Transition and Exit management on half-yearly basis or earlier in case of major changes during the entire contract duration.

   3) During the contract period or towards the end of the contract with SI, if any agency/ PSA's team is identified or selected for providing services related to SI's scope, the SI shall ensure satisfactory transition is made to the agency / PSA's team.

   4) Document all risk during transition stage and undertake mitigation measures to ensure smooth transition without any service disruption.

   5) Hand over the complete documentation related to the entire PhilSys Information System

   6) Hand over all AMC support related documents, credentials etc. for all OEM products supplied/maintained as part of this project.

   7) Ensure that no end of support products (software/hardware) exist at time of transition. In case any support products (software/hardware) is declared end of support, SI must replace the product at no additional cost.

   8) Hand over the list of complete inventories of all assets created for the project

   9) Give detailed walk-through and demos for the solution

   10) Hand over the entire PhilSys Information System including source code, program files, configuration files, setup files, project documentation, etc.

   11) Provide shadow support for at least three months and secondary support for further three months after the end of contract, at no additional cost to PSA

   12) Close all critical open issues as on date of exit. All other open issues as on date of Exit shall be listed and provided to PSA.SI shall be released from the project only when the successful transition is done meeting the parameters defined for successful transition.

   13) Submit a report on requirements (including infrastructure requirements) for running the Technical Helpdesk operations at least 6 months before the expiration of SI's contract. SI would also submit all manuals and other related documents to ensure that smooth transition of Technical Helpdesk services.

14) Train PSA staff on managing and running the Technical Helpdesk services at least 3 months prior to expiration of contract of the SI.

13 Implementation Schedule

For the purpose of implementation of the PhilSys Information System, two major milestones are defined:

a. **Development Phase**: Activities and Project Management till Go-Live of the PhilSys Information System

b. **Operations and Maintenance (O&M) Phase**: Activities and Project Management after Go-Live of the PhilSys Information System for the contract duration

13.1 Development Phase

a. The SI shall refer to the SI implementation timeline (see Section 13.3) for the timelines regarding the phases of development of PhilSys System Application. This development phase concerns with design, supply, built, benchmark, commission and acceptance of the PhilSys Information System.

b. During the development phase the SI is expected to deploy leadership manpower, architects, and engineers to design, build and commission the PhilSys Information System. The SI is expected to consider and deploy appropriate teams at the time of development phase.

c. The scope of work for the SI spans the complete Software Development Life Cycle from designing, developing, testing, maintaining and supporting the PhilSys Information System. SI shall work closely with PSA, or its appointed third party, during the software development to ensure successful implementation and operations of the PhilSys Information System. Implementation of PhilSys Information System is envisaged to be rolled out in the following versions:

- **PhilSys System Application Version_1:** this version is planned to be released in 120 days from Notice to Proceed. The modules included in this version are enumerated in Table 59

- **PhilSys System Application Version_2:** this version is planned to be released in 270 days from Notice to Proceed. The modules included in this version are enumerated in Table 59

- **PhilSys System Application Version_3:** this version is planned to be released in 420 days from Notice to Proceed. The modules included in this version are enumerated in Table 59

- **PhilSys System Application Version_4:** this version is planned to be released in 600 days from Notice to Proceed. The modules included in this version are enumerated in Table 59

13.2 Operation and Maintenance Phase

a. The Operation and Maintenance (O&M) phase shall commence after the Go-Live (PhilSys System Application version_4) and continue throughout the contract duration.
b. During this phase a counterpart team from the PSA will work together with the SI team. This team will correspond to the leadership team, the architect team and the business services and technical team of the SI.
c. At the end of the O&M phase, and six (6) months before the end of contractual period of the SI, knowledge transfer and transition activities shall commence, and the PSA team shall participate in the transition and knowledge transfer activity. During the phase of knowledge transfer the SI is expected to make the architects and engineers available for the purpose of transition and knowledge transfer.
d. The SI shall be responsible for Service Levels throughout the duration of the contract.

13.3 SI Implementation Timeline

Table 59. Implementation Timeline

Stage	Deliverables	Duration
Project Initiation Document (CY 2020)	• Approved project initiation document including risk analysis, project organization, deployment and delivery plan, training plan and project control. • Approved project implementation plan and system architecture. • Approved control test plan • Approved detailed functional and technical specifications (for Version_1) • Setup of Joint SI Project Management Team	30 Calendar days after issuance of Notice to Proceed
Delivery and acceptance of PhilSys Information System Application Version_1 and Hardware (CY 2020)	1. Delivery of application and hardware; and signed Certificate of Acceptance/Inspection for the following deliverables: a. Pre-Registration, b. Registration c. Uploading of registration packets d. Manual Verification System e. IAMS (Identity and Access Management) f. IDMS Integration with ABIS g. PSN Number Generation and Tokenization Management System (for PSNs and PCNs only) h. SMS and Email Solution (PSN and PhilID card issuance) i. CPMS j. Interface with PhilID card Personalization System deployed at BSP k. Central Workflow Engine for core integrations l. Record History (registration until PhilID card issuance) 2. Supply, Implementation and Commissioning of IT Hardware at Primary Data Center, Secondary and Disaster Recovery Site for Version_1 3. Approved detailed functional and technical specifications (for Version_2)	90 Calendar days after issuance of Notice to Proceed

Stage	Deliverables	Duration
Delivery and Acceptance of PhilSys Information System Application Version_2 and Hardware (CY 2021)	1. Delivery of application and hardware; and signed Certificate of Acceptance/Inspection for the following deliverables: a. PSN Generation and Tokenization Management System (for PSN tokens other than PCNs, integrated with Mobile Application and PhilSys Web Portal) b. Authentication Solution (core modules) c. SMS and Email Solution (authentication and enhancements) d. PhilSys Web Portal (core and authentication modules) e. Network Operations Center (NOC) operations (core setup and monitoring) f. Security Operations Center (SOC) operations (core setup and monitoring) g. Central Workflow Engine for incremental integrations h. Record history (authentication) 2. Supply, Implementation and Commissioning of IT Hardware at Primary Data Center, Secondary and Disaster Recovery Site for Version_2 3. Continuous Integration/Continuous Development (CI/CD) for cumulative system enhancements over previous versions/releases 4. Roll out of two (2) Priority Use Cases Application 5. Approved detailed functional and technical specifications (for Version_3)	270 Calendar days after issuance of Notice to Proceed
Delivery and Acceptance of PhilSys Information System Application Version_3 and Hardware (CY 2021)	1. Delivery of application and hardware; and signed Certificate of Acceptance/Inspection for the following deliverables: a. Authentication Solution (enhancements) b. PhilSys Web Portal (enhancements) c. NOC operations (enhancements) d. Security Operations Center (SOC) SOC operations (enhancements) e. Mobile Application f. Complete Call Center g. TSP and Relying Parties Application	420 Calendar days after issuance of Notice to Proceed

Stage	Deliverables	Duration
	h. Partner Management modules i. Central Workflow Engine for incremental integrations j. PSN Generation and Tokenization Management System (for backend systems and shared tokens) 2. Supply, Implementation and Commissioning of IT Hardware at Primary Data Center, Secondary and Disaster Recovery Site for Version_3 3. Continuous Integration/Continuous Development (CI/CD) for cumulative system enhancements over previous versions/releases. 4. Approved detailed functional and technical specifications (for Version_4)	
Delivery and Acceptance of PhilSys Information System Application Version_4 (CY 2022)	1. Delivery of application and hardware; and signed Certificate of Acceptance/Inspection for the following deliverables: a. BI and Data Analytics b. Dashboards c. Fraud engine set up d. Complete PhilSys Web Portal e. Enterprise Management System f. Payment gateway g. PhilSys Data Interoperability Service h. Benchmarking i. Commissioning and roll out of integrated full end-to-end system 2. Supply, Implementation and Commissioning of IT Hardware at Primary Data Center, Secondary and Disaster Recovery Site for Version_4 3. Continuous Integration/ Continuous Development (CI/CD) for cumulative system enhancements over previous versions/releases	600 Calendar days after issuance of Notice to Proceed
Support and Maintenance Services for PhilSys	Satisfactory quarterly evaluation report against agreed SLA on operations and maintenance of PhilSys	Jan 1, 2022 to Dec 31, 2022

Stage	Deliverables	Duration
(CY 2022)		
Support and Maintenance Services for PhilSys (CY 2023)	Satisfactory quarterly evaluation report against agreed SLA on operations and maintenance of PhilSys	Jan 1, 2023 to Dec 31, 2023
Support and Maintenance Services for PhilSys (CY 2024)	Satisfactory quarterly evaluation report against agreed SLA on operations and maintenance of PhilSys	Jan 1, 2024 to end of Contact

Maintaining up-to-date system documentation

a. During the full development lifecycle and during the operational phase, the SI will be required to maintain detailed system documentation including but not limited to:
    - Product requirements document
    - Product design document
    - UX Style Guide
    - System Interrelationship document
    - User Manual
    - FAQs
    - Technical Implementation guides
    - Service run-book
    - API specifications

b. The SI must update system documentation on the delivery of new phases of PhilSys development OR when delivering changes of fixes during any subsequent operational or maintenance operation.
c. Acceptance for SI deliverables (planned or maintenance) will be dependent on the SI completing relevant updates to system documentation.

14 Service Level Agreement

a. The Service Levels Agreement (SLA) defined for the project will specify the expected levels of service to be provided by the System Integrator (SI) to PSA. **Detailed provisions on service levels are provided in Annex G.**

b. The objectives of SLA governance model are to:

   1) Provide clear reference to service ownership, accountability, roles and responsibilities.

   2) Present a clear, concise and measurable description of service provisioning at each level.

   3) Bridge the gap between perceptions of expected service provisioning and actual service support and delivery.

c. The SLA is intended to:

   1) Make explicit and strict expectations that PSA has for performance and availability of services.

   2) Help PSA control and ensure the planned level and performance of business services.

   3) Trigger a process that brings PSA and SI's management attention to situations when any aspect of service delivery drops below an agreed upon threshold or target.

d. The performance of the services shall be measured against the SLA as detailed in Annex G.

e. The service level targets define the levels of service to be provided by the SI to PSA for the applicability period or duration of this contract, whichever is earlier, or until the stated SLA targets are amended.

f. Any degradation in the performance of the services undertaken by the SI's project team during the tenure of contract, will be subject to levy of liquidated damages against the quarterly payment. The liquidated damages mentioned in this Agreement are pre-estimate of damages likely to flow from the breach of timelines and service levels.

g. Liquidated damages will be calculated on quarterly basis.

h. The cumulative 'liquidated damages' for each quarter shall under no circumstances exceed 10% of the Planned Quarterly Payment (PQP)

i. The SI shall implement an SLA Management and Monitoring solution, configure the SLAs in the tool and enable automated monitoring and reporting of adherence to Service Levels. Manual intervention in computation of service levels should be avoided and all monitoring and measurement should be automated.

j. Any change in the SLAs during the term of Project [in terms of addition, alteration or deletion of certain parameters], would be initiated at the discretion of PSA, which would be subsequently discussed and agreed with the SI before putting the amended SLAs into effect.

k. SLA reporting reconciliation is set on a quarterly basis, with the nominated date of the last calendar date of the quarter (hereto known as cutoff).

l. SLA Performance Indicators must be embedded in the automated reporting pipeline of the identified software for Business Intelligence and Analytics System (see *Functional Requirements - Business Intelligence and Analytics System*).

m. For the purpose of transparency and auditability, all agreed SLA Performance Indicators (together with the logs, audit trail, and metadata used to automatically compute for such indicators), must be stored in a permanent and immutable storage for the duration of the Project.