



**THE GOVERNMENT OF THE DEMOCRATIC SOCIALIST REPUBLIC OF
SRI LANKA**

Ministry of Technology

**BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS
Volume 02 of 03 - Annexure 6: Transition and Exit Management
Single Stage Two Envelopes Bidding Procedure**

FOR THE

PROCUREMENT OF A MASTER SYSTEM INTEGRATOR (MSI) FOR DESIGNING, DEVELOPING, SUPPLYING, DELIVERING, INSTALLATION, IMPLEMENTING, SUPPORT AND MAINTAINING THE SOFTWARE, HARDWARE AND INFRASTRUCTURE FOR SRI LANKA UNIQUE DIGITAL IDENTITY (SL-UDI) PROJECT OF GOVERNMENT OF SRI LANKA

INVITATION FOR BIDS No: ICTA/SLUDI/IS/2022/01

May 07, 2023

Table of Contents

6.1.	Transition and Exit Strategy	3
6.1.1	Introduction	3
6.1.2	Stage-I (Implementation Stage).....	6
6.1.3	Stage-II-A (i) and (ii) (Normal Operations)	7
6.1.4	Normal Operations 2nd and 3rd year Stage-II-A (ii)	7
6.1.5	Stage-II-B (Normal Operations).....	8
6.2.	Guidelines for Knowledge Transfer	8
6.2.1	Software Solution	8
6.2.2	Hosting Infrastructure.....	11
6.2.3	Field Infrastructure	11
6.2.4	Enrolment Centres	11
6.2.5	Trainings.....	12
6.2.6	Information Security and Business Continuity.....	12
6.2.7	Support Centres (Helpdesk).....	13
6.2.8	Security and Network Operations	13
6.2.9	Business and Technical Services.....	13
6.2.10	Contract Management.....	14
6.2.11	Miscellaneous	15
6.3.	Exit Management Schedule	16
6.3.1	Purpose	16
6.3.2	Continuation Of Project.....	17
6.3.3	Cooperation and Provision Of Information	17
6.3.4	Confidential Information, Security And Data	18
6.3.5	Employees	18
6.3.6	Transfer Of Certain Agreements	19
6.3.7	Rights Of Access to Premises.....	19
6.3.8	General Obligations Of The MSI	19
6.3.9	Exit Management Plan	20

6.1. Transition and Exit Strategy

6.1.1 Introduction

In addition to selection of Master System Integrator (MSI), the ICTA is planning to engage a Managed Service Provider (MSP), a Sri Lankan Firm, for continuous enhancement, operations and maintenance of the SL-UDI systems and related processes.

Service providers responsible for implementing and operationally managing the SL-UDI framework is provided below. This reflects the high-level scope of each party involved.

a.	<p>The Master Systems Integrator (MSI) –</p> <p>An Indian firm procured through competitive procurement by GoSL, funded through the GoI grant assistance.</p>	<p>Responsible for Implementing the SL-UDI Solution, support and maintaining for implementation plus 3-years.</p>
b.	<p>The Managed Service Provider (MSP) –</p> <p>Sri Lankan firm procured through competitive procurement by GoSL.</p>	<p>Managed Service Provider for ICTA, responsible for the overall operations, audit, and governance of the SL-UDI.</p> <p>Responsible for administration, access control and operations management of the SL-UDI Framework.</p> <p>Responsible for taking over the SL-UDI MOSIP ID Framework and DRP workflow from the MSI at the end of the 1st year support time period.</p> <p>Providing Level 01 support for selected key components.</p>

Table 6.1: SL-UDI Implementation Parties

The MSP will be responsible to work along with the MSI, take operational handover from MSI after the end of go-live and take selected components as specified below from the MSI.

The Master Systems Integrator (MSI) is required to design, develop, supply, deliver, install, implement, support and maintaining the software hardware and infrastructure for SL-UDI as described in the Schedule of Requirement in volume 2. The total duration of the project is the SL-UDI framework implementation period and 3-year support and maintenance. The MSI is proposed to implement the Minimum Viable Product (MVP) of the SL-UDI framework (as Iteration 1) within 12-months, and support and maintain the SL-UDI framework for 3-years from the launch (go-live).

The SL-UDI implementation consists of 2 iterations.

- a. Iteration 1: Proposed duration 12 months from the project kick-off.
This includes 11-months for the implementation of the MVP and 1-month for the UAT (User Acceptance Testing)
- b. Iteration 2: Proposed duration 4 months from the Iteration 01 implementation completing date.
This includes 3-months for the implementation of the remaining requirement scope and 1-month for the UAT.
- c. The proposed total implementation time duration for both iterations 1 and 2 is 15 months, as depicted in Figure 6.1.

ii. Each iteration will consist of a 3-month OAT. Therefore, the Operational Acceptance (OAT) of the SL-UDI complete solution (both iteration 1 and 2) is proposed to be within 18 months from the date of project kick-off.

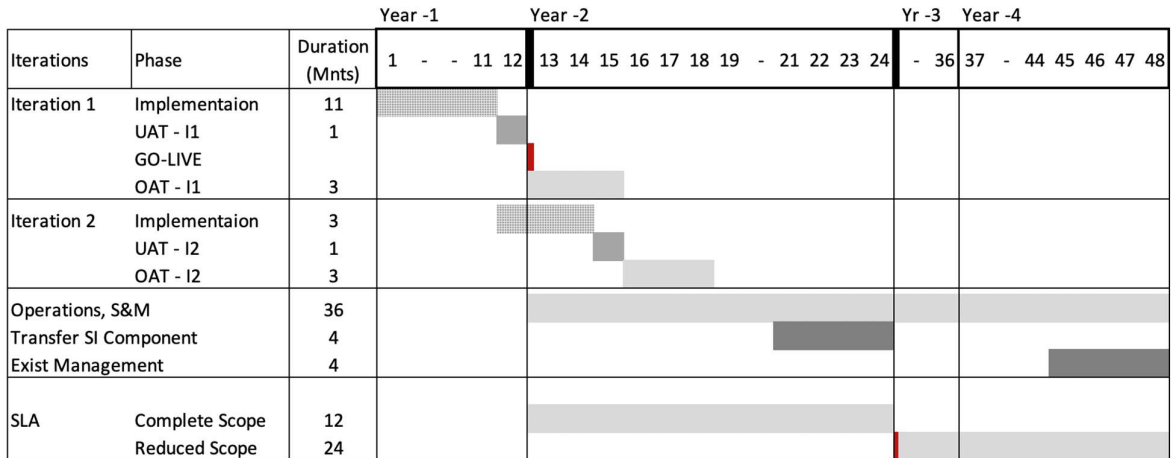


Figure 6.1: Implementation time duration

Stages	Name	Start	End	Scope
Stage-I	Implementation Stage	Project Commencement	Go-Live	
I-A	Iteration 01	Project Commencement	Completion of iteration 1	Requirement Gathering, Design, Development, Testing, and Launch, operations and support for the components in iteration 01.
I-B	Iteration 02	Completion of iteration 01	Completion of iteration 02	Rollout, operations, support, and stabilization of iteration_1 Requirement Gathering, Design, Development, Testing, and Launch for remaining SL-UDI components of iteration 02.
I-C	Acceptance and Go-Live	-	Go-Live	benchmarking, acceptance and go-live of the entire system
Stage-II	Operations Stage	Start	End	
II-A (i)	- Normal Operations - MOSIP, DRP workflow and related COTS, L1 by MSP - L2 & L3 Operations by MSI	Go-Live	End of First Year	Warranty, enhancement, operations, support, and maintenance of SI component.
II-A (ii)	Normal Operations MOSIP, DRP workflow and	End of first year	End of MSI contract	Warranty, enhancement, operations, support, and maintenance of MOSIP,

	related COTS, Refer Table 01 above) 2 nd and 3 rd year			DRP workflow and related COTS by MSP.
II-B	Normal Operations – (All other Components)	Go-Live	End of MSI contract	Warranty, enhancement, operations, support, and maintenance all other components excluding SI.

Table 6.3 : Detail Implementation description

Note: For detailed guidance on various areas, an indicative transition mechanism is provided in Section 6.2.

6.1.2 Stage-I (Implementation Stage)

Once the SL-UDI framework is in operation (from go-live) the MSI is required to provide support and maintenance services. The MSI is required to provide support services in accordance with the SLA agreement unchanged and for no additional cost.

The MSP will be selected and onboarded by ICTA within the implementation period of the MSI engagement. The MSI is expected to work closely with the MSP team in a harmonious manner and provide continuous guidance and enablement to the MSP so that the MSP team can be well-versed with all the aspects of the SL-UDI project.

At the end of this stage, there is expected to be a transition from MSI to MSP on SL-UDI MOSIP ID Framework and DRP workflow and Related COTS , further the following control aspects of the SL-UDI Framework will be entrusted with the Managed Service Provider (MSP) from the commencement of live operations (go-live).

- a. SL-UDI Administration, access control and operations management by MSP.
- b. Privilege and identity access management by MSP.
- c. Access to core data by MSP.
- d. Database activity monitor (DAM) management by MSP.
- e. Custody of the HSM to MSP.
- f. VPN and remote access managed by MSP.
- g. The SOC and NOC operations under the observation and monitoring by the MSP.
- h. Responsible for periodic reviews of related policies, processes and procedures to ensure information security and governance.

The MSI will also facilitate MSP to carry out the above activities by providing knowledge transfers and necessary operational support. The transition should start at least four months prior to the anticipated end date of this stage and shall continue till the end of this stage.

The transition needs to be meticulously planned and a detailed plan needs to be prepared by the MSI in consultation with ICTA and MSP. In this plan, a track-wise approach may be preferred to enable focussed transition of the various tracks of the project. Prior to the start of this transition, the plan should be approved by ICTA.

The MSI should submit a structured and detailed Transition and Exit Management plan along with its technical proposal. ICTA or nominated party shall evaluate all the Transition and Exit management plans submitted by various bidders. Post selection of the MSI, the transition and exit management plan shall be discussed and approved by the ICTA.

6.1.3 Stage-II-A (i) and (ii) (Normal Operations)

The MSI is expected to make a transition to the MSP for Stage-II-A (i). In this stage, the MSI is expected to provide services listed in the schedule of requirement section of the RFP, including but not limited to the following:

- (i) Software Enhancements, Updates/Upgrades, Support, etc.
- (ii) Training (Continuous Learning)
- (iii) Project Reporting
- (iv) Undertake initial troubleshooting and attempt resolution of incidents.
- (v) Responsible for reviewing and validation of assigned incident level based on service Incident Classification, applicable tiering and criteria detailed in the individual service SLA.
- (vi) Escalate and assign incident tasks to 2nd line support.
- (vii) Responsible for providing updates to Users, including communication of incident resolution and ticket closure.

6.1.4 Normal Operations 2nd and 3rd year Stage-II-A (ii)

The MSI is expected to make a hand over the operation and maintenance to the MSP. The activities related to for Stage-II-A (ii). In this stage, the MSP is expected handle the entire MOSIP, DRP workflow and related COTS.

The duration earmarked for exit management (Section 6.3), is towards the end of this stage. The MSI is expected to fully handover and transition all aspects of SL-UDI to ICTA or nominated party and MSI such that MSP are able to enhance, operate, support and maintain the entire system along with necessary support from OEMs (incl. MOSIP and OEM of ABIS and Biometric SDK), Data Centre Provider, Network Provider, etc.

6.1.5 Stage-II-B (Normal Operations)

In this stage, the MSI is expected to provide services listed in the schedule of requirement of the RFP, including but not limited to the following:

- Software Enhancements, Updates/Upgrades, Support, etc.
- Hosting Infrastructure Operations and Maintenance
- Network Infrastructure Operations and Maintenance
- Field Infrastructure (Service Centre, Spares, Troubleshooting, Maintenance, etc.)
- Training (Continuous Learning)
- Information Security and Business Continuity
- Support Centres (Contact Centre and Helpdesk)
- Business and Technical Services
- Security and Network Operations
- Warranty, Operations and Maintenance
- Project Reporting

Note: At the end of this stage, there is expected to be a transition from MSI to MSP on rest of the SL-UDI components (Except for the components which has been transferred already) and the transition activity for this should commence prior 4 months from the end of MSI contract.

6.2. Guidelines for Knowledge Transfer

This section provides broad guidelines for the Knowledge Transfer as part of the transition and exit management. The guidelines are provided for reference only and should not be considered as a definite scope of transition and/or exit management.

The Knowledge Transfer exercise will have to undergo a formal cycle of planning, preparation, execution, assessment, and closure. At each stage, the MSI will be required to work with the MSP and obtain the consent from MSP and obtain the sign-offs from the ICTA or nominated party. For assessment various methodologies may be adopted which may include reverse knowledge transfer from MSP to MSI.

6.2.1 Software Solution

The software engineering (refer Annexure-4) comprises of the delivery plan, requirements gathering, design, development & customization, testing, continuous build, change and version control, system documentation, issue identification and resolution.

- (i) Requirement Gathering: If onboarded in a timely manner, the MSP is expected to work with the MSI during the requirement gathering stage. The MSI is required to do knowledge transfer (KT) on the requirement gathering mechanism, provide information stakeholders involved in requirement gathering, KT on the requirement gathering

documents (functional requirements specification, use case design document, software requirements specifications, etc.). The MSI will be required to keep the aforementioned documents up-to-date through the course of the project.

- (ii) Design: The MSI is required to do KT on the design principles, architecture principles, high level design, low level design, traceability matrices, etc. In addition, the MSI will also be required to provide additional notes in form of design choices and rationale behind the design decisions and provisions for non-functional requirements such as future scalability, extensibility, maintainability, etc. The MSI will be required to keep the aforementioned documents up-to-date through the course of the project.
- (iii) Development and Customization: The MSI is required to document source code as per software industry best practices, maintain documentation (software/product documentation, user documentation, process documentation) as per applicable standards, setup the development environment, maintain configuration files, etc. The MSI is required to provide detailed KT on the entire aspects of software source code, associated documentation, corresponding hosting environment, development and customization related deliverables mentioned in Annexure-4, etc.
 - a. Scripts: backup procedures, manual operations done periodically, manual operations done exceptionally, documentation of third-party software or APIs, etc.
 - b. Information: Passwords, licenses, contacts, etc.
 - c. Documentation: formal documents, comments in code (esp. to clarify the intent of tricky parts), class and interaction diagrams at different levels of abstraction, etc.
 - d. Code: Enhance, build, test, and deploy code
 - e. Identify: critical components, most impacted parts by bugs, hotspots (e.g. Churn Vs Complexity), etc.
 - f. Issues: Open / Known Issues, etc.
- (iv) Testing: The MSI is required to document and maintain the test plan, test scripts, test data, testing tools, deliverables related to testing mentioned in Annexure-4, etc. as per software industry best practices, setup the testing and quality assurance environment, etc. The MSI is required to provide detailed KT on the entire aspects of different types of testing, associated documentation, corresponding hosting environment, etc.

- (v) Continuous build: The MSI will setup the DevSecOps environment including container architecture and CI/CD pipeline. The MSI is required to provide detailed KT on the entire aspects of architecture, deployment methodology, release management procedures, CI/CD pipeline, etc.
- (vi) Change and Version Control: The MSI will setup a repository for different types of artefacts with provision for version control. The MSI will maintain the change control history as part of the version control mechanism as per the industry standards and prevalent best practices. The MSI is required to provide detailed KT on methodologies/practices, configuration of repositories, etc.
- (vii) System Documentation: As part of the project, the MSI will be expected to create and maintain a wide variety of documents as per the industry standards and best practices. The MSI is required to provide detailed KT on the entire aspects of system documentation, methodology/best practices, documentation repository, etc.
- (viii) Issue identification and resolution: The MSI will develop frameworks, processes, procedures, SOPs, etc. for issue identification and resolution. The MSI needs to do the detailed KT on aforementioned documentation, all identified issues (irrespective of their status i.e. open, closed, in-process, etc.), resolution adopted for closed issues, etc. Prior to the closure of KT, the MSI is expected to close all in-process issues or open issues selected by the ICTA.
- (ix) Licenses: The MSI will be required to ensure that all the licenses required during the contract duration are valid, registered with OEM, verifiable, extendable beyond contract on payment (except the perpetual licenses), etc. All licenses purchases should be under ICTA.
- (x) Enhancements – The MSI is required to provide detailed KT on the enhancements carried out in the software. For details of the KT, please refer to all the other bulleted points given above.
- (xi) Overall – ICTA reserves the right to instruct the MSI to cover any missing knowledge transfer areas or to reconduct a knowledge transfer. ICTA will participate for the knowledge transfer sessions where it should exceed the expectation and meet the objective of the session.

6.2.2 Hosting Infrastructure

The hosting infrastructure comprises of the data centre, network service provider, etc.

- (i) **Data Centre:** The MSI will hire the colocation space in the two tier-III data centres in Sri Lanka. The MSI will setup the hosting infrastructure for the project in a caged environment within the data centres, a separate cage (within overall cage) may be planned for security components (esp. Hardware Security Module). The MSI will be required to provide detailed KT on the deliverables such as site setup, rack plan, deployment architecture, administration, environment setups, infrastructure setup (design, installation, configuration, testing, commission), etc.
- (ii) **Network:** The MSI will provide the network services (refer Volume-II for details) for the project in collaboration with the Network Service Providers (NSPs) of the country. The MSI will be required to provide detailed KT on the deliverables such as network architecture, network setup, network administration, network operations, network setup (design, installation, configuration, testing, commission), etc.

6.2.3 Field Infrastructure

The field infrastructure comprises of the biometric registration kit, service centre, spares, etc.

- (i) **Biometric Registration Kit:** The MSI will provide the biometric registration kits (refer Volume-II). The MSI will be required to provide detailed handover of the biometric registration kit. The handover will comprise of up-to-date software on enrolment software on biometric registration kit, well-maintained components of biometric registration kit, up-to-date information (master data, configurations, etc.), up-to-date end-points on the biometric registration kit, etc.
- (ii) **Service Centre:** The MSI will establish the service centre for maintenance of biometric registration kits. The MSI will operate the service centre till the end of contract and thereafter handover the same to ICTA or Nominated party.
- (iii) **Spares:** The MSI is required to maintain the spares (required to meet the SLA) in good and operational condition. The spares should be well-functioning in agreed quantity i.e. non-functional and faulty spares will have to be replaced by MSI as soon as they become non-functional or unrepairable. The MSI will be required to keep the software (firmware, MOSIP SBI, etc.) updated throughout the project.

6.2.4 Enrolment Centres

The enrolment centres will comprise of biometric registration kit (fixed and mobile), network connectivity, and other aspects of enrolment centre (design, operations, etc.)

- (i) Biometric Registration Kit: Please refer to the details provided earlier regarding biometric registration kit.
- (ii) Network Connectivity: Please refer to the details provided earlier regarding network connectivity.

6.2.5 Trainings

The MSI must repeat the trainings, mentioned in scope of work, once within the last four months of the contract period.

6.2.6 Information Security and Business Continuity

The MSI will implement the setup processes and procedures, security components, and maintain security standards.

- (i) Processes and procedures: The MSI will setup the processes and procedures and will conduct a detailed KT on them to the MSP.
- (ii) Security Components: The MSI will implement the security components and will conduct a detailed KT to the MSP, this will include architectures, manuals, configuration, etc.
- (iii) Security Standards: The MSI shall be responsible for development, documentation, implementation, and maintenance of minimum baseline security standards. The MSI shall develop, implement, and maintain version-wise hardening standards for all IT infrastructure while referencing Center for Internet Security (CIS) benchmarking or vendor specifications for hardening. The MSI will do a detailed KT to the MSP.
- (iv) Business Continuity: The MSI will setup and operationalize the process, maintain the RPO & RTO, setup and operationalize the backup strategy, maintain the HSM encryption keys, maintain the VPN access, setup and operationalize the disaster recovery strategy and procedures, and conducting the disaster recovery drills. The MSI will do a detailed KT of them to the MSP, and will ensure the disaster recovery mechanism are detailed, fully functional, and well tested.
- (v) Secure Keys: The MSI will handover to ICTA the necessary encryption and master keys in a manner which the MSP can continue to the operate the system, reuse (retrieve and/or decrypt) necessary information without requiring the intervention of MSI. As explained in the previous section.

6.2.7 Support Centres (Helpdesk)

The MSI will establish and operate the helpdesk.

- (i) Helpdesk: The helpdesk will comprise of the helpdesk solution, IT and Non-IT equipment, FAQs, SOPs, manpower, etc. The MSI will provide the same and will keep the same up-to-date throughout the project, and provide a detailed KT for the same comprising of all the aspects of the helpdesk. The MSI will be required to provide detailed KT on the deliverables such as installation, configuration, administration, and operations, and among other Incident management, escalations, BCP-DR, etc

MSI shall be responsible for setting up IT helpdesk and maintaining it for entire contract duration. At least 6 months before the expiration of MSI's contract, MSI should submit a report on requirements (including infrastructure requirements) for running the IT helpdesk and contact centre operations. MSI would also submit all manuals and other related documents to ensure that smooth transition of IT helpdesk and contact centre services.

MSI shall be responsible for installation and configuration of items procured by ICTA/DRP, as per the report of MSI.

MSI will also be responsible for training of staff for handling IT help desk.

6.2.8 Security and Network Operations

The MSI will do a detailed KT of the security and network operations.

- Network Operations Centre (NOC): The MSI will be required to provide detailed KT on the deliverables such as installation, configuration, administration and operations, among other : Incident management, escalations, BCP-DR , , etc.
- Security Operations Center (SOC): The MSI will be required to provide detailed KT on the deliverables such as installation, configuration, administration and Operations among other : Incident management, escalations, BCP-DR , , etc.

6.2.9 Business and Technical Services

The MSI will Conduct detailed KT of the business and technical services to the MSP.

- (i) Business Services: The MSI is required conduct a KT on the impact assessment, enrolment services, authentication services, ecosystem partner management, authentication service management, manual adjudication, enrolment officer certification program etc. The MSI will be required to prepare, keep the documents (such as design document, agreements, FAQs, SOPs, processes, procedures, manuals, training & certification content, etc.) up-to-date through the course of the project, and do the detailed KT for the same to MSP.

- (ii) **Technical Services:** The MSI is required to conduct KT for asset management, cell management, field network management, IP address management, software management, SMS services, payment gateway services, biometric solution management, and biometric device audit & certifications etc. The MSI will be required to prepare, keep the documents (such as design document, FAQs, SOPs, processes, procedures, manuals, etc.) up-to-date through the course of the project, and do the detailed KT for the same to MSP.

6.2.10 Contract Management

The MSI is expected to sign the contract with the Service Providers (Data Centre, Network, OEMs, etc.) in such a manner wherein the components can be transitioned in the name of ICTA or nominated party with provision to continue the services beyond the contract duration on same terms and conditions (including commercials, services, support, etc.).

The contract between the MSI and Service Providers should include provisions for contract transition, contract renewal/extension, infrastructure scaling, support services, single point of contact, escalation matrix, detailed roles and responsibilities of parties, services levels, payment terms, bill of material, item-wise unit cost, inclusion, exclusions, etc.

For the purpose of clarity, the indicative details are provided below. However, MSI should prepare a detailed plan such that there are no issues in the contractual handover from MSI to ICTA (or its representatives).

- (i) **Data Centre (DC and DR):** At the end of contract, ICTA or nominated party may want to continue the deployment of SL-UDI systems in the data centres hired by the MSI. The MSI should provision for adequate space in the data centres in such a manner to allow for gradual future expansion. The MSI through Data Centre Provider should ensure provisions for physical security, robust and spacious civil setup, reliable and consistent electrical setup (with power backup), and other industry standard facilities. The Data Centre Provider should allow all major network service providers to terminate their connection in their data centre premises proposed for this project.
- (ii) **IT Infrastructure:** The IT Infrastructure (servers, storage, enrolment kit, etc.) will be procured by MSI through multiple OEMs (including product warranty). ICTA will continue to utilize the IT Infrastructure beyond the MSI's contract. In such situation, the MSP will be required to provide the annual maintenance services for the aforementioned products. The agreement (or work order, purchase order, etc.) between MSI and OEM, should allow for such annual maintenance contract services to be provided by MSP. In case parts are required for product, the OEM should maintain the same. For scaling of infrastructure, ICTA should not be bound to procure additional infrastructure from same OEM. For replacement of unrepairable product, the OEM should offer either same or better product meeting the specifications specified in the RFP (or as amended in the service order).

- (iii) **Software:** The Software Infrastructure (system software, application software, etc.) will be procured by MSI through multiple OEMs (including product warranty). ICTA will continue to utilize the Software Infrastructure beyond the MSI's contract. Wherever possible, the perpetual product should be offered as part of the MSI. In such situation, the MSP will be required to provide the annual maintenance support services for the aforementioned products. The agreement (or work order, purchase order, etc.) between MSI and OEM, should allow for such annual maintenance support services to be provided by MSP. Wherever enterprise support as well as community edition support is available, for the period beyond MSI contract, the ICTA should be able to choose the suitable support at its own discretion. For scaling of software, ICTA should not be bound to procure additional licenses for same product. Wherever support is available through multiple agencies, ICTA should be able to choose the support agency at its own discretion.
- (iv) **Information Security and Business Continuity:** For security hardware and security software components, please refer to respective bulleted points above.
- (v) **Network:** The network connectivity will be procured by MSI through network service providers and these connections should be scalable. The ICTA will continue to utilize the network beyond the MSI's contract. The ICTA may choose to provide the network connectivity should through same or different network service provider.

6.2.11 Miscellaneous

The MSI must undertake the following activities to ensure a successful transition:

- (i) MSI shall hand over the complete documentation related to the entire SL-UDI Information System to ICTA or nominated agency.
- (ii) All risk during transition stage shall be properly documented by MSI and mitigation measures should be undertaken so as to ensure smooth transition without any service disruption.
- (iii) MSI shall handover all Annual Maintenance Contract (AMC) & Annual Technical Support (ATS) support related documents, credentials, contact details etc. for all OEM products supplied/maintained as part of this project.
- (iv) The MSI must ensure that no end of support products (software/hardware) exist at time of transition. In case any support products (software/hardware) are declared end of support, MSI must replace the product at no additional cost.
- (v) MSI shall handover the list of complete inventory of all assets created for the project.

- (vi) MSI shall conduct detective maintenance, preventive maintenance, corrective maintenance, performance tuning, and other such activities necessary to ensure that the entire system can operate with minimum intervention.
- (vii) MSI shall give detailed walk-through and demos for the solution.
- (viii) MSI to hand-over the entire SL-UDI Solution including source code (working condition), program files, dependencies/libraries, configuration files, setup files, project documentation, necessary intellectual property rights (use, modify/enhance, update, upgrade), etc. this should be accepted by ICTA and nominated party.
- (ix) MSI shall 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 ICTA.
- (x) MSI shall be released from the project responsibilities defined by ICTA only when the successful transition is done meeting the parameters defined for successful transition.
- (xi) MSI Shall ensure that all on going CR's are completed as per the agreed timelines.

6.3. Exit Management Schedule

6.3.1 Purpose

- a) This Schedule sets out the provisions which will apply three (3) months prior to expiry of the Term of the Agreement or from the effective date of termination of the Agreement. In the case of termination of any part of the Agreement or Services, the provisions of this Schedule shall, mutatis mutandis, apply to the part of Agreement or Services terminated.
- b) In this Schedule, the term 'MSP' shall mean any third party that ICTA or its nominated agencies appoint to replace the MSI upon expiry of the Term or earlier termination of this Agreement to undertake the Services or part thereof;
- c) The MSI shall ensure that its respective associated entities, subcontractors, MSIs carry out their respective obligations set out in this Exit Management Schedule.

6.3.2 Continuation Of Project

- a) In case of the Agreement being terminated by ICTA, ICTA reserves the right to ask the MSI to continue running the project operations for a period of 3 months after termination orders are issued and the MSI shall be obliged to provide such services for such period without any additional cost and expense to ICTA and without any impediment in the quality of services (measured against the target service levels defined in the Service Level Agreement of the RFP).
- b) The MSI will pass on to ICTA and/or to the MSP, the subsisting rights in any licensed products on terms not less favourable to ICTA/MSP, than that enjoyed by the MSI.

6.3.3 Cooperation and Provision Of Information

- a) During the exit management period:
 - i. The MSI will allow ICTA or its nominated agency access to information reasonably required to define the then current mode of operation associated with the provision of the Services to enable ICTA to assess the existing services being delivered;
 - ii. The MSI, on reasonable request by ICTA, shall promptly provide access to and copies (hard and soft copies as deemed necessary by ICTA) of all information held or controlled by the MSI which it has prepared or maintained in accordance with this Agreement relating to any material aspect of the Services (whether provided by the MSI or subcontractors appointed by the MSI). ICTA shall be entitled to copy of all such information. Such information shall include details pertaining to the services rendered and other performance data. The MSI shall permit ICTA and/or its nominated agencies to have reasonable access to the employees engaged for providing services and facilities as reasonably required by ICTA to understand the methods of delivery of the services employed by the MSI and to assist appropriate knowledge transfer.
- b) During the exit management period, the MSP shall submit periodic reports on the progress of the transition with ICTA and the MSI. The MSI shall ensure that any issues and gaps highlighted in such reports shall be resolved to the satisfaction of ICTA.

6.3.4 Confidential Information, Security And Data

- a) The MSI will promptly on the commencement of the exit management period supply to ICTA or its nominated agency the following:
 - (i). information relating to the current services rendered and customer and performance data relating to the performance of sub-contractors in relation to the services;
 - (ii). documentation relating to Project’s Intellectual Property Rights;
 - (iii). documentation relating to sub-contractors;
 - (iv). all current and updated data as is reasonably required for purposes of ICTA or its nominated agencies transitioning the services to its MSP in a readily available format nominated by ICTA and/or its nominated agency;
 - (v) all other information (including but not limited to documents, records, and agreements) relating to the services reasonably necessary to enable ICTA or its nominated agencies, or its MSP to carry out due diligence in order to transition the provision of the Services to ICTA or its nominated agencies, or MSP (as the case may be).
- b) Before the expiry of the exit management period, the MSI shall deliver to ICTA or its nominated agency all new or up-dated materials from the categories set out above (or any other information and data requested by ICTA) and shall not retain any copies thereof, except that the MSI may be permitted to retain one copy of such materials for archival purposes only as approved by ICTA.
- c) On completion of the exit management period, the MSI shall delete all confidential information and data from the MSI’s system and provide a certificate to ICTA stating the completion of deletion of all such data and information. (Note: The MSI’s system means the assets of MSI which the MSI is expected to take back at the end of project e.g. desktop/laptop of MSI manpower, etc.).

6.3.5 Employees

Promptly, on reasonable request at any time during the exit management period, the MSI shall, subject to Applicable Laws, restraints and regulations (including in particular those

relating to privacy) provide to ICTA or its nominated agency a list of all employees (with job titles and contact information) of the MSI and its sub-contractor dedicated to providing the services at the commencement of the exit management period.

6.3.6 *Transfer Of Certain Agreements*

On request by ICTA or its nominated agency the MSI shall effect such assignments, transfers, licences and sub-licences as ICTA may require in favour of ICTA or its nominated agencies or its MSP in relation to any equipment lease, maintenance or service provision agreement between the MSI and third party lessors, MSIs, and which are related to the services and reasonably necessary for the carrying out of replacement services by ICTA or its nominated agency or its MSP.

6.3.7 *Rights Of Access to Premises*

- a) At any time during the exit management period, where Assets are located at the MSI's premises, the MSI will be obliged to give reasonable rights of access to (or, in the case of Assets located on a third party's premises, procure reasonable rights of access to) ICTA or its nominated agency and/or MSP in order to make an inventory of the Assets.
- b) The MSI shall also give ICTA or its nominated agency, or any MSP right of reasonable access to the MSI's premises rights of access to relevant third party premises during the exit management period and for such period of time following termination or expiry of the Agreement as is reasonably necessary to migrate the services to ICTA or its nominated agency, or MSP.

6.3.8 *General Obligations Of The MSI*

- a) The MSI shall provide all such information as may reasonably be necessary to effect as seamless handover as practicable in the circumstances to ICTA or its nominated agency or its MSP and which the MSI has in its possession or control at any time during the exit management period.
- b) For the purposes of this Schedule, anything in the possession or control of any MSI, associated entity, or sub-contractor is deemed to be in the possession or control of the MSI.

- c) The MSI shall commit adequate resources to comply with its obligations under this Exit Management Schedule.

6.3.9 Exit Management Plan

- a) The MSI shall provide to ICTA or its nominated agency with a recommended exit management plan ("Exit Management Plan") which shall deal with at least the following aspects of exit management in relation to the Agreement as a whole and in relation to the various phases of the Project:
 - (i). a detailed program of the transfer process that could be used in conjunction with a MSP including details of the means to be used to ensure continuing provision of the services throughout the transfer process or until the cessation of the services and of the management structure to be used during the transfer;
 - (ii). plans for the communication with such of the MSI's sub-contractors, staff, suppliers, customers and any related third party as are necessary to avoid any material detrimental impact on ICTA's operations as a result of undertaking the transfer;
 - (iii). (if applicable) proposed arrangements for the segregation of the MSI's networks from the networks employed by ICTA and identification of specific security tasks necessary at termination;
 - (iv). Plans for provision of contingent support to ICTA, and MSP for a reasonable period after transfer.
- b) The MSI shall re-draft the Exit Management Plan every three (3) months thereafter to ensure that it is kept relevant and up to date.
- c) Each Exit Management Plan shall be presented by the MSI to and approved by ICTA or its nominated agencies.
- d) The terms of payment as stated in the Terms of Payment Schedule include the costs of the MSI complying with its obligations under this Schedule.
- e) In the event of termination of the Agreement/ Services or any part thereof, or 3 months prior to expiry of the Term of the Agreement, each Party shall comply with the Exit Management Plan envisaged in this Schedule.

- f) During the exit management period, the MSI shall use its best efforts to deliver the services.
- g) Payments during the Exit Management period shall be made in accordance with the Terms of Payment Schedule and the express provisions of the Agreement. However, the MSI shall, within 30 days of commencement of the exit management period, submit a complete, accurate and up to date account of (a) all payments made by ICTA till the effective date of commencement of the exit management period to the MSI; (b) all payments that are due and payable to the MSI by ICTA till the effective date of commencement of the exit management period; and (c) all payments that may be payable by ICTA to the MSI till the effective date of completion of the exit management period.
- h) This Exit Management plan shall be furnished in writing to ICTA or its nominated agencies within 90 days from the Effective Date of this Agreement.