THE GOVERNMENT OF THE DEMOCRATIC SOCIALIST REPUBLIC OF SRI LANKA

Ministry of Technology

BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS

Volume 02 of 03 - Annexure 9: Service Levels

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

9.1 Introduction for the SLA

The aim of this agreement is to provide a basis for close co-operation between the Employer and the Master System Integrator (MSI) for support and maintenance services to be provided by the MSI, thereby ensuring a timely and efficient support service is available.

This agreement is contingent upon each party knowing and fulfilling their responsibilities and generating an environment conducive to the achievement and maintenance of targeted service levels.

This section details the expected service levels for the services to be provided by the MSI. MSI service performance shall be measured against the Service Levels detailed in this section. MSI will be responsible to comply with the listed Service Levels throughout the duration of the contract.

9.1.1 Objectives of Service Level Agreements

(i) Provide clear reference to service ownership, accountability, roles and/or responsibilities

(ii) Present a clear, concise and measurable description of service provisioning at each level

(iii) Match perceptions of expected service provisioning with actual service support and delivery.

(iv) To create an environment conducive to a co-operative relationship between Employer, MSI and Employer's representatives (government organizations) to ensure the effective support of all end users.

(v) To document the responsibilities of all parties taking part in the Agreement.

(vi) To define the commencement of the agreement, its initial term, and the provision for reviews.

(vii) To define in detail the service to be delivered by each party and the level of service expected, thereby reducing the risk of misunderstandings.

(viii) To institute a formal system of objective service level monitoring ensuring that reviews of the agreement is based on factual data.

(ix) To provide a common understanding of service requirements/capabilities and of the principals involved in the measurement of service levels.

(x) To provide for all parties to the Service Level Agreement a single, easily referenced document which caters for all objectives as listed above.

9.1.2 Service Level Consideration

This section details the considerations that have been adopted in preparing the Service Levels:

i. Uniform approach to interpret Service Levels has been adopted and it will be based on coherent reading of Service Levels in-line with the Scope of Work stipulated in the RFP document.

ii. The Service Levels, with MSI, defined for implementation activities are applicable from the date of signing of contract, or effective date of the contract, whichever is earlier,

iii. The Service Levels defined for Operations are applicable from the date of Go-Live.

iv. Changes in the Service Levels may be discussed as per Service Levels change control mechanism (refer 9.1.5 SLA Change Control)

v. MSI would be responsible for the overall Service Levels for delivery of all components and services as per the requirement of the project as specified in Volume 2.

vi. Any change in the team of the MSI during implementation activities and operations activities will be governed by the Service Levels associated with Team Deployment category as detailed in the service levels.

vii. Metrics of all the Service Levels are within the MSI's control and are easily measurable.

viii. From the start of project, the MSI shall deploy automated and transparent tools for the measurement and reporting of Service Levels. The MSI will be responsible for customizing, deploying and maintenance of tool, however SL-UDI will have the control of the tool for measuring the Service Levels through different reports

9.1.3 Service Level Monitoring

The success of Service Level Agreements (SLA) depends fundamentally on the ability to measure performance comprehensively and accurately so that credible and reliable information can be provided to customers and support areas on the service provided.

For transparent and accurate monitoring of service levels, it is important that the information capture is automated as far as possible. Thus, the MSI will be responsible to identify (with detailed justifications) service levels for which information cannot be collected in an automated manner and obtain the sign-off on such list of service levels. For service levels identified for automated data collection, the MSI will be responsible for configuring the SLA tool in such a manner that the accurate information to monitor service levels is captured in an automated fashion. Wherever such automated capture of information is not feasible, the MSI shall provision an approval workflow within the SLA tool. The MSI will be responsible to enter the actual performance for each such service level along with necessary supporting evidence of the same. In some cases, the ICTA may be responsible for entering the details of actual performance on service levels (along with supporting documents), the SLA tool may be configured to cater to such requirements.

Service factors must be meaningful, measurable, and monitored constantly. Actual levels of service are to be compared with agreed target levels on a regular basis by both ICTA and MSI. In the event of a discrepancy between actual and targeted service levels the MSI is expected to identify and resolve the reason(s) for any discrepancies.

The performance of each service level will be coded as red (needs improvement), amber (needs attention) and green (satisfactory). In the report submitted by MSI, each service level will be dealt in the following manner:

(i) **Green** (Satisfactory): The report will contain the best practices carried out to ensure service level performance, and action items to ensuring continuity of good performance

(ii) **Amber (needs attention):** The report will contain the best practices, root cause analysis, and action items to ensure performance improves and does not get slipped.

(iii) **Red (needs improvement)**: The report will contain the best practices, root cause analysis, and action items to ensure performance improves substantially to meet the expectations.

Service level monitoring will be performed by ICTA or nominated partner where necessary reports and monitoring dashboards should be provided by the MSI. The reports will be produced as and when required and forwarded to the ICTA.

(i) Support monitoring of all SLAs defined in the RFP.

(ii) Integrate SLA monitoring with the Dashboard.

(iii) Support definition of thresholds of multiple levels for each SLA.

(iv) Show SLA violations by application, services, infrastructure.

(v) The dashboard should be customizable to show the required SLAs.

(vi) The SLA dashboard should be Real time.

(vii) The SLA dashboard should provide alerts via emails, SMS.

(viii) The alert definition should be configurable for each SLA.

(ix) The dashboard should indicate the service impact due to breach of any SLAs.

(x) The SL-UDI system 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.

9.1.4 Management of Service Levels

i. **Responsibility of MSI:** MSI is responsible for delivering the services described in the Schedule of Requirement in this RFP, as per the Service Levels and performance measures stipulated this section. MSI is also responsible for:

a) Periodic Reporting of Service Levels as per Reporting Procedure mentioned below.

b) Reporting of risks and issues with mitigation strategies to the ICTA as per procedure mentioned below.

c) Immediate action to mitigate the identified risks and issues.

ii. **Reporting Procedure**

a) Service Levels reporting should be done using an automated tool. To the extent possible Service Levels reporting should be based on automated logs with minimal manual intervention. Well-defined processes should be implemented for those Service Levels that require manual intervention for measurement and reporting.

b) The Service Levels and performance measurement reports should be submitted in an agreed upon format.

c) The reports should include “actual versus target” Service Levels, a variance analysis and discussion of appropriate issues or significant events.

iii. **Procedure for Mitigation of Issues**

a) A pre-defined exception handling process will be used for situations where issues are not resolved at project team level.

b) ICTA or MSI may raise an issue by documenting the business or technical problem, providing an objective summary of the issue under consideration.

c) ICTA shall determine which project committee or executive level should logically be involved in resolution.

d) A meeting shall be conducted to resolve the issue in a timely manner.

e) Thereafter, Management of ICTA and MSI will examine the report of the project committee and agree on a temporary or permanent solution for the issue under consideration. The MSI will then communicate the resolution to all concerned teams.

9.1.5 SLA Change Control

i. It is understood that the Service Levels may be required to undergo amendments with evolution of ICTA’s business needs during the course of the contract period. ICTA or the MSI can request a change in Service Levels. This section defines the following procedures required for amending the Service Levels and bring new Service Levels into effect:

a) SLA Change Process

b) Service Levels for a New Service, Optional Service or Additional Services

c) SLA Version Control

ii. **SLA Change Process:** The parties may amend the Service Levels by mutual agreement in accordance with the process described below:

a) Either party can review the Service Levels and initiate amendment request. After the joint review of change requirements, the discussion on changes of Service Levels shall be taken up in monthly review meetings or technical committee meeting. Following actions might result out of discussion:

- Add to, delete or change the Services to be measured and the corresponding Service Levels to reflect changes in SL-UDI operations; and
- Improve the existing Service Levels, where warranted, to reflect operational or technical improvements.

b) With respect to a New Service, Optional Service or Additional Services, MSI and ICTA will establish initial Service Levels following full implementation of such Services which will come into effect within the initial 90-day period of MSI providing such New Service, Optional Service or Additional Services. To the extent appropriate, such initial Service Levels will be the same as or similar to existing Service Levels for the same or similar Services. During these 90 days, MSI and ICTA will conduct a process for Measurement and Validation of Service Levels to validate the initial Service Levels and agree upon the final Service Levels. The finalized service levels shall be documented and implemented in accordance with the Service Levels version control process described below.

c) All negotiated and agreed Service Level changes will require changing the version control number of Service Level Agreement. Service Levels shall be documented for all new services, optional services and additional services following the completion of measurement and validation process for such services.

9.1.6 Service Levels Categories

The Service Levels have been grouped in the following categories:

(i) Service Levels for Implementation Services

(ii) Service Levels for Manpower

(iii) Service Level for Biometric Registration Kits

(iv) Service Level for Biometric Solution

(v) Service Levels for Application and Software

(vi) Service Level for Infrastructure

(vii) Service Levels for Business and Technical Services

(viii) Service Levels for Project Management Services

(ix) Service Levels for Security Services

**Note: For the components that are mentioned in the RFP to be transferred to MSP from the start of the 2nd support year will be excluded from the MSI's SLA commitment.*

The below are definitions specific to the SLA.

(i) **“Enrolment Transactions”** The transaction related to the successful de-duplication check to establish if there exist any duplicate(s) for one subject to be enrolled.

(ii) **“False Positive Identification”** A term applying to de-duplication transactions only. An incorrect decision of a biometric system that an applicant for a UID has previously been enrolled in the system, when in fact they have not.

(iii) **"False Positive Identification Rate (FPIR)"** A term applying to de-duplication transactions only. The ratio of number of false positive identification decisions to the total number of enrolment transactions by unenrolled individuals. This rate is expected to depend upon the size of the enrolled database and the database binning/partitioning used.

(iv) **"False Negative Identification"** A term applying to de-duplication transactions only. An incorrect decision of a biometric system that an applicant for a UID, making no attempt to avoid recognition, has not previously been enrolled in the system, when in fact they have. This failure to match might be caused by any algorithm in use by the system (segmentation, comparison, binning, quality, etc.).

(v) **"False Negative Identification Rate (FNIR)"** A term applying to de-duplication transactions only. The ratio of number of false negative identification decisions to the total number of enrolment transactions by enrolled individuals. This rate is expected to depend upon the database binning/partitioning used to meet throughput requirements.

(vi) As no failure-to-enrol decisions will be permitted for residents with any of the 12 biometrics available, failure-to-enrol rates are presumed to be zero and will not be considered in computing the false negative identification rate. Data from residents with none of the 12 biometrics will be exempted from the calculation of this rate.

(vii) **"False Acceptance"** A term applying to authentication transactions only. The decision of a biometric system that submitted biometric samples match enrolment data from a different data subject.

(viii) **"False Match Rate (FMR)"** A term applying to authentication transactions only. The ratio of number of verification transactions conducted by data subjects resulting in a false match to the total number of transactions. The definition of "transaction" shall be given by the respondent, with the provision that the same definition is used in determining "False Match Rate".

(ix) **"False Rejection"** A term applying to authentication transactions only. The decision of a biometric system that submitted biometric samples do not match enrolment data of the same data subject.

(x) **"False Non Match Rate (FNMR)"** A term applying to authentication transactions only. The ratio of number of authentication transactions conducted by data subjects resulting in a false non match to the total number of transactions. The definition of "transaction" shall be given by the respondent, with the provision that the same definition is used in determining "False Non Match Rate".

(xi) **"Successful De-Duplication"** means assurance through biometric comparisons that no enrolled person has been assigned more than one Unique Identity Number.

(xii) **"Enrolment Transactions"** mean the transaction to perform de-duplication check in order to establish if there exists any duplicate(s) for the subject to be enrolled.

(xiii) **"Allotted Enrolment Transactions"** mean the transaction allocated to a Biometric Solution to perform de-duplication in order to check if there exist any duplicate(s) for the subject being enrolled.

(xiv) **"Total Cost"** refers to the "Contract Value" defined in Payment Schedule in Volume-2.

(xv) "**Quarterly Revenue (QR)**" refers to Quarterly Amount Payable (definition given in Payment Schedule of Volume-2)

9.1.7 Performance and Liquidated Damages

This section details the Performance and Liquidated Damages applicable on MSI, as a result of not complying with the Service Levels as stipulated in this RFP.

i. A quarterly performance evaluation will be undertaken using the monthly reporting periods of that respective quarter.

ii. Where SLA measurement is done on a monthly basis, sum of Liquidated Damages associated with each month shall apply for the quarter.

iii. Performance Liquidated Damages shall be levied for not meeting each SLA.

iv. Based on the non-performance and its business impact, ICTA shall invoke the severity level as defined below:

Severity Level for non-compliance	Liquidated Damages as a percentage of total contract value
9	1.50% and ICTA may decide to issue Notice of Termination to MSI
8	1.25%
7	1.00%
6	0.50%
5	0.25%
4	0.125%
3	0.10%
2	0.05%
1	0.025%

Table 9.2 : Performance and Liquidated Damages

v. For implementation phase, the Cumulative Liquidated Damages for the Service Levels applicable in the Implementation Phase shall be capped to 10% of the Total Cost. In case the penalty exceeds 10% of the Total Cost, ICTA reserves the right to issue a notice of termination of contract to the MSI.

vi. For operations and maintenance phase, the Cumulative Liquidated Damages for each quarter under no circumstances shall exceed 10% of the fee payable for that quarter.

- If on Performance evaluation, it is found that the MSI has not met a measurement parameter for two consecutive quarters the same shall result in doubling the Liquidated Damages percentage of that measurement parameter.
- If on Performance evaluation it is realized that liquated damages deducted for each of the 3 consecutive quarters is equal to 10% of the fee payable for that quarter, ICTA reserves the right to issue a notice of termination of contract to the MSI.

9.2 Service Levels for Implementation Services

i. The Implementation Services comprise of activities relating to the implementation work by MSI. Service Levels related to Operation Services are detailed in Section 9.6 Service Levels for Application and Software Services of this document. The Phase wise implementation plan/ implementation roadmap is detailed in the document

   - Activation of Service Levels responsibility by MSI: The Service Levels specified in this section shall be activated from the date of signing of the contract.

De-activation of Service Levels responsibility by MSI: These Service Levels shall be de-activated from the date all service level milestones under this category are achieved by the MSI.

#	Category/ Component	Metric Type	Formula / Definition	Period and Time of Measurement	Target	Severity level
1	Setting up of Project Management Office, Kick-off meeting and commencement of work	Delay	Delay in number of calendar days from the date of signing of the contract Kick-off meeting within 7 calendar days, and Setting up of the Project Management Office within 30 days	One-time at the start of the project	Delay of <=14 days	0
					Delay >=15 days and <=30 days	3
					Delay >=31 days <=45 days	5
					Delay >=45 days	9

#	Category/ Component	Metric Type	Formula / Definition	Period and Time of Measurement	Target	Severity level
2	Timely achievement of milestones (all items of implementation schedule excluding Launch of Release_1 components, Launch of Release_2 Components, and Biometric Benchmarking and Acceptance)	Delay	Measured as the difference between the planned date for the milestone and the actual date of its completion in terms of delay in number of calendar days	Milestone based Measurement	Delay of <=14 days	0
					Delay >=15 days and <=30 days	5
					Delay >=30 days <=45 days	9
3	Launch of Release_1 Components	Delay	Measured as the difference between the planned date for the milestone and the actual date of its completion in terms of delay in number of calendar days For details about preparedness, please refer to the *Note-B* at the end of this table.	Milestone based Measurement	Delay of <=14 days	0
					Delay >=15 days and <=30 days	5
					Delay >=30 days	9

#	Category/ Component	Metric Type	Formula / Definition	Period and Time of Measurement	Target	Severity level
4	Launch of Release_2 Components	Delay	Measured as the difference between the planned date for the milestone and the actual date of its completion in terms of delay in number of calendar days For details about preparedness, please refer to the *Note-B* at the end of this table.	Milestone based Measurement	Delay of <=14 days	0
					Delay >15 days and <=30 days	5
					Delay >30 days	9
5	Biometric Benchmarking and Acceptance	Delay	Measured as the difference between the planned date for the milestone and the actual date of its completion in terms of delay in number of calendar days For details about preparedness, please refer to the *Note-B* at the end of this table.	Milestone based Measurement	Delay of <=14 days	0
					Delay >15 days and <=30 days	5
					Delay >30 days	9

Table 9.3 : Implementation Phase Service Levels

Note:

(A) The preparedness for the Launch of Release_1 would comprise of the following:

- **Hosting Infrastructure:** Supply, installation, configuration, integration and testing of all components and equipment as per the agreed bill of material, to the satisfaction of the ICTA

- **Software**: Supply of necessary licenses as per the agreed bill of material

- **Network Setup**: Installation, configuration, setup and testing of network for all locations (except network at the enrolment centres), to the satisfaction of the ICTA. The networks should be well-integrated with the network operation centres, to the satisfaction of the ICTA.

- **Security Components:** Supply, installation, configuration, integration and testing of all security components and equipment as per the agreed bill of material, to the satisfaction of the ICTA. The software components should be well-integrated with the network operation centres, to the satisfaction of the ICTA.

- **Field Infrastructure:** Supply, installation, configuration, integration and testing of all field infrastructure components and equipment as per agreed bill of material, to the satisfaction of the ICTA. This will include setup of the service centre and availability of all the spares in the agreed location. This shall exclude the installation of the enrolment software and user training.

- **Enrolment Centre**: Readiness of the enrolment centre in all aspects for which MSI is responsible.

- **Contact Centre and Helpdesk**: Establishment of the contact centre and helpdesk, finalization of documentation (FAQs, SOPs, etc.), availability and training of manpower, etc.

- **SOC and NOC**: Establishment of SOC & NOC, integration with network and security components, finalization of documentation, the availability and training of manpower, etc.

- **DevSecOps:** Setup and operationalization of CI/CD pipeline as per the DevSecOps

- **Project Management**: Finalization of all reporting formats, configuration of SLA reporting in the identified tool, readiness of risk & issue management related documents with latest information, and other information as expected to be completed prior to launch.

(B) In addition to the Note-A, the Launch of Release_1 and Release_2 would comprise of the following:

- **Requirement Gathering**: Sign-off from ICTA or nominated party. and DRP for all the requirement gathering (functional, non-functional) related deliverables relevant for the specific components which are part of respective releases.

- **Design**: Sign-off of design as per the gathered requirements, from ICTA and DRP for all the design documents for common aspects (such as architectures) and specific components which are part of respective releases.

- **Development and Customization**: Completion of the development and customization of the components, as per sign-off design, which are part of respective releases

- **Installation:** Installation of the software in the data centre environments including the production environment

- **Testing**: Completion of the testing such as integration testing, system testing, performance and load testing, security testing and user acceptance testing and sign-off from ICTA & DRP for aforementioned type of testing. This shall exclude the partial acceptance testing as well as benchmarking and final acceptance testing.

- **Training**: Completion of the training of the identified users.

- **Improvements (applicable for Release_2 only)**: Incorporation of learnings from the Launch of Release_1 in the applicable areas of the project under purview of the MSI

(C) In addition to the Note-A and Note-B, Go-Live would comprise of the following:

- **Benchmarking:** Completion of the testing, assessment of results, and sign-off of the results by ICTA and DRP.
- **Infrastructure Augmentation**: As per results of benchmarking, necessary augmentation of the infrastructure necessary to meet the required performance requirements of the project.
- **Final Acceptance Testing:** Completion of the final acceptance testing, assessment of results, completion of identified improvements and demonstration of improvements, and sign-off of the results by ICTA and DRP.

9.3 Service Levels for Manpower

#	Category/ Component	Metric Type	Formula / Definition	Period and Time of Measurement	Target	Severity level
1	Team Deployment	Availability	Resources to be mobilized on-time as per the Staffing Schedule submitted as part of MSI's Technical Bid. This penalty will be calculated for each resource.	First time deployment of each resource, as per the Staffing Schedule	Delay of <=14 days	0
					Delay of > 14 days	INR1,00,000 per resource per week
2	Manpower Presence and Deployment on project	Non-availability on working days	Number of days of absence on working days per month. This penalty will be calculated for each resource	Monthly	<= 2 days	0
					>=3 days and <= 5 days	INR 10,000 per resource per day

#	Category/ Component	Metric Type	Formula / Definition	Period and Time of Measurement	Target	Severity level
					>=6 days and <= 10 days	INR 25,000 per resource per day
					>10 days	INR 100,000 per resource per day
3	Change in named Key Personnel	Changes in Team	Key personnel team deputed at SL-UDI project to consist of same members whose names were proposed in the Bid/ project start Note: For project manager, the penalty will be double the amount mentioned in the table.	Quarterly	No changes	0
					1	INR 1,000,000 per resource
					2 to 4	INR 2,500,000 per resource
					5 or more	INR 5,000,000 per resource
4	Resource availability for front-end operations	Non-availability on working days	No. of shift days (8 hours per shift day) for which resource present at the designated location / Total no. of shift days	Quarterly	>= 99%	0
					>= 97 % to <99%	INR 1,000,000 per resource per day

#	Category/ Component	Metric Type	Formula / Definition	Period and Time of Measurement	Target	Severity level
			This will be averaged for all resources designated for Helpdesk		>=95 % to <97%	INR 2,000,000 per resource per day
					<95 %	INR 5,000,000 per resource per day

Table 9.4 : Service Levels for Manpower

9.4 Service Levels for Biometric Registration Kits

The ICTA and/or DRP (or their representatives) may make a complaint about the equipment/ service through letter, fax, e-mail, phone, SMS or any other means and updated on the respective issue management system, as the ICTA and/or DRP thinks fit or convenient to the Technical Helpdesk of MSI.

Note: The Category-1 locations would comprise of country capital and province headquarters, Category-2 would comprise of district locations, and remaining locations would form part of Category-3 locations.

S. No.	Item	Duration
1.	Telephonic Support (Diagnose the issue and resolve through telephonic support within 2 hours on receipt of the complaint)	Two hours
2.	Physical Visit	Next business day
3.	On receiving complaint about equipment/service, the MSI will respond and repair/replace or provide required services in Category-1 Locations	Two business days
4.	On receiving complaint about equipment/service, the MSI will respond and repair/replace or provide required services in Category-2 Locations	Three business days
5.	On receiving complaint about equipment/service, the MSI will respond and repair/replace or provide required services in Category-3 Locations	Four business days
6.	On receiving complaint about equipment/service, the MSI will respond and repair/replace or provide required services for mobile kits (anywhere in the country)	Two business days

Table 9.5: Service Levels for Biometric Registration Kits

Note: For replacements, the MSI may use the spares required to be arranged by the MSI under the project. These replacements should be of the same make and model which are part of the bill of material.

In case MSI fails to meet the above standards of maintenance, there will be per device per day penalty of 5% of the cost of the item. In case the equipment is not repaired/replaced even after one week after the stipulated timeline has passed, the penalty will be charged at 2 (twice) times of the aforementioned penalty.

S. No.	Item	Duration
1.	Regular Software Update	One month from the date of release of update by the OEM
2.	Critical Security Update / Patch and Hotfixes	As per the agreed schedule but no later than one week from the date of release of update/patch/hotfix by the OEM

Table 9.6 : Software Update Schedule

In case MSI fails to meet the above standards of maintenance for regular software update, there will be per day penalty of 0.5% of the cost of the item, for each week (or part thereof) of delay. In case the equipment is not repaired/replaced within four weeks, the penalty will be charged at 2 (times) times of the aforementioned penalty.

In case MSI fails to meet the above standards of maintenance for critical security update, there will be per day penalty of INR 100 or 1.0% of the cost of the item, whichever is higher, for each week (or part thereof) of delay. In case the equipment is not repaired/replaced within four weeks, the penalty will be charged at 5 (five) times of the penalty shown above.

9.5 Service Levels for Biometric Solution -

Following are the SLA principles adopted for Solution related performance levels

- The Performance targets for the Service Level Measurements during any period of assessment may not fixed for the entire contract period and may be revised for each period prior to the commencement of the period

#	Service Level	Metric Type	Formula/Definition	Period and Time of Measurement	Target	Consequence / Severity in case of Penalty
1	False Positive Identification Rate (FPIR)	Quality	FPIR = (Number of false positive identification decisions in the day)/ (total number of enrolment transactions by unenrolled individuals in the day).	Quarterly	<= 0.1% measured per month	0
					> 0.1% and <= 2% measured per month	7
					> 2% measured per month	8 or 9 (if breach occurred for two consecutive cycles Penalty of severity)
2	False Negative Identification Rate (FNIR)	Quality	FNIR = (Number of false negative identification decisions in the day)/ (total number of enrolment	Quarterly	<= 1% measured per month	0
					> 1% and <= 2% measured per month	7

#	Service Level	Metric Type	Formula/Definition	Period and Time of Measurement	Target	Consequence / Severity in case of Penalty
			transactions by unenrolled individuals in the day).		> 2% measured per month	8 or 9 (if breach occurred for two consecutive cycles Penalty of severity)
3	False Match Rate (FMR)	Quality	FMR = (Number of biometric verification transactions in the day resulting in a false match)/ (total number of biometric transactions).	Quarterly	<= 0.01% for all levels of verification measured per quarter	0
					> 0.01% and <= 0.1% for all levels of verification measured per quarter	6
					> 0.1% and <= 1% for all levels of verification measured per quarter	8

#	Service Level	Metric Type	Formula/Definition	Period and Time of Measurement	Target	Consequence / Severity in case of Penalty
					> 1% for all levels of verification measured per quarter	9
4	False Non-Match Rate (FNMR)	Quality	FNMR = (Number of biometric verification transactions resulting in a false non match)/ (total number of biometric transactions).	Quarterly	<= 2% for all levels of verification measured per quarter	0
					> 2% and <= 3% for all levels of verification measured per quarter	6
					> 3% and <= 4% for all levels of verification measured per quarter	8
					> 4% for all levels of verification measured per quarter	9
5		Throughput		Quarterly	=< 24 hours	0

#	Service Level	Metric Type	Formula/Definition	Period and Time of Measurement	Target	Consequence / Severity in case of Penalty
	Response Time per De-duplication check		Response Time = Average elapsed time between submission of an enrolment request to Biometric Solution and generation of response (Success or failure of de-duplication)		>24 hours to <=28 hours	5
					>28 hours to <=32 hours	6
					>32 hours to <=36 hours	7
					>36 hours	8
6	Fine tuning of Biometric Solution	As per scope of work	For each instance when fine-tuning is not carried out by the bidder within the specified timeline	Quarterly	Compliant	0
					Non-Compliance	8, or 9 (if breach occurred for two consecutive fine-tunings)

Table 9.7: Service Levels for Biometric Solution

9.6 Service Levels for Application and Software Services

#	Category/ Component	Metric Type	Formula/Definition	Period and Time of Measurement	Target	Severity Level
1	Authentication Services	Availability	**Metric:** % of Uptime for Authentication Services **Formula:** Uptime % = {1-[(Total Downtime) / (Total Time)]} *100 For the purpose of this SLA, Authentication Services Components comprises of Data Centre and Associated Networks, Fraud Management System, Biometric SDK, Authentication Solution, Resident Data Store, Partner and Device Management Solution, Device management Server, Service Billing System, API Gateway, IDAM, and other components on which the authentication service is responsive and available to the end-users. **Total Time:** 24 hours x 30 days **Total Downtime:** Total cumulative time the Applications are NOT Available. ***Note:*** There is no planned downtime for this service.	Monthly	>= 99.95%	0
					< 99.95% and >=99.90%	3
					<99.90%	6

#	Category/ Component	Metric Type	Formula/Definition	Period and Time of Measurement	Target	Severity Level
2	Enrolment Services	Availability	**Metric:** % of Uptime for Enrolment Services **Formula:** Uptime % = {1-[(Total Downtime) / (Total Time – Planned Downtime)]} *100 For the purpose of this SLA, Enrolment Services Components comprises of Data Centre and Associated Networks, Registration Processor, ID repository, ABIS, Biometric Middleware, Manual Adjudication, and other components on which the enrolment service is responsive and available to the process the enrolment packets. **Total Time:** 24 hours x 30 days **Total Downtime:** Total cumulative time the Applications are NOT Available. **Planned Downtime:** Total maintenance time as defined and agreed upon between MSI and ICTA.	Monthly	>= 99.0%	0
					< 99.0% and >=98.5%	3
					<98.4%	6
3	External facing components (except those covered under	Availability	**Metric:** % of Uptime for External Facing Components **Formula:** Uptime % = {1-[(Total Downtime) / (Total Time – Planned Downtime)]} *100	Monthly	>= 99.5%	0

#	Category/ Component	Metric Type	Formula/Definition	Period and Time of Measurement	Target	Severity Level
	Enrolment and Authentication Services)		For the purpose of this SLA, External Facing Components comprises of Pre-Enrolment, Portals, Call Centre Services, Helpdesk Services, Partner and Device Management, Queue Management System, ITSM, etc.		< 99.50% and >=99.00%	3
			Total Time: 24 hours x 30 days **Total Downtime:** Total cumulative time the Applications are NOT Available. **Planned Downtime:** Total maintenance time as defined and agreed upon between MSI and ICTA.		<99.00%	6
4	Internal facing components (critical components) (except those components which are covered under authentication services, enrolment services and external facing components)	Availability	**Metric:** % of Uptime for External Facing Components **Formula:** Uptime % = {1-[(Total Downtime) / (Total Time – Planned Downtime)]} *100	Monthly	>= 99.90%	0
			For the purpose of this SLA, Internal Facing (Critical Components) comprise of NOC, SOC, BI & Analytics, EMS, etc.		< 99.90% and >=99.5%	3
			Total Time: 24 hours x 30 days		<99.50%	6

#	Category/ Component	Metric Type	Formula/Definition	Period and Time of Measurement	Target	Severity Level
			Total Downtime: Total cumulative time the Applications are NOT Available. **Planned Downtime:** Total maintenance time as defined and agreed upon between MSI and ICTA.			
5	Internal facing components (non-critical components and other components not covered in other SLAs)	Availability	**Metric:** % of Uptime for External Facing Components **Formula:** Uptime % = {1-[(Total Downtime) / (Total Time – Planned Downtime)]} *100	Monthly	>= 99.0%	0
			For the purpose of this SLA, Internal Facing (Non-Critical Components) comprise of Cards Management System, KMS, LMS, Project Management Tool, etc.		< 99.0% and >=98.5%	3
			Total Time: 24 hours x 30 days **Total Downtime:** Total cumulative time the Applications are NOT Available. **Planned Downtime:** Total maintenance time as defined and agreed upon between MSI and ICTA.		<98.4%	6

Table 9.8 : Service Levels for Application and Software Services

9.7 Service Levels for Infrastructure

#	Category/ Component	Metric Type	Formula/Definition	Period and Time of Measurement	Target	Severity Level
1	Hosting Infrastructure	Availability	**Metric:** % of Uptime for Overall SL-UDI DS **Formula:** Uptime % = {1-[(Total Downtime) / (Total Time – Planned Downtime)]} *100 **Total Downtime** - Total cumulative time the hosting services are NOT Available. **Planned Downtime** -Total maintenance time as defined and agreed upon by MSI and ICTA.	• Available - 24 X 7, measured over a period of month. • Monthly Measurement	>= 99.95%	0
					< 99.95% & >= 99.50%	4
					< 99.50% & >= 99%	7
					<99%	8

Table 9.9 : Service Levels for Infrastructure

The service support quality matrix provides the details of parameters on which the service support of the MSI shall be evaluated and measured. The service requests and tickets shall have graded priorities (From P1 to P4) based on the business impact and criticality of issue decided by ICTA or nominated party.

Highly Critical	Critical	Less-Critical	Non- Critical
Total failure of hardware/network equipment - Virtual appliances/ Security device and Solutions/ Virtualization and container	Total failure of hardware/network equipment, Virtual appliances / Security device and Solutions /Virtualization and container platforms but no down-time	Partial failure of hardware/network equipment, Virtual appliances/ Security device and Solutions	Alert/ warning Any critical alert or warning of any of the

Highly Critical	Critical	Less-Critical	Non- Critical
platforms affecting complete or partial down-time Any of the -Active hardware component, sub-component, - Passive hardware component (ex. Patch cable), - Firmware, - Any related equipment - Virtual appliances - Security device and Solutions - Virtualization and container platforms Deployed malfunctioning or failure, which leads to partial or complete outage.	Any of the - Active hardware component, sub-component, - Passive hardware component (ex. Patch cable), - Firmware, - Any related equipment - Disk failure - Virtual appliances - Security device and Solutions - Virtualization and container platforms Deployed malfunctioning or partial failure, but no partial or complete outage or degraded performance (>5%). (Ex: total failure of redundant firewall or power supply)	/Virtualization and container platforms no down-time Any of the - Active hardware component, sub-component, - Passive hardware component (ex. Patch cable), - Firmware, - Any related equipment - Virtual appliances - Security device and Solutions - Virtualization and container platforms Deployed malfunctioning which leads to degraded performance (>5%).	- Active hardware component, sub-component, - Passive hardware component (ex. Patch cable), - Firmware, - Any related equipment - Virtual appliances - Security device and Solutions - Virtualization and container platforms Without any partial or total failure or degraded performance (>5%).

Table 9.10 : Service Support Quality Matrix

#	Category/ Component	Metric Type	Formula/Definition	Period and Time of Measurement	Target	Severity Level
1	Incident Response Time (P1)	Response Time	Average Time taken to acknowledge and respond once a ticket/incident is logged through calls, email or Ticketing System. This is calculated for all tickets/incidents reported within the reporting month. Target: 15 Minutes	Monthly	100% within the defined target	0
					>=99% and <100% meeting the target	1
					>=97% and <99% meeting the target	3
					>=95% and 97% meeting the target	5
2	Incident Response Time (P2)	Response Time	Average Time taken to acknowledge and respond once a ticket/incident is logged through calls, email or Ticketing System. This is calculated for all tickets/incidents reported within the reporting month. Target: 30 Minutes	Monthly	100% within the defined target	0
					>=99% and <100% meeting the target	1
					>=97% and <99% meeting the target	3
					>=95% and 97% meeting the target	5
3	Incident Response Time (P3)	Response Time	Average Time taken to acknowledge and respond once	Monthly	100% within the defined target	0

#	Category/ Component	Metric Type	Formula/Definition	Period and Time of Measurement	Target	Severity Level
			a ticket/incident is logged through calls, email or Ticketing System. This is calculated for all tickets/incidents reported within the reporting month. Target: 45 Minutes		>=99% and <100% meeting the target	1
					>=97% and <99% meeting the target	3
					>=95% and 97% meeting the target	5
4	Incident Response Time (P4)	Response Time	Average Time taken to acknowledge and respond once a ticket/incident is logged through calls, email or Ticketing System. This is calculated for all tickets/incidents reported within the reporting month. Target: 60 Minutes	Monthly	100% within the defined target	0
					>=99% and <100% meeting the target	1
					>=97% and <99% meeting the target	3
					>=95% and 97% meeting the target	5

Table 9.11: Incident Response Times

9.8 Service Levels for Business and Technical Services

The service support quality matrix provides the details of parameters on which the service support of the MSI shall be evaluated and measured. The service requests and tickets shall have graded priorities (From P1 to P5) based on the business impact and criticality of issue decided by ICTA.

While the service desk shall only be measured on response to incidents, other teams like incident management and problem management shall be measured on restoration of service and resolution of the issues.

				Priority (in hours)				
Service	**Request Type**	**Responsibility**	**Metric**	**P1**	**P2**	**P3**	**P4**	**P5**
Incident Management	Incident Resolution – Resolution of Issue (like security incidents, data theft, etc.) after incident was logged in the system	IT Help Desk	Resolution Time (In Hrs.)	0.50	2	24	48	96

Table 9.11 : Service Levels for Business and Technical Services

#	Category/ Component	Metric Type	Formula/Definition	Period and Time of Measurement	Target	Severity Level
1	IT Help Desk	Restoration Time	**Metric**: % of Priority-1 Tickets restored within 2 hours **Formula**: Number of tickets responded within 2 hours/ Total Number of Tickets raised in that Month	Monthly	>= 99%	0
					>= 98% to 99%	1
					>= 97% to 98%	2
					>= 95% to 97%	3
					>= 90% to 95%	4
					<90%	5

#	Category/ Component	Metric Type	Formula/Definition	Period and Time of Measurement	Target	Severity Level
2	IT Help Desk	Restoration Time	**Metric**: % of Priority-2 Tickets restored within 24 hours **Formula**: Number of tickets responded within 24 hours/ Total Number of Tickets raised in that Month	Monthly	>= 99%	0
					>= 98% to 99%	1
					>= 97% to 98%	2
					>= 95% to 97%	3
					>= 90% to 95%	4
					<90%	5
3	IT Help Desk	Restoration Time	**Metric**: % of Priority-3 Tickets restored within 48 hours **Formula**: Number of tickets responded within 48 hours/ Total Number of Tickets raised in that Month	Monthly	>= 99%	0
					>= 98% to 99%	1
					>= 97% to 98%	2
					>= 95% to 97%	3
					>= 90% to 95%	4
					<90%	5
4	IT Help Desk	Restoration Time		Monthly	>= 99%	0
					>= 98% to 99%	1

#	Category/ Component	Metric Type	Formula/Definition	Period and Time of Measurement	Target	Severity Level
			Metric: % of Priority-4 Tickets restored within 96 hours **Formula**: Number of tickets responded within 96 hours/ Total Number of Tickets raised in that Month		>= 97% to 98%	2
					>= 95% to 97%	3
					>= 90% to 95%	4
					<90%	5
5	IT Help Desk	Restoration Time	**Metric**: % of Priority-5 incidents resolved within 144 hours **Formula**: Number of tickets responded within 144 hours/ Total Number of Tickets raised in that Month	Monthly	>= 99%	0
					>= 98% to 99%	1
					>= 97% to 98%	2
					>= 95% to 97%	3
					>= 90% to 95%	4
					<90%	5

Table 9.12 : SLA for IT Helpdesk

Note: (A) “Restoration Time” means time taken (after the trouble call has been logged on the helpdesk), in resolving (diagnosing, troubleshooting, and fixing) or escalating (to the second level to respective OEM, getting the confirmatory details about the same from the OEM and resolving the same). Provisioning of standby, if required, should be done along with associated data being restored, services reinitiated and SLA conditions being met. Final Resolution shall be deemed to be complete only after the original equipment is replaced / reinitiated along with data being restored to the correct state and services are resumed.

Note: (B) Time taken (after the trouble call has been logged on the helpdesk), in resolving (diagnosing, troubleshooting and fixing) or escalating (to the second level to respective OEMs, getting the confirmatory details about the same from the OEM and resolving the same). Provisioning of standby, if required, should be done along with associated data being restored, services reinitiated and SLA conditions being met. Final Resolution shall be deemed to be complete only after the original equipment is replaced / reinitiated along with data being restored to the correct state and services are resumed

#	Category/ Component	Metric Type	Formula/Definition	Period and Time of Measurement	Target	Severity Level
1	Root cause analysis	Problem set management	Should perform an analysis on the alerts and incidents triggered in SL-UDI system to detect the root cause of the incidents and to fine-tune the configured rules. A detailed report including the action plan should be submitted to ICTA management for necessary actions. Root cause analysis shall be done for Priority 1 (P1) and Priority 2 (P2): a. P1 – within 24 hrs. of actual resolution of the incident b. P2 – within 48 hrs. of actual resolution of the incident Priority of the incident will be decided after discussion with ICTA Formula RCA Completion percent = (Number of tickets on which RCA was completed within defined timelines / Number of tickets for which RCA was due as per assessment) * 100	During operations and maintenance phase on a quarterly basis	>=100%	0
					<100% and >=95%	1
					<95% and >=90%	2
					<90% and >=85%	3
					<85	4

9.9 Service Levels for Project Management Services

#	Category/ Component	Metric Type	Formula/Definition	Period and Time of Measurement	Target	Severity Level
1	Project Management	Schedule Variance (SV)	**Metric:** % Variance between allotted time for development / change and estimated time **Formula:** SV = (Actual Elapsed Time – Estimated Elapsed Time) /Estimated Elapsed Time **Period of Measurement:** Quarterly	Monthly	<= 5%	0
					>5%	4
2	Reporting	Scheduled Reporting	**Metric:** Compliance to the reporting schedule and format as approved by ICTA **How:** Adherence to reporting timelines **Period of Measurement:** Monthly	Monthly	100%	0
					< 100%	3
3	SLA and KPI Reporting	Monitoring of the systems	**Metric:** Availability of a dashboard to track and monitor 100% of the SLAs and KPIs	Monthly	100%	0

#	Category/ Component	Metric Type	Formula/Definition	Period and Time of Measurement	Target	Severity Level
			How: Availability of dashboard and generation of reports in prescribed format **Period of Measurement:** Business hours (9 am to 7 pm)		< 100%	5
4	Data Quality Monitoring & Reporting	Weekly reports as per scope of work	**Metric:** Availability of a report to track and monitor 100% of the Data Quality **How:** Availability of reports in prescribed format	Monthly	100%	0
					< 100%	6
5	ABIS reporting	Weekly reports as per scope of work	**Metric:** Availability of dashboards and generation of report to track and monitor ABIS **How:** Availability of dashboard reports in prescribed format	Monthly	100%	0
					< 100%	6
6	Incident and Issue Reporting			Monthly	100%	0

#	Category/ Component	Metric Type	Formula/Definition	Period and Time of Measurement	Target	Severity Level
		Weekly reports as per scope of work	**Metric:** Availability of dashboards and generation of report to track and monitor incidents and issues **How:** Availability of dashboard reports in prescribed format		< 100%	5

Table 9.13: Service Levels for Project Management Services

9.10 Service Levels for Security Services

9.10.1 Documentation SLAs

#	Category / Component	Metric type	Formula/Definition	Period and Time of Measurement	Target	Severity Levels
1	SLA measurement methodology	Completion and coverage	MSI shall prepare a measurement methodology for all the SLAs defined in the RFP. Under no circumstances MSI shall change the target or definition and shall only suggest method(s) to measure the SLAs.	One time	T+12 weeks	0
					Delay of <=2 weeks from target	1
					Delay of more than 2 weeks but <=4 weeks from target.	2
					More than 4 weeks delay from target.	3
2	Policy, procedure and hardening standards review / design	Completion and coverage	MSI should review, update, design or create (as applicable) all the security and privacy policies, standard operating procedures, hardening standards and workflows required for effective security	First time: 3 months after Go-live.	As per target	0
					Delay of <=1 month from target	1

#	Category / Component	Metric type	Formula/Definition	Period and Time of Measurement	Target	Severity Levels
			of SL-UDI program as mentioned in the RFP. The list of all such documents should be decided in advance by MSI and approved by ICTA. All the documents should be submitted within the defined timelines. This activity should be performed for the first time within 3 months of Go-Live and then on an annual basis.	Thereafter: Annually Finally, upon exiting the contract.	Delay of more than 1 month but <=2 months from target	2
					More than 2 months delay from target	3

Table 9.13 : Documentation SLAs

Note: T= effective date of contract

9.10.2 Process Reviews

#	Category / Component	Metric type	Definition	Period and Time of Measurement	Target	Severity level
1	Periodic process reviews and activities	Completion and coverage	Applies to all periodic activities described in scope of work in the RFP. This will include but not be limited to the following: a) Access Reconciliation b) Asset management review c) Change management review d) Patch management review e) Encryption review f) Backup review g) Biometric deduplication review h) Personnel security review i) Physical security review j) Security Operations Center (SOC) review k) BCP-DR review l) Exception management review m) Any other periodic activity described in the scope of work in the RFP All the documents should be submitted within the defined timelines. This activity should be performed for the first time within 3 months of Go-Live and then on a half yearly basis. MSI is expected to prepare a detailed plan for conducting process	During operations and maintenance phase First time: 3 months after Go-live. Thereafter: Every six months Finally, upon exiting the contract.	As per target	0
					Delay of <=1 month from target	1
					Delay of more than 1 month but <=2 months from target	2
					More than 2 months delay from target	3

#	Category / Component	Metric type	Definition	Period and Time of Measurement	Target	Severity level
			reviews. MSI shall submit the plan to ICTA for approval. The detailed plan shall cover the scope of review, frequency, approach, methodology, international standards, frameworks, best practices, document / deliverable acceptance criteria, etc. The process reviews shall be conducted as per the plan approved by the ICTA.			

Table 9.14 :SLA for Process Reviews

Note: T= effective date of contract

9.10.3 Audits and Risk Assessments

#	Category / Component	Metric type	Definition	Period and Time of Measurement	Target	Severity level
1	Internal Audit	Completion and coverage	Completion as per schedule based on security policy, procedures, ISO 27001 standard and regulatory compliance requirements. MSI is expected to prepare a detailed audit plan/ Gap Analysis for	First time: before Go-live.	Half yearly as per defined schedule	0

#	Category / Component	Metric type	Definition	Period and Time of Measurement	Target	Severity level
			conducting internal audit. MSI shall submit the plan to ICTA for approval. The detailed plan shall cover the scope of review, frequency, approach, methodology, international standards, frameworks, best practices, report acceptance criteria, etc. The internal audit shall be conducted as per the plan approved by the ICTA. This activity should be performed as per the ‘Period and Time of Measurement’ column.	Thereafter: Every six months Finally, upon exiting the contract.	Delay by <=1 month from target	1
					Delay by more than 1 month and <=2 months from target	2
					More than 2 months delay from target	3
2	Risk assessment	Completion and coverage	Completion as per schedule based on risk assessment / treatment methodology approved by ICTA. This activity should be performed as per the ‘Period and Time of Measurement’ column.	First time: before Go-live. Thereafter: Every six months	Annually as per defined schedule	0
					Delay by <=1 month from target	1
					Delay by more than 1	2

#	Category / Component	Metric type	Definition	Period and Time of Measurement	Target	Severity level
				Finally, upon exiting the contract.	month and <=2 months from target	
					More than 2 months delay from target	3
3	Privacy gap assessment and privacy impact assessment	Completion and coverage	Completion as per schedule based on privacy policy, procedures and relevant laws applicable. MSI is expected to prepare a detailed plan for conducting privacy gap assessment and privacy impact assessment as per **ISO 27701, ISO29100 or BS10012, NIST Privacy Framework, etc.** MSI shall submit the plan to ICTA or nominated party for approval. The detailed plan shall cover the relevant details for conducting this activity including but not limited to scope, standards to be followed, approach and methodology, report acceptance criteria, among others. The privacy gap assessment and privacy impact assessment shall be conducted as per the plan approved by ICTA. This activity	First time: before Go-live. Thereafter: Every six months Finally, upon exiting the contract.	Annually as per defined schedule	0
					Delay by <=1 month from target	1
					Delay by more than 1 month and <=2 months from target	2
					More than 2 months	3

#	Category / Component	Metric type	Definition	Period and Time of Measurement	Target	Severity level
			should be performed as per the 'Period and Time of Measurement' column.		delay from target	
4	Findings closure tracker and management dashboard (including internal audit, risk assessment, process reviews, privacy reviews, security solutions review, etc.)	Completion	Completion as per schedule for all findings identified during go-live, or while conducting internal audit, risk assessment, process reviews, privacy reviews, security solutions review, etc. It is expected, that MSI shall maintain a tracker for issues faced / identified during Implementation phase as well as the findings from periodic reviews / assessments during the Operations and Maintenance phase. All such issues / findings should be tracked towards closure and dashboard presented to the management on a monthly basis during the project.	Monthly	Monthly as per defined schedule	0
					Delay by <=1 week from target	1
					Delay by more than 1 week and <=2 weeks from target	2
					More than 2 weeks delay from target	3

#	Category / Component	Metric type	Definition	Period and Time of Measurement	Target	Severity level
5	Compliance for assessments conducted by third party / external auditor	Percent of findings/ gaps closure	Applies to the findings of any assessments (including security and privacy reviews, process reviews, technology reviews, etc.) conducted by external auditor or any third party vendor against policies and procedures of SL UDI program from time to time. In order to measure the success of closure of findings of all assessments, MSI should address the findings/gaps for closure with relevant artefact in support within defined timeline: 100% closure of identified findings / observations / gaps within 90 days of receipt. Formula Closure compliance= [No. of closures accepted by ICTA within defined timeline / Total number of findings/gaps (excluding findings/gaps for which specific exceptions have been obtained from ICTA) reported] * 100.	First time: before go live, Post Go Live: bi-annually	Closure compliance = 100%	0
					Closure compliance <100% and >=95%	1
					Closure compliance <95%	3
6	Obtain necessary		MSI shall obtain the necessary certifications where applicable such as ISO 27001, ISO 22301, etc. as decided by ICTA from time to	First time: 6 months after	No non-compliance	0

#	Category / Component	Metric type	Definition	Period and Time of Measurement	Target	Severity level
	certifications (Technical Aspects)	Completion and coverage	time. The MSI shall work with MSP in order to obtain the certification. MSI is expected to perform the following activities including but not limited to: Pre-Certification Assessment: Assessment of implemented controls against ISO 27001 / 22301, identification of minor and major non-conformities, observations, and scope for improvement, corrective action plan and remediation of gaps. Final Certification: Assistance in identification of certification agency, development of a comprehensive timeline and plan for the certification and complete the actual certification audit / process. In order to measure the success of this SLA, MSI should address the findings/gaps for closure identified during pre-certification assessment with relevant artefact in support. No non-compliances should be given by the certification agency during the certification audit process.	Go-live. Post this, annually.	Any non-compliance reported during the certification audit	2

Table 9.15 : Audits and Risk Assessments

9.10.4 Security Operations SLAs

#	Category / Component	Metric type	Definition	Period and Time of Measurement	Target	Severity level
1	Device integration with SIEM and custom parsers implementation	Event source coverage	All the new hardware and software that are being implemented in the ICTA infrastructure should be integrated with SIEM before go-live of that particular hardware / software (including writing custom parsers, testing, alerting etc.)	During operations and maintenance phase on a quarterly basis	100% coverage	0
					<100 and >=98%	1
					<98 and >=95%	2
					<95%	3
					<90%	4
2	Alerts monitoring	Monitoring	All the alerts generated in SOC against any of the rule configured in SOC should be tracked and investigated. Alerts which are false positives shall be documented as false positives in the ticket for analysis purpose. Tickets shall be logged for all alerts triggered in SIEM solution.	During operations and maintenance phase on a quarterly basis	100% of alerts should be logged as tickets	0
					<100 and >=98%	1
					<98 and >=95%	2

#	Category / Component	Metric type	Definition	Period and Time of Measurement	Target	Severity level
					<95 and >=90%	3
					<90%	4
3	Missed Security incident	Missed incident (per incident)	Missed security incidents are those security incidents for which alerts are not generated by SOC. There shall be no security incidents which are missed by SOC. Security incident for the purpose of this SLA means any malicious activity in SL UDI infrastructure that could compromise the security even if has not been executed successfully. For e.g., if SQL injection attempts on applications are not detected by SOC even if those did not result in data breach, these shall be considered as missed security incidents or if brute force attacks on password of external applications such as email are not detected, even if there is no compromise, these shall be considered as missed security incidents.	During operations and maintenance phase on a quarterly basis	No incident	0
					Occurrence of an incident	5
4	Quality of tickets	Problem set management	Quality of tickets would mean appropriate classification, detailed notes in the ticket describing the incident, appropriate bucketisation, appropriate assignment, appropriate status etc. as per the security incident management policy and procedure.	During operations and maintenance	>=90%	0
					<90% and >=80%	1

#	Category / Component	Metric type	Definition	Period and Time of Measurement	Target	Severity level
			Formula – (Total score for all tickets audited / (100* number of samples selected for audit)) * 100 Random tests with reasonable sampling should be carried out. Checklist with scoring for each parameter shall be formulated for measurement. Score shall be measured from 1 to 100. MSI is expected to prepare a detailed plan for conducting the tests. MSI shall submit the plan to ICTA for approval and begin the exercise post approval.	phase on a quarterly basis	<80% and >=70%	2
					<70% and >=60%	3
					<60%	4
5	Security incident response	Timely response	Definition: Response to security incidents shall be done in a timely manner: a. P1 incidents shall be responded within 15 minutes b. P2 incidents shall be responded within 30 minutes c. P3 incidents shall be responded within 45 minutes d. P4 incidents shall be responded within 60 minutes Formula**:** (Number of tickets opened during the period and for which response is provided within defined timelines / Number of total tickets opened during the period) * 100	During operations and maintenance phase on a quarterly basis	>=95%	0
					<95% and >=90%	1
					<90% and >=80%	2
					<80% and >=70%	3
					<70%	4

#	Category / Component	Metric type	Definition	Period and Time of Measurement	Target	Severity level
6	Security incident resolution	Timely response	Definition: Resolution to security incidents shall be done in a timely manner: a. P1 incidents shall be resolved/closed within 8 hours b. P2 incidents shall be resolved/closed within 2 days c. P3 incidents shall be resolved/closed within 5 days d. P4 incidents shall be resolved/closed within 15 days Formula**:** (Number of tickets opened during the period and for which resolution is provided within defined timelines / Number of total tickets opened during the period) * 100	During operations and maintenance phase on a quarterly basis	>=95%	0
					<95% and >=90%	1
					<90% and >=80%	2
					<80% and >=70%	3
					<70%	4
7	Security and Privacy breach including Data Theft / Loss / Corruption / Mining	Completion	Any incident where-in a system is compromised, privacy breached, data is corrupted, data is mined or any case wherein data theft occurs (including internal incidents) impacting business operations in a major way. MSI shall provide a report on the breach including remediation measures taken to mitigate the security breach. The report shall be submitted within 5 working days to ICTA management.	Annually	No breach	0
					Any security or privacy breach These penalties will not be part of overall SLA penalties cap. In case of serious breach	8

#	Category / Component	Metric type	Definition	Period and Time of Measurement	Target	Severity level
					of security wherein the data is stolen, mined, privacy breached or corrupted, ICTA reserves the right to terminate the contract or impose appropriate penalties.	
8	Maintenance of Access control matrix	Accuracy of Access control matrix	Any access provisioning/deprovisioning/update should be reported within the defined timeline in the prescribed format as per the defined policies and procedures and updated in the access control matrix/access list. Access list should be updated on a regular basis (near real time). Random access reconciliations exercise with reasonable sampling	During operations and maintenance phase on a monthly basis	100%	0
					<100 and >=98%	1
					<98 and >=95%	2

#	Category / Component	Metric type	Definition	Period and Time of Measurement	Target	Severity level
			will be carried out to check for the accuracy of the access list. MSI is expected to prepare a detailed plan for conducting the access reconciliation exercise. MSI shall submit the plan to ICTA for approval and begin the exercise post approval.		<95 and >=90%	3
					<90%	4
9	EDR	EDR installation and coverage	All hosts should have EDR installed as per the defined policies of SL UDI program. Console report showcasing EDR coverage	During operations and maintenance phase on a monthly basis	100% coverage	0
					<100 and >=98%	1
					<98 and >=95%	2
					<95 and >=90%	3
					<90%	4
10	Inventory management	Accuracy of Inventory	Any asset provisioning / deprovisioning / update should be reported within the defined timeline in the prescribed format as per the defined policies and procedures and updated in asset list	During operations and maintenance	100%	0
					<100 and >=98%	1

#	Category / Component	Metric type	Definition	Period and Time of Measurement	Target	Severity level
			Random tests with reasonable sampling will be carried out to check for the accuracy of the inventory. MSI is expected to prepare a detailed plan for conducting these tests and submit the same to ICTA for approval and begin the tests post approval.	phase on a monthly basis	<98 and >=95%	2
					<95 and >=90%	3
					<90%	4
11	Malware detection	Malware scan periodicity	All hosts should be subjected to an anti-virus / malware scan at least once every week. SLA applies to all Active Devices in SL UDI ecosystem - physical, virtual machine, containers, Management IPs. Formula: Scan Coverage (%) = (Sum of number of active devices scanned each week of the month / Sum of number of active devices each week of the month) * 100	During operations and maintenance phase on a monthly basis	100%	0
					<100%	2
	Vulnerability assessment	Frequency and coverage	Vulnerability assessment of all IT assets should be carried out before go-live (both during implementation phase and operations and maintenance phase for new assets introduced in the	First time: At Go-live.	100%	0

#	Category / Component	Metric type	Definition	Period and Time of Measurement	Target	Severity level
			ecosystem) and at least once every quarter. MSI should discover the live hosts, identify IP ranges for scanning and verify the identified information from ICTA every quarter and also take information from asset management database to identify the scan range. MSI is expected to prepare a detailed plan for conducting these assessments and submit the same to ICTA for approval and begin the assessments post approval.	Post this, every quarter.	<100%	2
12	Web Application security testing	Frequency and coverage	All web applications, APIs, shall undergo security testing before go-live (both during implementation phase and operations and maintenance phase for new applications and APIs introduced in the ecosystem) and on a half yearly basis. MSI shall gather list of applications, APIs etc. every half yearly from the ICTA management before initiating the testing. MSI is expected to prepare a detailed plan for conducting the security testing and submit the same to ICTA for approval and begin the testing post approval.	First time: At Go-live. Post this, every half year.	100%	0
					<100%	2
			All applications shall undergo secure code review before go-live (both during implementation phase and operations and	First time: At Go-live.	100%	0

#	Category / Component	Metric type	Definition	Period and Time of Measurement	Target	Severity level
13	Secure code review	Frequency and coverage	maintenance phase for new applications introduced in the ecosystem) and on an annual basis. MSI shall gather list of applications, APIs etc. every year from the ICTA management before initiating the testing. MSI is expected to prepare a detailed plan for conducting the secure code review and submit the same to ICTA for approval and begin the review post approval.	Post this, annually.	<100%	2
14 **15**	Patch management and vulnerability remediation	Patch application and vulnerability remediation	Time taken to apply patch after the patch is released by OEM/Vendor or a vulnerability is reported. The scope should cover the following: a. All OEM devices, software, tools (including OS, DB and applications) for which patch has been released by respective vendors / OEMS. b. All vulnerabilities / findings reported through Vulnerability Assessments / Secure Code Reviews / Web Application Security Assessments etc. a. Patch/Vulnerability with critical severity (including anti-virus updation) – 24 hours on all systems b. Patch/Vulnerability with high severity – 7 days on all systems c. Patch/Vulnerability with medium/low severity – By the end of the quarter	First time: At Go-live. Post this, every quarter.	100%	0
					<100 and >=98%	1
					<98 and >=95%	2
					<95 and >=90%	3
					<90%	4

#	Category / Component	Metric type	Definition	Period and Time of Measurement	Target	Severity level
			Severity shall be defined by MSI and approved by ICTA. Patching activity shall be carried by MSI as per the patch management process and ensuring patches are applied only after applicability is determined and testing is performed. Formula – (number of systems requiring patches that were updated within timeline / Total number of systems that required patching) * 100			
16	Patch management	Regression test	Simulation testing of patches before deployment in test environment which should be replica of production. 100% of the patches to be successfully tested in test environment before deployment. Formula: percent of regression testing done = (No. of Regression Testing of Patches / No. of actual patch upgrades) * 100	First time: At Go-live. Post this, every quarter.	100%	0
					<100 and >=98%	1
					<98 and >=95%	2
					<95 and >=90%	3
					<90%	4
17					100%	0

#	Category / Component	Metric type	Definition	Period and Time of Measurement	Target	Severity level
	Change Management	Completion	Changes should be tracked formally and should be as per the Change Management procedure defined and all changes should be carried out within the timelines defined in the procedure document. 100% of change implementation as per agreed timelines for each change request. Formula – (number of changes that were done within timeline as per the process defined / total number of changes) * 100	During operations and maintenance phase on a quarterly basis	<100 and >=98%	1
					<98 and >=95%	2
					<95 and >=90%	3
					<90%	4
18	Phishing simulation	Completion	Phishing simulation exercise should be conducted (such as sending email from outside domain) for all users of ICTA, MSI and other ecosystem partners of SL-UDI including but not limited to targeting of critical roles, senior management etc. MSI is also expected to prepare a detailed plan for phishing simulation and submit the same to ICTA for approval and begin the exercise post approval. All the phishing simulation exercises shall be completed within the defined timelines. This activity should be performed on a half yearly basis during the operations and maintenance phase.	During operations and maintenance phase on a half yearly basis	100% coverage of the users for the phishing exercise and its completion within defined timeline	0
					<100%	2

#	Category / Component	Metric type	Definition	Period and Time of Measurement	Target	Severity level
20	Training and awareness	Completion	MSI should conduct periodic training and awareness sessions for all the users (ICTA, MSP and other ecosystem partners of SL-UDI) on an annual basis (including ransomware awareness sessions). The various topics to be included as part of the training and awareness should include but not limited to information security and privacy policies, procedures, Do's and Don'ts, role-based training for critical positions among others. Effectiveness of these trainings should also be measured post each training session. MSI is also expected to prepare a detailed training calendar and plan for conducting training and awareness and submit the same to ICTA or nominated party for approval and begin the exercise post approval. All the training and awareness sessions shall be conducted within the defined timelines. This activity should be performed for the first time within 3 months of Go-Live and then on a half yearly basis.	During operations and maintenance phase First time: 3 months after Go-live. Post this, annually.	100% coverage of the users for training and awareness sessions and its completion within defined timeline	0
					<100%	2

#	Category / Component	Metric type	Definition	Period and Time of Measurement	Target	Severity level
19						

Table 9.16 :Security Operations SLAs

9.10.5 Security solution review SLAs

#	Category / Component	Metric type	Definition	Period and Time of Measurement	Target	Severity level
1	Security Solution review and improvement Refer *Note-A*	Periodic security review of all tools	Periodic review and improvement of security solutions shall include (but not limited to): a. Periodic review of the security solution for all aspects such as architecture, integration with other devices, effectiveness, coverage etc. b. Fine-tuning of security solution based on inputs received from other assessments (such as risk assessment, internal audits, third party audits, vulnerability assessments, etc.) c. Suggestions / Measures to improve the effectiveness of the security solution d. Successful closure of any identified gaps or detailed plan of action for improvement e. Submission of review and improvement report to ICTA for review and approval. f. Conduct workshop with ICTA stakeholders highlighting the output of review and improvements for each security solution g. Any other activity included in the scope of work of this RFP For list of security solutions refer to the Scope of Work	During operations and maintenance phase First time: 4 months after Go-live. Thereafter, every six months Finally, before exiting the contract.	As per target	0
					Delay of <=1 month from target	1
					Delay of more than 1 month but <=2 months from target	2
					More than 2 months delay from target	3

#	Category / Component	Metric type	Definition	Period and Time of Measurement	Target	Severity level
			of this RFP. All the security solutions review should be completed within defined timeline. MSI is expected to prepare a detailed plan for conducting technology solutions review. MSI shall submit the plan to ICTA for approval. The detailed plan shall cover the scope of review, frequency, approach, methodology, best practices, report / deliverable acceptance criteria. etc. The technology solution reviews shall be conducted as per the plan approved by the ICTA. The review of all the security solutions should be done as per the timeline mentioned in 'Period and Time of Measurement' column			

Table 9.17 : Security solution review SLAs

Note-A: (SIEM solution, IDAM solution, PIM / PAM solution, NextGen Firewall (Internal and External), Network Vulnerability assessment tool, Patch management tool, IPS/IDS, Code review tool, Database Activity monitoring, Access Control System and Directory Services, Virtual Desktop Infrastructure, Web Application Firewall (WAF), HIPS, Data Leakage Prevention (DLP), Email gateway, Web gateway, SSL VPN, 2 Factor Authentication, HSM, EDR solution, Anti APT solution, Anti-DDoS solution, Security Orchestration Automation and Response (SOAR), Web Vulnerability Scanner and any other solution as mentioned in the scope of work)

9.10.6 Fraud SLAs

Definition of fraud includes identity fraud related to UIN in enrolment, authentication, logistics, CRM etc. as applicable.

#	Category / Component	Metric type	Definition	Period and Time of Measurement	Target	Severity level
1	Identify frauds in Enrolment and authentication and revise fraud rules accordingly, if any.	Completion and coverage	Prepare fraud reports as per the rules defined and revise the fraud rules based on the fraud reports or actual frauds occurring, analysis of frauds outside of SL UDI ecosystem, and brainstorming. Reports shall be submitted to ICTA every quarter during the operations and maintenance phase.	During operations and maintenance phase Quarterly	Quarterly report submission on time	0
					Delay of <=2 week from target	1
					Delay of more than 2 week but <=4 week from target	2
					More than 4 weeks delay from target	3
2	Occurrence of critical / high business	Calculated on a per event basis	Security incident / fraud whose possibility has not been reported internally prior to occurrence of the actual security incident / fraud.	Occurrence of an event in operations and	No such security incident / fraud	0

#	Category / Component	Metric type	Definition	Period and Time of Measurement	Target	Severity level
	impact security incidents / frauds (possibility of which has not been reported by MSI)		Each event will be considered as separate event for SLA calculation	maintenance phase	3= Occurrence of an event	3

Table 9.18 : Fraud SLAs

Note: T= effective date of contract

9.10.7 Business Continuity Management

#	Service Level	Metric Type	Definition	Period and Time of Measurement	Target	Severity Leve
1	DR Drill for enrolment and authentication	Compliance	Timely conduct of DR drills on half-yearly basis For each instance when DR drill is not carried out for the reasons attributable to the bidder	Quarterly	Per Instance	6
2	DR Drills (Overall)	On Time	Number of drills NOT Conducted as per the defined BCP policy	Quarterly	Per Instance	6
3	Sample restoration of data from backup tapes	Compliance	Timely conduct of successful sample restoration on fortnightly basis For each instance when either restoration is not carried out or restoration is unsuccessful for the reasons attributable to the bidder	Quarterly	Per Instance	6
4	Full Data backup from tapes	Compliance	Timely conduct of successful full backup restoration on half-yearly basis For each instance when either restoration is not carried out or restoration is unsuccessful for the reasons attributable to the bidder	Quarterly	Per Instance	8 or; 9 (if breach occurred for two consecutive instances)

#	Service Level	Metric Type	Definition	Period and Time of Measurement	Target	Severity Leve
5	RPO	Compliance	Timely and successful demonstration of RPO For each instance when either demonstration is not carried out or demonstration hasn't achieved the intended levels of RPO for enrolment and authentication	Quarterly	Per Instance	8 or; 9 (if breach occurred for two consecutive instances)
6	RTO	Compliance	Timely and successful demonstration of RTO For each instance when either demonstration is not carried out or demonstration hasn't achieved the intended levels of RTO for enrolment and authentication	Quarterly	Per Instance	8 or; 9 (if breach occurred for two consecutive instances)
					Per Instance	
7	Backup and Restore	Scheduled Backups	**Metric**: Compliance to the backup schedule as agreed upon by the MSI and ICTA **How**: Monthly reporting of successful backup activities	Monthly	100%	0
					< 100%	5

Table 9.20: Business Continuity Management