NATIONAL INSTITUTE FOR SMART GOVERNMENT
ON BEHALF OF
THE GOVERNMENT OF THE DEMOCRATIC SOCIALIST REPUBLIC OF SRI LANKA

Ministry of Digital Economy

BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS

Volume 02 of 03 - Annexure 3: Minimum Technical Specification

Two Stage Bidding Procedure

FOR THE

APPOINTMENT OF A MASTER SYSTEM INTEGRATOR (MSI) FOR DEVELOPMENT, IMPLEMENTATION AND MAINTENANCE OF THE "UNIQUE DIGITAL IDENTITY (SL-UDI) PROJECT" OF GOVERNMENT OF SRI LANKA

INVITATION FOR BIDS No: NISG/SLUDI-2025

June, 2025

Table of Contents

3.1 Introduction

This Annexure deals with Minimum Technical Requirements in four categories of components:

1. Software **(Section 3.3)**
2. Infrastructure and Security **(Section 3.4)**
3. Field Infrastructure **(Section 3.5)**
4. Biometric Software and Hardware **(Section 3.6)**

The above headings are dealt with in detail in the relevant section of this Annexure. The details bring out the minimum indicative specifications of items in all the four categories mentioned above. The MSI is expected to provide compliance of the minimum specification of each item by marking 'Y/N' as mentioned in the respective table and, reasons for non-compliance can be provided in the remarks column.

The components in the above-mentioned categories are indicative components for which minimum specifications are provided. The MSI can also quote additional components which are necessary to meet the solution requirements.

3.2 Product Benchmarking

All components proposed (hardware/software except Biometric Devices and Biometric Software), unless otherwise specified, must be as per criteria defined below:

a. The product cited must be in the Leaders Quadrant of Gartner Magic Quadrant or Leaders Quadrant of Forrester Wave or Leader in IDC MarketScape, for their product categories. Submission of a copy of the relevant section of the analysis report with the technical proposal is mandatory.

b. Reports eligible for reference must be published within the last 3 years, i.e. calendar year 2021, 2022 and 2023

c. In case less than 4 distinct products that meet the solution, requirements are available in the Leaders Quadrant of Gartner Magic Quadrant or Leaders Wave of Forrester Wave or Leader in IDC MarketScape, the vendor may offer products from the next category of these analyst reports, i.e. Challengers Quadrant of Gartner Magic Quadrant or Strong Performers Wave of Forrester Wave or Major Players in IDC MarketScape.

d. the Vendor has to *mandatorily* provide at least 2 case studies of similar complexity, sensitivity and scale where the proposed product is successfully implemented and is in operations for at least last two years i.e. calendar year 2022 and 2023. The case study should provide i) name of the client ii) description of the solution iii) scale of the solution in terms of size, number of transactions, data and users being handled iv) details of the scenario for

which the product is being used v) client reference vi) supporting evidence of having the product in operations satisfactorily from the client

e. In case Gartner Quadrant / Forrester Wave / IDC MarketScape report (for the product or product category) does not exist for a specific product or product category, the vendor must mandatory provide at least 1 case studies of similar complexity and dimension where the proposed product is successfully implemented and has been in operation for at least two years as on March 2024. The case study should provide i) name of the customer ii) description of the solution iii) dimension of the solution in terms of size, number of transactions, data and users handled iv) details of the scenario for which the product is used v) customer reference vi) supporting evidence that the product has been used satisfactorily by the customer

f. In any of the cases above, any product (hardware or software) proposed by the Vendor should not be End of Life or End of Support and the respective OEM has to provide an undertaking to this effect as part of the technical proposal submission. During the course of the implementation or the operations of the project, if any of the products is declared as End of Life or End of Support, the Vendor has to replace the product at its own cost.

g. In the table below are provided some of the COTS products (software and hardware) that the Vendor has to provide to execute the engagement. As already explained before, this table only provides an indicative requirement and it is Vendor's responsibility to bring/arrange in all required hardware and software components required for developing and running the proposed SL-UDI system in a secure and efficient manner, meeting the overall functional, technical, performance and security considerations towards successful delivery of the system:

#	Solution Component	Specification Reference
Software (Non-MOSIP Components)		Section 3.3
1	Portal Solution	Section 3.3.2.2
2	Mobile Application	Section 3.3.2.3
3	Customer Relationship Management	Section 3.3.2.4
4	BI & Reporting Solution	Section 3.3.2.5
5	Knowledge and Learning Management System	Section 3.3.2.6
6	Billing and Payment System	Section 3.3.2.7
7	Document Management System	Section 3.3.2.8

#	Solution Component	Specification Reference
8	Fraud Management System	Section 3.3.2.9
9	Enterprise Service Bus	Deleted
10	API Gateway	Section 3.3.2.11
11	Business Rules Engine	Section 3.3.2.12
12	Business Process Management Suite	Section 3.4.2.13
13	Distributed Caching	Section 3.3.2.14
14	SMS Gateway	Section 3.3.2.15
15	Messaging Platform - Publish/Subscribe Queues	Section 3.3.2.16
16	Database Solution (Relational Database Management Solution)	Section 3.3.2.17
17	Web Server	Section 3.3.2.20
18	Enterprise Container Application Platform	Section 3.4.2.5
19	Program / Project Management Tool	Section 3.4.2.13
20	Version management (Software Code Version Management System)	Section 3.4.2.15
21	Virtualization Platform	Section 3.4.2.1
22	Operating Systems	As per the requirement,
23	Performance Testing Tool	Section 3.4.2.16
24	Network Access Control	Section 3.4.1.15
25	Replication and Backup Solution	Section 3.4.2.2
27	IT Service Management Tools	Section 3.4.2.12
28	Enterprise Management System	Section 3.4.2.10
29	Database Activity Monitoring	Section 3.4.3.14
30	SLA Monitoring	Section 3.4.2.11

#	Solution Component	Specification Reference
31	Project Management Tool	Section 3.4.2.13
32	Enterprise Container Orchestration Platform	Section 3.4.2.14
33	Enterprise Grade Container registry	Section
34	Container Runtime Security and East west Traffic Inspection and Attack Mitigation Solution	Section 3.4.2.7
Hardware (Server Side)		
35	Blade Servers	Section 3.4.1.1
36	Blade Chassis	Section 3.4.1.3
37	Rack Server	Section 3.4.1.2
38	Racks	Section 3.6.2.4
39	SAN	Section 3.4.1.5
40	SAN Switch	Section 3.4.1.6
41	Tape Library	Section 3.4.1.7
42	Virtual Tape Library	Section 3.4.1.8
43	Internet Router	Section 3.4.1.9
44	MPLS Router	Section 3.4.1.9
45	Global Load Balancer	Section 3.4.1.14
46	Application Load Controller (Server / Application Load Balancer)	Section 3.4.1.14 and 3.4.1.13
47	Core Switches	Section 3.4.1.10
48	Access Switch LAN	Section 3.4.1.12
49	Data Centre Access Switch	Section 3.4.1.1
Security Component (Software)		
50	DLP Solution	Section 3.4.3.1

#	Solution Component	Specification Reference
51	Network Vulnerability Scanner	Section 3.4.1.2
52	Anti-Advanced Persistent Threat (APT)	Section 3.4.2.1
53	Privilege Access Management	Section 3.4.3.3
54	Two Factor Authentication	Section 3.4.3.4
55	Web Gateway with content Filtering & Proxy Solution	Section 3.4.3.5
56	Web Vulnerability Scanner	Section 3.4.3.24
57	Code Review Tool	Section 3.4.3.6
58	Anti-Virus Solution	Kindly refer to EDR specifications.
59	Virtual Desktop Infrastructure Solution	Section 3.4.3.7
60	Identity and Access Management	Section 3.4.3.8
Security Component (Hardware)		
61	Hardware Security Module	Section 3.4.3.9
62	Anti-DDoS solution	Section 3.4.3.10
63	Security Information and Event Monitoring (SIEM) Solution	Section 3.4.3.11
64	Patch Management Solution	Section 3.4.3.12
65	Email Gateway (Security Solution)	Section 3.4.3.13
66	SSL VPN / IPSec	Section 3.4.3.15
67	External Firewall	Section 3.4.3.16
68	Internal Firewall	Section 3.4.3.17
69	Web Application Firewall	Section 3.4.3.18
70	Host Intrusion Prevention System	Section 3.4.3.20
71	Intrusion Detection System / Intrusion Prevention System	Section 3.4.2.19

#	Solution Component	Specification Reference
72	Security Orchestration Automation and Response (SOAR) with High Availability	Section 3.4.3.21
73	Access Control and Directory Services with High Availability	Section 3.4.3.22
74	Endpoint Detection and Response (EDR)	Section 3.4.3.23
75	Security Testing Solution	Section 3.4.3.24
76	Security Racks (same as other racks)	Same as other racks
77	Network Detection and Response (NDR)	Section 3.4.3.27
78	SOC / NOC – Desktop	Section 3.4.3.28
79	SOC / NOC – Laptop	Section 3.4.3.29
80	NOC/SOC UPS	Section 3.4.3.30
81	PABX	Section 3.4.3.31
82	IP Phones	Section 3.4.3.32
Hardware (Field Side)		
83	Fingerprint Scanner – Enrolment	Section 3.5.2.1
84	Fingerprint Scanner - Authentication	Section 3.5.2.2
85	Iris Scanner – Enrolment	Section 3.5.2.3
86	Iris Scanner – Authentication	Section 3.5.2.4
87	Web Camera – Enrolment	
88	Camera – Authentication	
Biometric Solution (Software)		
89	ABIS (including Manual Adjudication)	Section 3.6.1.1
90	Multimodal SDK	Section 3.6.1.2
91	Backup and Restoration Solution	Section 3.4.2.2 and 3.4.2.3

#	Solution Component	Specification Reference
92	Other tools required to operate biometric solution (operating system, database, application server, etc.)	Section
Biometric Solution (Hardware)		
93	Blade Chassis	Section 3.6.2.1
94	Blade Server	Section 3.6.2.2
95	Rack Server	Section 3.6.2.3
96	Rack	Section 3.6.2.4
97	SAN	Section 3.6.2.5
98	SAN Switch	Section 3.6.2.6
99	Tape Library and Tapes	Section refers to the tapes section

3.3 Minimum Technical Specifications for Software

3.3.1 The key elements of procurement and their corresponding providers

They key elements of procurement and their corresponding providers are provided in the table given below, the detailed minimum technical specification is provided below.

#	Solution Component	Provider
Software		
1	Pre-registration Application (based on MOSIP)	MSI
2	Registration Software (based on MOSIP)	MSI
3	Identity Management System (based on MOSIP)	MSI
4	Unique Identity Generator (based on MOSIP)	MSI
5	Authentication Solution (based on MOSIP)	MSI
6	Partner and Device Management (based on MOSIP)	MSI
7	Integration Middleware	MSI
8	Biometric SDK	BSP
9	Automated Biometric Identification System	BSP
10	Portal Solution	MSI
11	Customer Relationship Management	MSI
12	BI & Reporting Solution	MSI

#	Solution Component	Provider
13	Document Management System	MSI
14	Fraud Management System	MSI
15	Service Billing System	MSI
16	Knowledge Management System	MSI
17	Learning Management System	MSI
18	Trusted Service Provider (TSP) and User Agency (UA) Software	MSI
20	API Gateway	MSI
21	Business Rules Engine	MSI
22	Business Process Management Suite	MSI
23	Application Server and Container	MSI
24	Web Server	MSI
25	Distributed Caching	MSI
26	Program/Project Management Tool	MSI
27	Version management	MSI
28	Virtualization Software	MSI
29	Operating System	MSI
30	Database Solution	MSI
31	Performance Testing Tool	MSI
32	Messaging Platform - Publish/Subscribe Queues	MSI
33	Large-Scale Random-Access Storage	MSI
34	IT Service Management Tools	MSI
35	Enterprise Management System	MSI
36	Replication and Backup Solution (Note: MSI and BSP may bring same solution or their separate solutions)	MSI and BSP
37	Network Access Controller	MSI
38	Email Solution	MSI
Data Center Space		
39	Data Center Hosting Space (Primary Site)	MSI
40	Data Center Hosting Space (Secondary Site)	MSI
Hardware (Server Side)		
41	Blade Servers (Biometric Solution)	BSP
42	Blade Chassis (Biometric Solution)	BSP

#	Solution Component	Provider
43	Rack Server (Biometric Solution)	BSP
44	Server Rack (Biometric Solution)	BSP
45	SAN (Biometric Solution)	BSP
46	SAN Switch (Biometric Solution)	BSP
47	Tape Library and Tapes (Biometric Solution)	BSP
48	Blade Servers (Other than Biometric Solution)	MSI
49	Blade Chassis (Other than Biometric Solution)	MSI
50	Rack Server (Other than Biometric Solution)	MSI
51	Server Rack (Other than Biometric Solution)	MSI
52	SAN (Other than Biometric Solution)	MSI
53	SAN Switch (Other than Biometric Solution)	MSI
54	Tape Library (Other than Biometric Solution)	MSI
55	Virtual Tape Library (Other than Biometric Solution)	MSI
56	Internet Router (For entire infrastructure)	MSI
57	MPLS Router (For entire infrastructure)	MSI
58	Global Load Balancer (For entire infrastructure)	MSI
59	Application Load Controller - Server / Application Load Balancer (For entire infrastructure)	MSI
60	Core Switches (For entire infrastructure)	MSI
61	Access Switch LAN (For entire infrastructure)	MSI
62	Data Center Access Switches (For entire infrastructure)	MSI
63	Enterprise Management System	MSI
64	Replication and Backup Solution	MSI
65	Network Access Controller	MSI
Network Connectivity		
66	Data Center – Interconnection Network	MSI
67	Data Centers (DC & DR) – Internet Links	MSI
68	WAN Connectivity at field offices (fixed registration centers)	MSI
69	Internet Connectivity for mobile registration centers	MSI
70.	Data Centers (DC & DR) – NOC	MSI
71	Data Centers (DC & DR) – SOC	MSI
72	Data Centers (DC & DR) – Contact Center	MSI

#	Solution Component	Provider
73	Data Centers (DC & DR) – Technical Helpdesk	MSI
74	Data Centers (DC & DR) – DRP Hosting Infrastructure	MSI
75	Data Centers (DC & DR) – DRP Head Office	MSI
76	Data Centers (DC & DR) – ICTA Head Office	MSI
Field Infrastructure		
77	Location, Civil and Electrical Work	DRP
78	Fingerprint Scanner (enrolment and authentication)	Please refer to Section 5.3 Field Infrastructure.
79	Iris Scanner (enrolment and authentication)	
80	Web Camera (enrolment)	
81	Digital Camera (authentication)	
82	Laptop for mobile registration kits	
83	Desktop for fixed registration kits	
84	Additional Monitor	
85	Scanner	
86	Printer	
87	USB Hub	
88	Background Screen	
89	Flashlight	
90	Enrolment Kit Container for mobile registration kits	
91	USB Storage Device for mobile registration kits	
Security Component (Software)		
92	DLP Solution	MSI
93	Network Vulnerability Scanner	MSI
94	Anti-Advanced Persistent Threat (APT)	MSI
95	Privilege Access Management	MSI
96	Two Factor Authentication	MSI
97	Web Gateway with content Filtering & Proxy Solution	MSI
98	Web Vulnerability Scanner	MSI
99	Code Review Tool	MSI
100	Anti-Virus Solution	MSI
101	Virtual Desktop Infrastructure Solution	MSI
102	Identity and Access Management	MSI

#	Solution Component	Provider
Security Component (Hardware)		
103	Hardware Security Module	MSI
104	Anti-DDoS solution	MSI
105	Security Information and Event Monitoring (SIEM) Solution	MSI
106	Patch Management Solution	MSI
107	Email Gateway (Security Solution)	MSI
108	Database Activity Monitoring	MSI
109	SSL VPN	MSI
110	External Firewall	MSI
111	Internal Firewall	MSI
112	Web Application Firewall	MSI
113	Host Intrusion Prevention System	MSI
113	Host Intrusion Prevention System	MSI
114	Network Intrusion Prevention System (NIPS) and NIDS	MSI
115	Intrusion Detection System / Intrusion Prevention System	MSI
116	Security Racks (same as other racks)	MSI
117	Security Testing Solution	MSI

3.3.2 MOSIP related components

The MSI is expected to refer to the table below, it shows the key components of MOSIP application. However, these are only indicated for understanding of MSI about MOSIP application and compliance is not required to be provided as part of bid response. **These functionalities and technical requirements would be part of MOSIP application whereas MSI will need to do necessary customization on the MOSIP application to meet the SL-UDI project requirements**. In addition to this, this document also provides the minimum specifications/requirements of other support applications (non-MOSIP components) which are to be deployed by MSI. MSI is expected to provide compliance for the support applications. From an architecture perspective and platform feature, it should have a thin add on functional module/utility/small system to enable the SL-UDI to add enhance functionalities

#	Key Components of MOSIP application
1	Pre-enrolment Application
2	Enrolment Software

#	Key Components of MOSIP application
3	Identity Management System
4	UDI Generator
5	Authentication Solution
6	Integration Middleware
7	Partner and Device Management
8	Identity and Access Management

3.3.2.1 Pre-Enrolment

#	Requirement Title	Compliance (Y/N)	Remarks
1	All the functions are to be exposed as Restful API / Web services.		
2	API's directly consumed by mobile need to be exposed on an API Gateway.		
3	Web Pages/Mobile screens need to be designed as per guidelines for Sri Lanka government websites & mobile applications		
4	All the scans and documents to be maintained in a DMS system		
5	API's need to be exposed for transliteration of data between Sinhala and Tamil.		
6	Enrolment Centers to be geotagged in the Pre-enrolment database.		
7	Static information like locations etc. to be maintained in a cache on a distributed cache layer.		
8	Timeslot to be locked in case the timeslot is selected by the citizen during pre-enrolment so that it is not chosen by anyone else during the time the citizen is actively entering his/her data.		
9	A common location dictionary can be leveraged for pre-enrolment. The location dictionary would contain the		

#	Requirement Title	Compliance (Y/N)	Remarks
	geographical hierarchy starting from province / state to locality levels. Dictionary to have location codes for geographical locations and Enrolment centers.		
10	A Transliteration engine to be created and used for language transliteration. This engine can also be leveraged for the enrolment clients.		
11	Acknowledgement number to be generated using a random generator		
12.	Application to leverage common SMS/Email webservices provided by the email server/SMS gateway to send Appointment related messages.		
13	Web Pages/Mobile app to show map links showing location of Enrolment centers.		
14	Languages to be used for filling would be either of English, Sinhala or Tamil		
15	Language transliteration would be done for the identified fields captured		
16	Application to be available on the Internet and Secured Intranet		

3.3.2.2 Enrolment Software

#	Requirement Title	Compliance (Y/N)	Remarks
General Client Features			
1	Capability to Store Master Data in local storage in secure encrypted fashion		
2	Ability to Import/Query Pre-enrolment Data online using Open API's		
3	Ability to Pull up Citizen Record Locally from Imported Pre- enrolment Data		

#	Requirement Title	Compliance (Y/N)	Remarks
4	Support for Multiple Pre-enrolment Data Sources		
5	Ability to Print Enrolment Receipt		
6.	Ability to Capture Usage Metadata for Analysis		
7	Support for Local Sri Lankan Languages for transliteration purpose		
8	Support for Audio Messaging (confirmations, instructions, etc.) in Languages in Sri Lanka		
9	Support for Exceptional conditions such as ability to handle residents with disabilities, citizen without documents etc.		
Biometric Data Collection			
10	Ability to Integrate with Fingerprint Reader and Capture Finger Prints as per Specification		
11	Ability to Integrate with Web-Camera and Capture Photo as per Specification		
12	Ability to Integrate with IRIS Scanner and Capture Iris as per Specification		
13	Ability to Integrate with Retina Scanner and Capture Retina Scans as per Specification		
14	Ability to Export Enrolment Data		
15	Ability to Check Biometrics Quality as per Standards		
16	Ability to Perform Segmentation		
17	Ability to Retry Specific Number of Times		
18	Automatic Audit of Forced Capture		
19	Support for Local Duplicate Checks		
20	Biometric Sample		
21	Biometric Bundle		

#	Requirement Title	Compliance (Y/N)	Remarks
22	Ability to generate Individual Biometric Templates from Raw Biometrics Captured		
23	Ability to generate multimodal biometric templates from Raw Biometric captured.		
Client Manageability			
24	Ability to Easily Install the Client/Client Patch using a Dongle		
25	Ability to Auto Update from a Central Server		
26	Ability to Upgrade with Small Patches		
27	Ability to Export and Import Master Data		
28	Retention of Data till Server Receipt Confirmation		
29	Recovery of Data in case of Disk Failure		
30	Ability to freeze client once a new version is available, after a certain cutoff date		
31	Ability to render packets as expired once they are older than a particular date		
Client Security			
32	Support for Operator Authentication – Biometric, Multi-factor		
33	ACL Based Authorization and Task Management		
34	Support for Detailed Audit Trail		
35	Ability to Secure Enrolment Data from Theft and Illegal Transmission		
36	Ability to Secure Enrolment Data from Tampering		
37	Ability to Secure Enrolment Client from Tampering		
38	Ability to Authorize Supervisory Overrides		

#	Requirement Title	Compliance (Y/N)	Remarks
39	Ability to Protect Data from Malware and Viruses		
40	Ability to Protect Specific Master Data from Tampering		
41	Ability to provide access to secure configurations such as public keys, enrolment packets by providing read only access to the client software/enrolment officer's account.		
42	Ability to capture photos of persons with exceptional conditions (Handicap etc.) as evidence of exception as per photo specifications.		
43	Ability to integrate a hardened VM through a dongle		
44	Ability to store Biometric of Enrolment officer in secure and tamper proof fashion for local login.		
45	Ability to only retrieve pre-enrolment data for residents on the day of enrolment only. This data should only be downloadable by the enrolment officer of the center chosen by the citizen on the day of appointment.		
46	Ability to generate Unique EIN number locally. This unique number could be a concatenation of Device Id/Dongle id which is the id of the device on which the data is captured.		
Integration Features			
47	Ability to Synchronize Master Data with SL-UDI-DS Servers		
48	Ability to Upload Enrolment Data to SL-UDI-DS Server through Secure Channel		
49	Ability to Receive Processing Confirmations for Enrolment Requests		
50	Ability to work in Online mode – where minutia + Demographic details can be sent to SL-UDI-DS through an online web-service and get near real time		

#	Requirement Title	Compliance (Y/N)	Remarks
	YES or NO confirmation that the citizen is successfully deduped and good for a UDI generation		
51	Ability to integrate with SL-UDI-DS in batch mode where complete packet is sent in a batch for detailed evaluation and UDI generation.		
Demographic Data Collection Features			
52	Capturing UDI (Unique Digital ID) Data Fields as per Specification		
53	Supporting Language transliteration for Sri Lanka		
54	Supporting local data validation using local master data stored.		
55	Supporting address validation with master data.		
56	Mapping zip codes/region codes to regions /provinces etc.		
57	Ability to auto suggest fields such as names, locations etc. based on live fuzzy matching from a Local Location and Names Master data		
58	Ability to integrate with SL-UDI-DS to confirm packets that have been successfully received at SL-UDI-DS		
59	Printing Screen Features		
60	Ability to generate enrolment receipt with a unique enrolment reference number		
61	Ability to transfer bulk packets to SL-UDI-DS		
62	Ability to transfer data over a secured intranet		
63	Ability to transfer data in encrypted format		

3.3.2.3 Identity Management System

#	Requirement Title	Compliance (Y/N)	Remarks
General Server Features			
1	Ability to Perform Unbundle and Consistency Check		
2	Ability to Process Batch Enrolments with multiple processing hops		
3	Ability to Validate Enrolment Requests		
4	Integrate with Biometric Server for De-duplication		
5	Publishing Events to Other Parts of the System		
6	Ability to Audit Enrolment Processing		
7	Ability to Store Intermediate Enrolment Data		
8	Generating UDI Number as per Specification		
9	Tracking Statuses Based on Enrolment Workflow		
10	Ability to Manually Take Decisions on Exceptions		
11	Should support batch processing mode with consistency checks		
12	Processing stages to be loosely coupled through messaging queues		
Integration Features			
13	Supporting Integration with Enrolment Clients for Master Data and software Update		
14	Supporting Integration with Enrolment Client for Enrolment Data Upload		
15	Integration with Biometric Server		
16	Integration with Authentication Server		
17	Integration with Letter Delivery System		
18	Responding to Enrolment Requests for Feedback to Enrolment Client System		

#	Requirement Title	Compliance (Y/N)	Remarks
19	Integration capability with SMS and Email servers		
20	Capability to Dynamically allocate Biometric Deduplication requests to the Biometric Identification solution based on failure rates and response time		
21	Integration with electronic birth registry using APIs		
22	All Integration with external system shall be implemented as run time plug-in libraries, allowing for the reuse of official container images to facilitate simpler upgrades and maintenance process.		
Data Storage			
22	Ability to Store Data Across Multiple Storage Schemes		
23	Ability to Partition Data Horizontally and Vertically and Distribute across Nodes		
24	Ability to Secure Data Storage for all UDI Data		
Batch Processing Framework			
25	Ability to administer one or many jobs that may be scheduled to run periodically or at specified times of the day. Capability to maintain a job repository that can survive Node restarts.		
26	Ability to query list and statuses of various executing jobs.		
27	Ability to configure exception handling strategies and implementations i.e. ability to automatically or manually restart failed jobs.		
28	Ability to execute multiple jobs in parallel and to parallelize step execution within jobs.		
29	Ability to process (read) data from multiple sources and write to different destinations. The sources and destinations relevant to IDMS are regular File system, Distributed File System, RDBMS, Non-Relational Databases and Messaging queues.		

#	Requirement Title	Compliance (Y/N)	Remarks
30	Ability to isolate batch processing framework interfaces from the actual job implementation.		
31	Provide the ability to configure 'maximum number of retries.'		
Load Balanced Managed Queues			
32	The queues permit location transparency of the Event Driven instances.		
33	Ensure delivery of a message to a single subscriber		
Non-Functional Requirements			
	Scalability and Performance		
34	As a general principle, the system shall be designed specifically for country scaled deployment ensuring scalability, High Availability and Security to handle large volumes of authentication requests		
35	Application should be able to scale within servers, across servers. Micro-service-based architecture for all platform services for modularity and scalability.		
36	Stateless nature of the stages in the UID generation workflow to ensure horizontal scalability		
37	Application should use an asynchronous messaging middleware as transport between stages and use of store and forward semantics.		
38	Application should use multiple stores to distribute data across multiple data stores along with partition and sharing for performance and scalability reasons.		
39	The solution should have the ability to perform enrolment within the expected time under peak load.		
40	Minimal data transformations between the IDMS processes and third-party systems such as the biometric servers.		
41	Minimal I/O processing and I/O wait time by reducing inter- process control flow by co-locating the process		

#	Requirement Title	Compliance (Y/N)	Remarks
	and data required for it within the same process as much as possible.		
42	***Security***		
43	The Application must safeguard against multiple security hazards including but not limited to: Numbers from 44 to 68		
44	Submission of UDI enrolment data packet by un-authorized enrolment agencies and operators.		
45	Unauthorized or any un-intended tampering of citizen enrolment data.		
46	Submission of malicious scripts to the IDMS		
47	Unauthorized machines connecting to the SL-UDI-DS and IDMS		
48	DOS Attacks		
49	XML injections/XML manipulations		
50	Manual recovery of UIN/Biometric data from decrypted files		
51	Manual recovery of UIN/Biometric data from OS files		
52	Manual recovery of UIN/Biometric data from database		
53	Easy numbers in the generation		
54	Enumeration of UDI numbers from log files		
55	Tampering with dedupe threshold or any business rules		
56	Spoofing of machines in the compute grid		
57	Unauthorized back-end scripts running independently over the DB		
58	Hardcoded passwords or keys		
59	Deletion of UDI record		
60	Modification of UDI records		

#	Requirement Title	Compliance (Y/N)	Remarks
61	Unauthorized exception handling on client		
62	Time bound anomalies in code		
63	Logic bound anomalies in code		
64	Command injection attacks		
65	Object injection attacks		
66	Replay attacks		
67	Distributed processing with concurrent deduplication		
68	SQL injection attacks		
69	***Interoperability***		
70	Ability to interoperate with other systems/services using open interfaces and ability to continually re-factor and/or replace specific components without affecting rest of the system.		
71	Use of standard and widely accepted interface standards for communication protocols, integration approaches and patterns should be used.		
72	Component design should follow design principles and interface abstraction using published public API or define an API that will be implemented by all involved third party solutions		
73	Adoption of efficient data exchange formats that are acceptable to different sub-systems running on potentially different runtimes.		
74	Should make use of open standards.		
75	The product shall implement OpenID connect (OIDC) flows to enable standardized, secured user verification, supporting quick and seamless integration for relying parties through the use of pre-existing OIDC libraries. Only secured OIDC flows such as authentication code flows with proof key for code exchange (PKCE) where applicable shall be supported to ensure that resident data is handled with the highest level of security.		

3.3.2.4 Authentication Application Software

#	Requirement Title	Compliance (Y/N)	Remarks
ETL/ELT			
1	Solution should provide native connectivity for different types of sources from database, flat files, unstructured data, directories etc.		
2	In case of version updates / migration to a higher version, the product should be able to seamlessly migrate existing ETL/ELT jobs with minimal changes		
3	The system should be resilient to temporary system failures.		
4	ETL/ELT tool interface allows the developer to preview data from the Source Systems for quick profiling and on a need basis		
5	Tool should show adequate throughput when sourcing large files		
6	Tool should support using SSH FTP as connection to pull the required files		
7	a. The tool should provide standard out of the box functionalities for Manipulation of data, Aggregation of data, Enrichment of data, Grouping of data, Maintaining transactional boundaries, Dynamic creation of files, Filtering of data, Rich set of connectivity, Parameterization. b. The tool shall provide extensive built in library for transformations so as to minimize writing of code c. Tool should also provide ability to add logic via custom transformation not supported by standard transformations		
8	Single administration console for user management across multiple environments Controls via GUI & command line for: a. Start Up / Shutdown of ETL/ELT servers / services b. Configuration of server / service parameters		

#	Requirement Title	Compliance (Y/N)	Remarks
	c. Backup / restore of repository contents d. Role based Security Access and privileges at a granular level e. Provide options to integrate with LDAP and likewise user management system f. Allow monitoring of services and resilience g. Provide easy interface for product upgrades and emergency fixes		
9	Tool should have capability to optimize resources such as memory, cores available and other system resources		
10	The tool should support data source (and target) ranging from GBs to TBs without significantly degrading performance. The solution should therefore provide horizontal scalability and vertical scalability with minimum to no-downtime.		
11	Focus exclusively on resident authentication and verification only. < Additional functionalities such as role and session management are expected to be handled by external systems >		
Data Quality Management Tool			
11	Ability to provide integration of data quality functionality as API/ web service to other portals/business applications (especially internal applications)		
12	Range of pre-built analyses on individual attributes/columns/fields, such as min, max, frequency distributions of value and patterns, etc.		
13	**Dependency analyses**: Range of pre-built analyses to identify relationships, patterns, integrity gaps, duplication between and across multiple attributes/columns/fields and across tables, databases, and files		

#	Requirement Title	Compliance (Y/N)	Remarks
14	**Analyses on data profiling:** Pre-built functionality to analyze trends in profiling results over time. In addition to this, tool should have ability to configure and execute user-defined profiling analyses		
15	a. Ability to perform parsing operations to parse data into multiple fields such parsing name into first name, last name etc., or parsing address in building, locality, city, landmark etc. b. The solution should also provide provision for customization of parsing schemes through GUI		
16	Ability to define rules for common standardization and cleansing operations, such as formatting of addresses, telephone numbers etc.		
17	a. Ability to define rules for common standardization and cleansing operations b. Facilities for developing custom transformations and extending packaged transformations		
18	a. Deterministic Matching Capability b. Pre-defined algorithms for fuzzy matching for demographic attributes c. The solution should be able to integrate a hybrid approach towards matching of entities and combine both deterministic and probabilistic approaches to provide optimum results.		
19	a. Ability to weight, prioritize, and tune matching rules (for example, to optimize the frequency/number of potential matches, or the "tightness" or "looseness" of matching) b. Facilities for implementing and customizing rules by which duplicate or related records can be merged into a single record		

#	Requirement Title	Compliance (Y/N)	Remarks
20	a. Ability to deploy monitoring rules within existing applications and data flows, or as a stand-alone process b. Capability to generate alerts of various types (email, error message, etc.) when monitoring rules are violated c. Provide DQ monitor repository for storing various predefined rules, action. These rules and actions should be re-usable.		
21	Team-based development capabilities such as version control and collaboration		
22	Collection of run-time statistics to determine usage and efficiency, as well as an application-style interface for visualization and evaluation		
23	a. Ability to perform data cleaning during transportation of data from source systems b. Ability to perform data cleaning during migration of historical data		
24	a. Ability to integrate with data extractors/crawlers to access semi-structured / unstructured data, such as e-mail, Web sites, office documents and content repositories b. Ability to integrate with the Big Data Solution proposed by the BISP as well as with the integration solutions for Big Data Systems (Sqoop, Flume etc.)		
Data Warehouse			
25	Support for Relational and non-relational data sources		
26	Structured flat file load - predefined formats		
27	Interaction capability with various “non/semi-structured” file formats such as XML, JSON, CSV, pdf, doc, images and fixed format files etc.		

#	Requirement Title	Compliance (Y/N)	Remarks
28	Accept different data types/formats for similar data elements (e.g. different date formats) and store them in a single uniform format		
Analytics			
29	If needed, the proposed solution should be capable of executing advanced analytics algorithms in database and without any need for taking the data out of the database.		
30	**Predictive Analytics:** Predictive analytics to explore large quantities of data and discover relationships and patterns and identify anomalies using **univariate and multivariate techniques**		
31	The proposed solution shall be capable of performing data analytics **on both structured and unstructured data**		
32	System should bring in **advanced algorithms widely used for purposes** of Data Mining.		
33	Support for **Identification of anomalies, outliers etc**. in data		
34	a. BI System shall bring in advanced Machine Learning Techniques including capabilities for Supervised Learning, Clustering, Dimensionality Reduction, Neural Nets, Reinforcement Learnings b. Should support advanced decision trees methodologies. c. Support multiple regression techniques both linear and non- linear, cross validation, fast forward stepwise least squares regression d. Should be able to incorporate prior probabilities into the model development process		
35	Development of criteria for choosing between re-weighting and imputation Approaches		

#	Requirement Title	Compliance (Y/N)	Remarks
36	a. Solution has to be equipped with various corrective measures for exceptional handling whenever exceptional patterns in data are observed b. Generation of alerts based on implemented functionalities/models relating to text analytics, network analytics, geospatial analytics etc.		
Visualization & Reporting			
37	Proposed solution should be capable of seamless integration with leading Office tools		
38	Data Visualization solution should be capable of integration with leading analytics, EDW and BI Solutions to provide interactive visualizations. Preference would be given to solutions with auto charting facilities.		
39	Proposed solution should be capable of generating highly formatted, interactive visualizations with parameterization, slice & dice and drill down/ drill through capabilities. Should also have strong ad hoc visualization generating capabilities and have strong visualization recommendation features.		
40	The solution should have the ability to format (page size, row, columns, fonts, colors, tables etc.), allow data manipulation (slice & dice multidimensional data on the fly, pivoting, sorting, ranking, rearranging columns, etc.)		
41	The solution must enable business user to mash-up structured and unstructured data and create visualizations integrating data from both the repositories (structured and unstructured)		
42	Provide ability to change representation layout and visual formatting on the chart (e.g. sunbursts, bars, columns, radial bars, maps etc.). The users should be able to alter visualizations rapidly into new chart types but also back-up, redo and undo work.		

#	Requirement Title	Compliance (Y/N)	Remarks
43	The solution should have user friendly GUI to enhance end user experience and should support export of resulting data to other applications such as Excel, Notes, and CSV.).		
44	The solution should have integration capabilities e.g. ability to integrate in the proposed SL-UDI Portal. The solution should be able to publish all visualization elements (at least in static format) on to a portal and have the ability to archive them.		
45	The solution should be able to distribute reports and also have the ability to save data for later use or to a local PC/laptop or for other users to view. It should support offline viewing. It should be able to send reports electronically to other users.		
46	The proposed application should be extendable / scalable to manage visualization based on big data.		
47	Should be able to source data from identified and a few source systems (mostly flat files) to aid in analysis and decision making		
48	Should support both Rich Client Visual Analysis environment as well as Web Based link analysis & visualization of complex networks		
49	Provide features for dynamic filtering the entities based on attributes and render in form of Histograms & Heat maps		
50	Wherever required, the solution should allow selected users to interact and explore data residing in any layer of the BI System (ODS, DW, the staging layer, data in DFS), through an easy-to-use visualization mechanism. End users themselves should be able to select the required data and load the same for visualization		
51	Unified Exploration & Visualization - The steps of querying, exploring and visualization of data must be		

#	Requirement Title	Compliance (Y/N)	Remarks
	unified in a single process. The data and the visualization must work in tandem		
52	Should have drill-down capabilities (ability to drill down to various levels of a hierarchy).		
53	Drill-down and drill-in capabilities would be able to call other applications.		
	Reporting Capabilities		
54	The BI application needs to have the BI capabilities like Drill down, Slice and Dice, Multi-Dimensional Analysis, Ad-Hoc analysis		
55	Proposed solution should have provisions for auto charting (based on underlying data) and interactive reporting		
56	The proposed software needs to have capability to extend or integrate with components of advanced analytics.		
57	The proposed BI solution should allow the users to access reports, receive alerts to update report over web, on the network and on mobile devices		
58	The solution should provide native access to leading RDBMS and Non-relational database solutions and should have capability to connect with big data components based on HDFS like spark, hive, impala, No SQL.		
59	Given that most users would use office documents like word, excel and power point documents in day-to-day operations, the BI solution must provide an ability to embed application data in the form of graphs and charts into Office documents while providing role-based access to data.		
60	a. Tool must provide an analytical solution enabling a web based ad-hoc analysis where end user can		

#	Requirement Title	Compliance (Y/N)	Remarks
	interact with logical view of information creating charts, pivot tables, reports, gauges, dashboards etc. b. It should have facility to create ad hoc queries through use of simple business terms for querying the data sources c. It should have facility to save the queries and edit the same in future to derive newer queries d. It should have the ability for the business users to create their own charts and graphs based on their requirement. It should have the ability to convert a tabular report into a chart by passing the relevant parameters.		
61	Should integrate with a mapping Solution / have one of its own to show geographic activity in terms of a map.		
62	Should have ability to integrate with LDAP / ADS / any other enterprise authentication mechanism for single sign on		
63	The Solution should support object level as well as row level security		
64	a. Save and Share Capability: After the end user spends time and creates, adds, deletes, changes the pivot table views, he/she should be able to save these changes and share the updated view with a group of users. b. Ability to export the data or report to spread sheets including graphics and to flat file and into CSV, pdf, xls, html formats c. Ability to directly send the report for printing on a LAN printer / personal printer d. Dashboard Capability: End users should interact using rich, interactive, role based, easy to understand web-based dashboard. It should be able to represent and highlight changes in the data in the form of live		

#	Requirement Title	Compliance (Y/N)	Remarks
	reports, prompts, charts, tickers, pivot tables and graphics. e. Should allow end users to create their own dash boards via a simple drag and drop mechanism		
65	**OLAP Analysis Capability:** Ability to do OLAP analysis, depending on the requirement, needs to be catered to by the Solution.		
66	The BI solution should provide ability to do analysis on both operational data and historical data.		
67	The BI solution must be hot pluggable in any hosted data source. This means that BI layer should be able to work seamlessly with any popular data source, business application and security infrastructure		
68	The disconnected mode of Dashboards - The BI Solution should have the facility to generate dashboards that can be used by authorized users without having access to the BI server / Internet.		
69	Information dissemination via mobile with compatibility required for standard operating systems (such as iOS, Android, Windows)		

3.3.3 Non-MOSIP Components

3.3.3.1 Queue Management System

#	Requirement Title	Compliance (Y/N)	Remarks
1	The solution should support scheduling of appointments through web portal as well as through mobile application		
2	The solution should provide personalized notifications and alerts to be sent to the users who are in waiting in a queue for availing their service.		
3	The solution generates a ticket that will showcase the complete details of the service that the user is going to avail.		
4	The software should display the number of waiting users, the length of the line and also the complete digital signage functionality.		
5	The solution should be configurable through a web portal and minimal customization should be required for providing the services		
6	The solution should support collection of timely feedback from users on service standard, experience and areas of improvement		
7	The solution should be able to provide real-time information to optimize operations, while generating analysis and reports to aid in planning, management and future projections.		
8	The solution should ensure that user data is secure and protected and that there is functionality to meet National data protection guidelines		
9	The solution should be scalable and able to meet the growing demands in terms of number of contact centers, offices and services		
10	It is required to provide services over a large geographical area and hence solution should be able to provide omnichannel experience in physical and digital environments		
11	The solution should be able integrate with all customer channels such as web portals, mobile apps, messaging services, social media platforms, live chats etc.		

#	Requirement Title	Compliance (Y/N)	Remarks
12	The solution should be able to collect data and feedback from all touch points		
13	The solution should support customization if required to meet integration requirements of third-party applications		
14	The solution will integrate with the CRM solution, SMS and Email gateway etc.		
15	The solution should support API based integration for real time processing.		
16	Digital Signage systems are placed in the waiting area where all the promotional videos are played along with the information about the current serving tokens.		
17	Token Machines are installed at the strategic points where users walks-in and gets a token for the service they want to seek		
18	The solution should adhere the overall standards of the ID solution of reliability, availability, scalability and performance		

3.3.3.2 Portal Solution

#	Requirement Title	Compliance (Y/N)	Remarks
1	The portal should be capable of being deployed in High-availability and load balanced manner at both DC and DR.		
2	The portal should be web-based portal based on open standards		
3	The portal should have in-built security controls to protect against any malicious activity.		
4	The portal should support integration with the centralized LDAP/Identity Management solution for single sign-on		
5	The portal should have the capability to integrate with enterprise document management system and Content Management System etc.		

#	Requirement Title	Compliance (Y/N)	Remarks
6	The portal should support multiple languages in Sri Lanka (Sinhala/Tamil min.)		
7	The portal should be accessible through Mobile Devices and support multiple mobile OS such as Android, and iOS		
8	The intranet portal must offer key capabilities including User Profile management, Micro-blogging, Bookmark, Communities, File upload & sharing, Wikis, Blogs, Forums, Event Calendar, Media Gallery, Ideation Blogs, Activities, Activity Streams, Reporting Structure, tagging, Rating, publishing Workflow etc.		
9	The portals should provide the granular access to file such as Reader access, Editor access and owner.		
10	Must allow reporting capabilities such as number of visits, most active content, top contributor, top content and top activity and other ad-hoc reports.		
11	The solution should provide version control for files		
12	The solution should have designer tool to perform any customizations, if required		
13	The solution should integrate with the Mail and Messaging solution proposed by the bidder.		
14	Solution must support major browser such as Apple Safari, Google Chrome, Microsoft Internet Explorer and edge, Mozilla Firefox, opera etc.		
15	The intranet portal should be deployed in High-availability and load balanced manner at both DC and DR.		
16	The intranet portal should be web-based portal based on open standards		
17	The intranet portal should have in-built security controls to protect against any malicious activity.		
18	The intranet portal should have the capability to integrate with enterprise document management system		

3.3.3.3 Mobile Application

#	Requirement Title	Compliance (Y/N)	Remarks
1	While building the mobility solutions services should be available in a low bandwidth scenario. Mobile solution usage mostly will be user on road/transit, example by the flying Squared		
2	The Mobile Application should provide an intuitive and user-friendly GUI that enables users to navigate and apply actions with ease. The GUI should be responsive with very little or no delays or time lag at launch or whilst navigating through screens.		
3	It should enable ease of configuration and changes to existing GUIs and support the introduction of new screens.		
4	It should provide on screen tips and online help to aid users while interacting with it.		
5	Should make use of data available in the existing database and reduce duplicate data entry		
6	Incorporate analytics into mobile app, to track and identify users experience and actions.		
7	Apps should be easily customizable and easy to Administer data in the SL-UDI database		
8	Network level security, traffic should be encrypted using secured connectivity		
9	Spatial mobility should also be considered to support GIS services		
10	Should structure overall content with proper tagging to make them screen reader friendly.		
11	Application should ensure compatibility with all platforms such as, Android and Mac iOS.		

#	Requirement Title	Compliance (Y/N)	Remarks
12	Solution should develop resolution independent design structure i.e. Mobile Application should adjust itself automatically as per the screen resolution of the Mobile		
13	Mobile Apps should work flawlessly across different platforms		
14	There should be minimum use flash contents so that home page should be loaded quickly		
15	Apps should not occupy excess client's Mobile RAM (should be <200MB).		
16	Should provide Role Based Access control		
17	Should come with mobile threat prevention and recovery system		
18	Should have facility to download and upload files		
19	Mobile development platform/framework should be leveraged for development of mobile application		

3.3.3.4 Customer Relationship Management

#	Requirement Title	Compliance (Y/N)	Remarks
1	A single point of contact for services and business operations queries and grievances. The system shall be designed to serve as a single platform for all interactions.		
2	The CRM solution must provide for logging of calls, categorization, ticket generation, status tracking and resolution time tracking.		
3	The CRM solution must be integrated with other SL-UDI-DS to access information of residents, enrolments under processing etc.		
4	The CRM solution shall maintain history regarding complaints/grievances of and shall also obtain data		

#	Requirement Title	Compliance (Y/N)	Remarks
	from relevant databases securely using Secure HTTP or a better solution.		
5	CRM solution should be integrated with Document Management System (DMS)		
6	The CRM solution shall be integrated with IVR/Voice, SMS Gateway, USSD Gateway, Email, messaging platforms, social media platforms, Live Chat and FAX for both inbound and outbound communication.		
7	The CRM solution should provide special functionality of handling handwritten letters as a part of grievance redressal. The letters shall be scanned and maintained in the CRM solution.		
8	CRM solution should be integrated with BI (ETL Tool) to send the data to BI System for reporting and analytics.		
9	Real-time decision support (analytics) to understand nature of inquiries and complaints and customize responses and interactions accordingly		
10	The CRM solution shall support relevant screen pop-ups, to the helpdesk/contact center agent along with the details of the previous calls during the last 30 days.		
11	The CRM solution should support call routing functionalities.		
12	Support languages in Sri Lanka as per the need		
13	The CRM solution shall provision for both inbound and outbound channel support with associated technologies as mentioned below: a. CRM (product) b. IVRS c. ACD d. CTI e. Call logger f. Quality Management System		

#	Requirement Title	Compliance (Y/N)	Remarks
	g. Email response system h. Reporting systems i. Scanning Solution for letters & faxes j. Messaging Platforms k. Social Media Platforms management l. Live Chat		
14	For queries which cannot be answered using a pre-defined script, the query shall be logged in the CRM and track them to resolution.		
15	The CRM solution proposed must have provision to create and maintain knowledge bases to assist helpdesk and contact center users, thereby enabling them to resolve the queries faster and being effective in problem diagnosis, trouble shooting and resolution.		
16	The CRM shall provide advanced analytics services to reduce queries & grievances and improve quality of service by the contact center. Examples include: root cause analysis of top 10 queries/complaints across regions, early detection of issues, number and type of calls by the users in the last 6 months, etc.		
17	The CRM solution shall also measure performance indicators and SLAs for contact center and contact center agents. Some examples of the measurements are a. Response and Resolution times for grievances b. Average Handling Time (AHT) and c. IVRS Efficiency d. First Time Resolution (FTR) e. User interaction drop rates such as call drop rates, user interactions not responded etc.		

3.3.3.5 BI & Analytics

#	Requirement Title	Compliance (Y/N)	Remarks
1	Use of Analytics Reporting Services has been considered to be the most important aspect of the integrated SL-UDI SI system, in terms of getting intelligent insights out of the streaming data received real-time from smart devices and social media apps. The users will be able to generate the Analytics Reports at various levels to perform predictive analysis, operational analysis, risk modelling, statistical analysis and monetization analysis for taking informed decisions. The proposed solution architecture will make use of the open standards framework compatible with the technology pl The Reporting tool should have robust visualizations such as graphs, charts, and histograms.		
2	The reporting tool should have slicing and dicing features facilitating ad-hoc management reporting on the fly.		
3	The reporting tool should have basic statistical modelling properties, so that users can create clusters, regression analysis, and other modelling techniques dynamically.		
4	The reporting tool should output data in various formats.		
5	The Reports generated by the system should be made accessible through API or an interface (for portal) to be viewed by the authorized users. The tool should enable different types of users to perform analysis on data across the Enterprise without the need to Subset / sample / create multiple views of data. The interface for the authorized users should be simple with user friendly features such as drop-down list, drag and drop utilities etc., and should be built with focus on users with elementary statistical knowledge		
6	DBAs and end users to use a web-based portal to evaluate and understand the state of their system		

#	Requirement Title	Compliance (Y/N)	Remarks
7	The management console should be Web based and should not require any client installation.		
8.	The solution shall provide a common management console to monitor multiple systems in Test, Development, production systems across multiple instances and across locations		
9	The proposed solution should be capable of seamless integration with leading Office tools both for import and export of data and reports in multiple formats. The solution should allow data to be accessed from any industry standard data source using native connectors. It should also allow data load jobs to be scheduled to automate the process of loading data into the system for Analysis Data Visualization tool capable of interactive visualizations. Preference would be given to tools with auto charting facilities		
10	The analytics and reporting solution should integrate a market leading Data Visualization tool capable of interactive visualizations. Preference would be given to tools with auto charting facilities		
11	Solution should be capable of generating highly formatted, interactive reports/ dashboards with or without parameters. Should also have strong ad hoc report generating capabilities		
12	The solution should have the ability to format (page size, row, columns, fonts, colors, tables etc.), allow data manipulation (slice & dice multidimensional data on the fly, pivoting, sorting, ranking, rearranging columns, etc.). The solution should have drill-down capabilities (ability to drill down to various levels of a hierarchy).		

#	Requirement Title	Compliance (Y/N)	Remarks
13	The solution should have the capability of raising exception alarms (e.g. email notification). Should provide for exception reporting (ability to set certain thresholds).		
14	The solution should have user friendly GUI to allow easy generation of reports and exporting capabilities (ability to export resulting data to other applications such as Excel, Notes, CSV.).		
15	The solution should have integration capabilities e.g. ability to integrate in existing portal. The solution should be able to publish all the reports on the portal and have the ability to archive reports.		
16	The solution should provide for a browser-based interface to view reports.		
17	The solution should have the ability to schedule reports.		
18	The solution should be able to sort/filter without re-querying.		
19	The solution should be able to distribute reports and also have the ability to save data for later use or to a local PC/laptop or for other users to view. It should support offline viewing. It should be able to send reports electronically to other users.		

3.3.3.6 Knowledge and Learning Management System

#	Requirement Title	Compliance (Y/N)	Remarks
1	Should have the ability to create new courses		
2	Must have the ability to add course material to new/existing courses		

#	Requirement Title	Compliance (Y/N)	Remarks
3	Support for online training, instructor-led training, and informal learning objects (such as on-the-job training) to be assigned and tracked by the LMS		
4	Allow administrator to select the option for learner to mark a user-defined learning object as complete		
5	Has the ability to integrate with thousands of courses from any vendor or custom content built by a customer that follows AICC or SCORM standards		
6	Mass registration for multiple learners to a course		
7	Interoperability with NON-standards compliant content		
8	Manage course properties (CEU, duration, test requirements, etc.)		
9	Can deactivate a course without removing it from the LMS		
10	Set the duration of course accessibility based on the registration date (definition of an expiration period)		
11	Manage the gradebook by marking any learning object as complete or incomplete		
12	The learner can self-register for learning offers		
13	The learner can unsubscribe from all learning offers		
14	The learner can unsubscribe from the training given by an instructor		
15	The learner can register at the ILT course level		
16	Ability to define prerequisites for courses		
17	Assign multiple instructors to a class and/or session		
18	Ability to set (and override) maximum students for a course at session level		

#	Requirement Title	Compliance (Y/N)	Remarks
19	Access online resources (i.e. PDF instructor posted for a course)		
20	Registration and cancellation of registrations for learning activities		
21	Registration confirmation by email		
22	Manage a queue of registration requests (approve/deny)		
23	Courses can be grouped into programs and subjects in the catalog		
24	Create, edit, and delete learning plan templates		
25	Manage Waiting List and List		
26	Edit the content of a learning plan for all users		
27	Set due dates for full completion of the plan (i.e. certification deadline)		
28	Require that courses be completed in a set order		
29	Assign due dates to employee learning activities		
30	Certification tracking		
31	Survey Creation Ability		
32	Ability to set passing scores for tests		
33	Possibility to require passing the test to complete the course		
34	Define how many times a test can be attempted		
35	Select general business rules for how users will access the catalog and register for courses		
36	The report can be run on demand via the LMS interface		

#	Requirement Title	Compliance (Y/N)	Remarks
37	Web-based reporting interface with results appearing in the application workspace		
38	The report can be printed from the application workspace without having to export		
39	Ability to export report data		
40	Report formats (browser view, .xls, .csv, .doc, etc.)		
41	Ability to complete ILT and informal training		
42	Report on the progress of the learning plan in groups / in the world		
43	Student Transcripts (Viewable and Printable)		
44	Dashboard Reports and Analytics		
45	Auto-Registration/Un-registration by Email		

3.3.3.7 Billing and Payment System

#	Requirement Title	Compliance (Y/N)	Remarks
1.	The solution should support template customization of invoice templates		
2.	Solution should be able to generate invoices for the services available by end users		
3.	The Solution should capture all the required tax information for each transaction and include the breakup in the invoice		
4.	View all user transaction history in one place		
5.	Customize: add logo and colours		

#	Requirement Title	Compliance (Y/N)	Remarks
6.	Organize the content of the invoices with drag-and-drop line items		
7.	Automatic and seamless accounting software integration		
8.	The solution should support ~~online~~ payment functionality through cash, banks, credit and debit cards, wallets etc.		
9.	The solution should be able to integrate with the CRM solution		
10.	The solution should have reporting functionality to provide standard reports on daily/weekly/monthly/annual basis		
11.	The solution should be able to integrate with BI and Analytics solution to derive advanced analytical reports.		
12.	The solution should be able to support multiple tax rates		
13.	The solution should be able to send notifications through SMS, Email, Messaging platforms		
14.	The solution should adhere the overall standards of the ID solution of reliability, availability, scalability and performance		

3.3.3.8 Document Management System

#	Requirement Title	Compliance (Y/N)	Remarks
1.	Document Management System should allow inputting files through following sources: a. Scanners b. Email c. Manual Upload d. Bulk Upload		

#	Requirement Title	Compliance (Y/N)	Remarks
	e. Mobile Apps f. Web Services g. Office Suite h. Messaging Platforms i. Social Media Platforms j. Live Chat		
2.	Document Management System should provide: a. Defining document category classification b. Indexing of all documents c. Custom Automatic Document Numbering d. Content recognition and indexing e. Indexing Meta Data f. Indexing all revisions g. OCR in different language h. Supports innumerable formats i. Extendable meta data fields j. Archival of Documents		
3.	The Document search engine should provide following search features: a. Safe and Powerful Search b. Document content and meta data search c. Advanced search on all document attributes d. Scalable document search engine		
4.	DMS should provide following document processing features: a. Create Documents using Templates b. Link Document to records in System c. Forward, Move, Share Documents d. Email Documents e. Revise Documents		

#	Requirement Title	Compliance (Y/N)	Remarks
	f. Inbuilt Document Editors for various file types g. Check-In and Check-out documents h. API based accessibility of document for viewing or uploading documents		
5.	DMS should provide following workflow automation features: a. Rule based processing on incoming documents b. Setup individual rules and document actions c. Automatic and Manual workflow d. Document Routing e. Business Process Modeling with Customized Windows, Re- ports f. Configure multi-level approvals g. Automatic creation of records based on documents h. Update records based on documents		
6.	DMS should provide following document security features a. Audit Trail a. User and Roles b. Advanced Access rights c. Encrypted Documents on file system d. Indexing all revisions e. Supports SSL f. Modify Ownership		

#	Requirement Title	Compliance (Y/N)	Remarks
7.	DMS should provide following DMS interface/Dashboard features a. Workflow Inbox b. Document inbox c. Alerts and Notifications d. Reporting Dashboard e. Follow-ups and Chat f. Inbuilt Calendar, Email, SMS		
8.	Document Management System should provide a certain level of customization allowing users to: a. Create customized Windows and Records b. Generate Custom Fields and Reports c. Add custom Document Attributes d. Describe custom workflow e. Create Custom Dashboard Reports		

3.3.3.9 Fraud Management

#	Requirement Title	Compliance (Y/N)	Remarks
1	Supporting Black List Input		
2	Audit Trails as Input		
3	Supporting Internal Feedback for Learning		
4	Updating Blacklist based on Patterns		
5	Supporting Manual Investigation		
6	**Fraud Data Store**		
7	Creating Data Store		
8	Supporting Storage of UDI Fields for Optimal Analysis		
9	Supporting Storage of Audit Trails for Optimal Analysis		

#	Requirement Title	Compliance (Y/N)	Remarks
10	Supporting Reputation scores		
11	Supporting Extensible Metadata		
12	Supporting Pluggable Engine based on Interfaces		
13	Supporting Read/Write Interfaces to SL-UDI Server		
14	Supporting Read/Write Interfaces to Fraud Engine		
15	Supporting Read/Write Interfaces to Action Engine		
16	Process Session Data		
17	Supporting Detailed Logging		
18	Supporting ACLs		
19	**Fraud Engine**		
20	Rules Interfaces		
21	Supporting Job Scheduler		
22	Methods for detecting fraud		
23	Detecting Data Anomalies		
24	Supporting State Driven Transitions		
25	Supporting Setting Limits		
26	Supporting Geographical analysis		
27	Providing Rule engine		
28	**Inspection Console**		
29	User Interface for Manual Inspections		
30	User Interface for Configuration of Fraud Engine		
31	**Action Engine**		
32	Supporting Configurable Action Engine Workflow		

#	Requirement Title	Compliance (Y/N)	Remarks
33	Keeping Track of Action Event Creator Identity		
34	Keeping Track of Action Event Triggered		
35	Configuring Action Event processing		
36	Publishing Action Event Results		
37	Integrated Workflow Management Tool		
38	Supporting Configurable Action Engine Workflow		

3.3.3.10 API Gateway

#	Requirement Title	Compliance (Y/N)	Remarks
1	The proposed solution shall be on premise solution and not a cloud-based solution.		
2	The proposed solution shall provide API Lifecycle maintenance capabilities including definition, creation, security, monitoring and management		
3	The proposed solution shall have API cataloguing capabilities along with mechanism to set up and externalize the APIs.		
4	The proposed solution shall have capabilities to manage revision and archiving of APIs as part of the life cycle and associated version control.		
5	The proposed solution shall have Policy Management capabilities for APIs and shall bring in provisions for consumer contracts, provisioning and identity management		
6	The proposed solution shall have capabilities for Mobile Integration		
7	The proposed solution shall bring in standard API governance features		

#	Requirement Title	Compliance (Y/N)	Remarks
8	The proposed solution shall have capabilities of traffic throttling, prioritization and routing.		
9	**Control**		
9.1	Shall support SLA configuration on specific API calls for traffic control		
9.2	Shall support intelligent load distribution and dynamic routing of incoming requests		
10	Shall support JSON & XML schema validation, filter and transformation		
11	Shall support query, extract, filter, transform JSON messages with JSONiq		
12	Shall support following Message Formats SOAP, XML, JSON, Non-XML		
13	Shall support monitoring of API calls - request / response		
14	Shall support SOAP/REST/HTTP protocols		
15	Shall support REST to SOAP and SOAP to REST conversions		
16	**Security**		
17	Shall support authentication (client id and secret key) and Authorization of client messages / requests		
18	Shall support Oauth 2.0, SAML, LTPA, Kerberos & WS-Security specifications		
19	Shall support SSL Transport and SSL termination for services Calls		
20	Shall support SSL client certificate-based authentication		

#	Requirement Title	Compliance (Y/N)	Remarks
21	Shall support encryption, decryption, digital signatures and validation of digital signatures for incoming or outgoing messages		
22	Shall support XML & JSON Threat protection and also support content filtering		
23	Shall support integration with LDAP to offer AAA		
24	Shall support TLS 1.1 & TLS 1.2 or latest to offer strict security requirements		
25	**High Availability, Administration & Performance**		
26	Shall offer web-based administration console		
27	Shall support multiple instances of service governance gateway software to be configured in active - active mode		
28	Shall support intelligent load balancing capabilities for backend Application server / mobile server instances		
29	Shall support operational governance of incoming requests with SLAs and throttling policy		
30	**Threat Detection and Policy Enforcement**		
31	Brute Force Attacks Mitigation		
32	Session Attacks Mitigation (Cookie, Form Parameter, URI rewrite)		
33	Ability to filter by inspecting the content of a message		
34	Support for request throttling per device / per IP / number of requests		
35	Support for request size limitation (request and response)		
36	Ability to detect and mitigate XML injection (DTD Include, Depth, Recursive Payload)		

#	Requirement Title	Compliance (Y/N)	Remarks
37	Ability to detect and mitigate Cross Site Scripting injection		
38	Ability to detect and mitigate SQL injection		
39	Ability to detect and mitigate excessive use of whitespace		
40	Ability to detect and mitigate IP Denial of Service		
41	Ability to detect and mitigate XML Denial of Service attacks		
42	Ability to detect and mitigate replay attacks		
43	It shall support various database like oracle MS SQL, My SQL etc.		

3.3.3.11 Business Rules Engine

#	Requirement Title	Compliance (Y/N)	Remarks
1	The solution shall support data verification and consistency checks.		
2	The solution shall support Phreak & Reteoo algorithm		
3	The Rules Engine must be able to submit business rules to an external repository at such time as the repository exists.		
4	The RE must be JSR94 compliant. The JSR 94 defines a standard API for a rules engine. It is important for the rules engine to comply with JSR94, so that it provides a common interface to the application development team		
5	Support both embedded and stand-alone services. Other requirements beyond java compatible.		
6	The Solution shall support Compute values based on input data		

#	Requirement Title	Compliance (Y/N)	Remarks
7	The Solution shall support mechanisms and ease of use for users to edit rules.		
8	The Solution shall have the ability to tune individual steps in the overall decision process for maximum performance by the execution engine		
9	The system shall have the feature like a. Complex event Processing (CEP) b. Stateless & Stateful rules c. Backward & Forward chaining rules d. Business Resource Planner		
10	The Solution shall support repository infrastructure for rule storage and versioning		
11	The Solution shall easily integrate with the rest of proposed Solution		
12	The Solution shall support seamless and easy user interaction		
13	Ability to capture and maintain rules centrally.		
14	Support for user roles and configurable permissions by role. The rule repository must support fine grained user/group access controls. System must provide a robust governance framework to manage business rule change.		
15	Ability to test and verify combinations of rules produce the desired outcome. The system must allow the user to define key measurements against which the business logic can be verified.		

3.3.3.12 BPM & Workflow (Business Process Management Suite)

#	Requirement Title	Compliance (Y/N)	Remarks
1	Support easy workflow configuration, its maintenance, and need based modification, addition alteration of the steps.		
2	Support process modelling based on BPMN2 notation standard		
3	Facility to simulate a process before launching it so that appropriate changes can be made based on findings.		
4	Provide business rule engine and a management platform. Users shall be able to modify the business rules online without any need of deployment. System shall also have business rule connector so that it can talk to any 3rd party business rule engine		
5	Allow saving custom BPM templates so that end user can tailor a business process based on any of the custom template.		
6	Offer performance monitoring features for the business processes. The system shall be capable of identifying, reporting inefficient processes and operations and/or those with high level of error and omission		
7	Expose W3C standard web services and REST based web services so that it can communicate to any other technology layer seamlessly.		
8	Have capabilities which will enable business activity monitoring and capture audit trail of all transactions as well. Web based dashboard shall be made available for accessing all reports.		
9	Provide dashboard view for showing multiple reports. Dashboard view and content can be customized for individuals.		

3.3.3.13 Distributed Caching

#	Requirement Title	Compliance (Y/N)	Remarks
1	Product shall be able to support application data models without requiring any changes given the data meets Java serialization requirements.		
2	Product shall enable a continuous integration development environment.		
3	Product shall minimize vendor lock-in.		
4	The developer shall be shielded from the inner workings of the distributed cache; cache shall however allow access to its inner workings shall greater control be required.		
5	Product shall be able to deliver consistent throughout and latency under peak load scenario and circumvent execution environment specific issues		
6	Product must allow an unlimited number of nodes to scale horizontally in support of an individual cache.		
7	Product must have the ability to scale vertically and perform equally as well with a single node installation, if provided sufficient CPU, memory, and I/O as a multi-node deployment.		
8	Product shall be able to scale horizontally and able to handle more application throughout and larger data size by runtime augmentation of additional computers/nodes		
9	Product shall have ability to maximize the available RAM utilization and remain agnostic to Java GC issues		
10	Product shall have the ability to locate data as close to where it is needed as possible, and in an efficient format for where it is needed		
11	The product shall support in memory access time of micro second latencies for a very large, distributed data set without impacting the JVM GC behavior		

#	Requirement Title	Compliance (Y/N)	Remarks
12	The product in process cache shall always be in sync with latest updates in cluster.		
13	Product shall have the capability to automatically detect and recover from failure. Caching infrastructure shall allow tunable SLAs against different kind of infrastructure failure.		
14	The product shall allow clients to be dynamically switched to an alternate server, if the server they are communicating with has a high processing load or becomes unavailable.		
15	The product shall efficiently distribute data across the cache for high performance and robustness.		
16	The product shall be fully JTA standard compliant.		
17	The product shall support queues and topics for persistence. (asynch write to backend) (write behind) The product shall support asynchronous write to backend persistence store		
18	The product shall support multiple API calls simultaneously (multi-threading)		
19	The product shall be readily integrated with the major ORM frameworks like hibernate.		
20	Editing Cache Configuration -The cache solution shall provide following editable configuration properties for each cache • Cache – The name of the cache as it is configured in the System configuration resource. • Time-To-Idle (TTI) – The maximum number of seconds an Object can exist in the cache without being accessed • Time-To-Live (TTL) – The maximum number of seconds an Object can exist in the cache regardless of use.		

3.3.3.14 SMS Gateway

#	Requirement Title	Compliance (Y/N)	Remarks
1	The Solution needs to provide the SMPP and/or HTTPS - API with/without XML support for sending messages. This shall be the primary channel for communication.		
2	The Gateway shall support the encryption-decryption for the entire API parameters supporting DES/ 3DES/ AES algorithm or latest.		
3	The solution shall have the facility of online filtering of the DND numbers.		
4	The SMS services shall be scalable to meet the requirements for the next 5 years from the date of placing the Purchase Order. Considering the similar growth on year-on-year basis.		
5	The gateway shall provide facility for bulk SMS upload or SL-UDI may request SI to upload the file for bulk SMS on behalf of the SL-UDI. Format for file is to be provided by the bidder.		
6	The gateway shall be able to comply with latest regulations/ guidelines issued by government of Sri Lanka's telecom regulatory agencies. Also, the bidder shall be able to comply with all future changes effected by government regulatory agencies.		
7	The Gateway shall have the ability to send and receive National /Push and Pull messages to Q from national GSM, CDMA as well as 3G/4G/5G mobile handsets.		
8	Features like monitoring of total SMSes sent/ received within a day/ week/ month, time delay (if any) in sending the SMSes, no failed SMSes, invalid mobile numbers, no of push and pull SMSes sent.		

#	Requirement Title	Compliance (Y/N)	Remarks
9	SL-UDI Shall be able to generate detailed reports in Excel/ Pdf and any other format specified. SL-UDI shall be able to generate Product-wise, Date-wise, Category-wise reports, transaction-based reports, aggregated reports per category. The reports shall contain timestamps of SMS received at SI's Server, SMS sent to the Telecom operator and the actual delivery to the end user.		
10	The SI shall be able to integrate their SMS gateway with other applications such as authentication, IDMS, CRM and other related systems in coordination with respective vendors.		
11	The API shall support the encryption-decryption for the entire API parameters supporting DES/ 3DES/ AES algorithm.		
12	SMS gateway shall support templatization of SMS text and function/utilities such as addition, modification, cancellation, expiry timestamp etc.		

3.3.3.15 Distributed Messaging

#	Requirement Title	Compliance (Y/N)	Remarks
1	The proposed SL-UDI system must support an Enterprise Messaging Platform to seamlessly integrate the Kernel system.		
2	Messaging platform solution must be robust to easily handle very large volumes (in the order of 10K to 20K bps)		
3	Messaging platform shall be work on open standards such as AMQP		
4	The SL-UDI services preferably be integrated using open source/standard version of Enterprise Service Integration platforms		

#	Requirement Title	Compliance (Y/N)	Remarks
5	These services must also be stateless in nature and shall be horizontally scale able		
6	These services shall be designed to be highly fault tolerant and in built design mechanisms to retry failed requests seamlessly		
7	The network shall be structured as a hub-and-spoke topology.		
8	It shall be designed as a distributed system which is very easy to scale out		
9	It shall offers high throughput for both publishing and subscribing		
10	It shall supports multi-subscribers and automatically balances the consumers during failure		
11	It shall persist messages on disk and thus can be used for batched consumption such as ETL, in addition to real time applications		

3.3.3.16 Relational Database Management System/ Non – Relational Database Management System

#	Requirement Title	Compliance (Y/N)	Remarks
1	All the applications implemented shall have provision for optimizing the number of static connections to the database using connection pooling. All the applications implemented shall also optimize the duration of connection to the database by using techniques like session time out.		
2	Database shall have perpetual and enterprise wide/subscription-based licenses. They shall have proven scalability credentials to cater to any system load.		
3	It shall provide Unicode support.		

#	Requirement Title	Compliance (Y/N)	Remarks
4	It shall support User-defined Data Types & User-defined Functions.		
5	Database shall support advanced data compression, self-healing and deployment in various cluster topology.		
6	The database platform shall support enhanced configuration and management of audits.		
7	The database platform shall support Failover Clustering and disaster recovery solutions.		
8	It shall support online indexing operations and parallel indexing operations		
9	Database shall support Schemas, Roles Based Privileges & Authentication.		
10	The data platform shall support policy-based system for managing one or more instances across enterprise		
11	It shall provide a scripting shell that lets administrators and developers automate server administration		
12	The database shall have enterprise level DB- support center with a 24*7 helpdesk support.		
13	Other than built in database access logic in application, a separate database security layer will be required to control direct access to database server by any unauthorized user.		
14	The database platform shall support defining resource limits and priorities for different workloads, which enables concurrent workloads to provide consistent performance		
15	Database security shall provide different layers of database users with overall control of database security administrator, only authorized database administration users with assigned privilege shall be allowed to access database.		

#	Requirement Title	Compliance (Y/N)	Remarks
16	A separate audit trail shall be maintained for any direct modification, deletion and addition in RDBMS/Non-Relational database in database structure or records. Users, even the database administrator shall not be allowed to tamper with audit log. Database server shall support most granular column encryption to encrypt sensitive data.		
17	The selected RDBMS / Non-Relational database shall have abilities for fault tolerance, linear scalability, mixed workload capability		
18	Database shall support the option of different partitioning schemes within the database to split large volumes of data into separate pieces or partitions, which can be managed independently. It shall support physical columns. The partitioning shall enhance the performance, manage huge volumes of data and shall provide foundation for Information Life Cycle Management.		
19	The RDBMS/Non-relational database shall preferably provide options for Automated/manual performance analysis with diagnosis of the cause of performance related issues with possible resolutions.		
20	RDBMS/Non-relational database licenses shall be unrestricted and full use licenses (read, write and modify). RDBMS/Non-relational database shall allow storing scanned images, text documents, XML, multimedia inside the tables. It shall be part of the basic database distribution without any additional cost to the organization		
21	RDBMS/Non-relational database shall support the separation of security functionality from application functionality and database administration functionality.		
22	Any proprietary OEM specific functionality of RDBMS/Non-relational database shall not be used.		

#	Requirement Title	Compliance (Y/N)	Remarks
23	There shall be capability to store spatial data.		
24	All the applications implemented shall have provision for optimizing the number of static connections to the database using connection pooling. All the applications implemented shall also optimize the duration of connection to the database by using techniques like session time out.		

3.3.3.17 Email Solution

#	Requirement Title	Compliance (Y/N)	Remarks
Technical			
1	The email solution shall support all popular web browsers complaint to HTTP-1.0 and HTTP-1.1 like Internet Explorer, Mozilla Firefox, Chrome, Safari etc.		
2	The mail solution shall run over secure HTTP		
3	The email solution shall provide MAPI-based synchronization of mail, contacts, and calendar data between Outlook and the proposed solution server		
4	It shall also ensure that the synchronization operations are cached and synchronized as an asynchronous process, enabling optimal Offline performance		
5	It shall be able to provide access to the Mail server via IMAP (Internet Message Access Protocol) clients and POP (Post Office Protocol) clients, with the option to connect over SSL/TLS		
6	AJAX-based end user interface: Rich, interactive, web-based interface for end user functions (access via HTTP and HTTPS)		
7	The webmail client shall be tightly bound with the messaging software and shall be from the same OEM		

#	Requirement Title	Compliance (Y/N)	Remarks
8	HTML 5 based offline access of mails on the web client		
9	Shall provide synchronization of Email, Contact, Calendar, address book lookup through ActiveSync on iPhone and android mobile phones		
10	The Mobile synchronization shall not happen on POP/IMAP		
11	The mail server shall support features for sharing documents with version control/access control out of the box with no additional software/application		
General			
12	User mail box size should be 20 GB minimum		
13	The Proposed solution shall store audit logs at least for 6 months		
14	Proposed solution shall provide a secure mechanism for mail relaying for 3rd party applications.		
15	Proposed solution shall support recovery or restoration of any specified email box without impacting / downtime for other users in online and offline mode.		
16	Email auto saving function while composing.		
17	Proposed solution shall have client-side spam detection using keywords or patterns and block junk emails		
18	End user should have access to the email even in the low bandwidth connections		
19	The proposed email solution should not duplicate attachments delivered in messages addressed to numerous recipients in each mailbox in the system.		
20	The solution should encrypt data both at rest and in transit		
21	The proposed system should include the possibility for end users to manage their information rights. End users must be able to apply restrictions such as preventing		

#	Requirement Title	Compliance (Y/N)	Remarks
	forwarding, editing, printing, storing, preventing attachment downloads, message expiration, and so on.		
22	The proposed system must provide archiving policy enforcement based on pre-defined parameters, as well as automatic archiving based on policies.		
23	Proposed solution shall have ability to validate incoming emails through DomainKeys Identified Mail (DKIM), and Domain- based Message Authentication, Reporting & Conformance (DMARC)		
24	The solution should integrate with the proposed LDAP and PAM/PIM solution.		
25	The solution should integrate and work with Backup solutions, Secure Email gateway, Network and Security solutions, SIEM Solution, etc.		
Web mail client			
26	Shall support advanced search and file indexing for large inboxes		
27	Shall support e-mail, Address Book, Calendar, Task & File Server		
28	Users shall be able to restore a mail deleted from the Trash folder – Dumpster		
29	Ability to utilize Active Directory for user authentication and/or Global Address List		
30	Option to check and correct spelling in a mail message, calendar appointment		
31	Ability to share Address Books, Calendars, and Notebooks (Documents) with internal users and groups (read or write access)		

#	Requirement Title	Compliance (Y/N)	Remarks
32	Ability to quickly categorize messages, contacts, and/or documents by attaching "Tags" with user defined names and colors		
33	Option to quickly view attachments in HTML format		
34	Ability to print a message and see a print preview		
35	Ability to sort messages based on subject, date, or sender		
36	Ability to flag/unflag messages/conversations for follow up		
37	Ability to define filter rules and priorities for incoming messages		
38	Ability to enable/disable a custom away message (Out Of Office), Separate for Internal & External Users		
39	The user shall be able to define the rules for sorting mails and moving mails to folders.		
40	Ability to add a custom signature to a message		
41	Ability to save in-progress messages to a Drafts folder		
42	The user shall be able to set the message priority through web mail interface like highest, high, medium and low.		
43	Ability for a user to set an automatic forwarding address and choose whether to leave a copy in the primary mailbox		
44	Right-clicking a message displays a menu of actions to take on that message (e.g. Mark Read, Reply, Delete)		
45	Ability to toggle between Reply and Reply-All while composing a reply		
46	The interface shall have support for the junk mail folder and ability to set the level of junk mails it can receive or forward to the junk mail folder		

#	Requirement Title	Compliance (Y/N)	Remarks
47	Users can share their mailbox folders and set the permission levels to manage or to view-only		
48	User can send an email in the mail box as an attachment		
49	Save attachments in Briefcase rather than as message attachments		
50	Users can attach a URL to an email message		
51	Users can define multiple email signatures to use		
52	Users can set notification of new mail		
53	Multiple messages can be selected and forwarded in one email		
54	Functionality for users to upload documents in the repository which can be then shared with the other users within the organization & outside as well		
55	The Documents uploaded in the repository shall be de-duplicated to save the storage		
56	Server-Side Filtering allowing filtering of the mails on the basis of all or part of text in all standard headers (such as To, From, Subject, Reply-to, CC, BCC, Date), text in message body shall be available		
57	Shall be able to send and receive files as MIME (Multipurpose Internet Mail Extensions) attachments		
58	Shall support auto completion of email address		
59	The Mail Messaging Solution shall have support for Mail Blocking at user level.		
60	Compose email even when not online-messages to be sent are saved in the "Outbox" and are sent when connected again		

#	Requirement Title	Compliance (Y/N)	Remarks
61	The Mail Messaging Solution shall provide feature of auto saving of message while composing		
62	Add tasks and set the start and due date, set the priority and keep track of the progress and percentage complete		
Desktop client / Thick offline client			
63	OEM shall have their own Desktop client which can be installed on Windows, Mac & Linux with no separate licensing to the desktop client		
64	The OEM Shall provide support to the desktop client		
65	The Desktop mail client shall be able to set priority of the messages like high, medium and low		
66	Powerful quick search-based senders, recipients, message, subject, data, status etc.		
67	Spell check facility		
68	Personal and global Address Book		
69	Calendar, Group Scheduling, Personal Task Management Mail Archiving to local disk		
70	Drag & Drop Attachment		
71	The Desktop Client & the web client shall be able to sync features like filters/folders/recent contacts for type ahead addresses etc.		
72	Add email signatures for each account and automatically reply with the correct "from" address		
73	Supports plain text and html message formatting		
74	Compose email even when not online-messages to be sent are saved in the "Outbox" and are sent when connected again		

#	Requirement Title	Compliance (Y/N)	Remarks
75	The document sharing component shall be accessible through the Native Desktop Client		
Interface			
76	Users can set their default preference for viewing messages in the reading pane		
77	Users can right click on a folder to see the number of messages and the total size of items in folder		
78	Users can check multiple emails in the list view to mark as read/unread/tag, delete, or to move to a different folder		
79	The interface shall have support for folder nesting (folders within folders)		
80	Users can set the default font family, font size and font color to use when composing email messages and Documents pages		
81	Users can double-click on a message in message view to expand the view pane to full view		
82	The interface shall support for composing the mail in HTML and plain text format.		
83	User shall be able to see full message headers.		
84	Interface shall have support for spell check at the time of composing the mail.		
85	User shall be able to configure the Message view like: preview of number of messages, tool bar positioning and font view		
86	User can send an email in the mail box as an attachment		
87	Functionality to collapse email threads into a single Conversation View to simplify inbox		

#	Requirement Title	Compliance (Y/N)	Remarks
88	Users shall be able of do drag & Drop etc. from the web UI		
Address Book			
89	Business card view of Contacts		
90	Ability to import/export Contacts in .csv format and vCard (.vcf) format		
91	Ability to print a single Contact or list of Contacts and see a print preview		
92	Right-clicking a Contact displays a menu of actions to take on the Contact (e.g. compose message, search for messages)		
93	Ability to drag a Contact to a mini-calendar date to create an appointment with that Contact		
94	Ability to create multiple Address Books in a single mailbox		
95	Ability to move/copy contacts from one Address Book to another (based on access privileges)		
96	Ability to create group contact lists in their user Address Books		
97	Address book displays individual contact information in tabbed view		
98	Photos and images can be uploaded to contacts in Address Books		
Search			
99	The Mail Messaging solution shall provide an extensive search mechanism able to search mail, attachment content, contact		
100	Server-side indexing of mailbox content, enabling fast and efficient search from the web interface		

#	Requirement Title	Compliance (Y/N)	Remarks
101	Ability for a search to include any number of conditions combined via Boolean-like expressions (AND, OR, NOT, etc.)		
102	Ability to search using a prefix plus a wildcard		
103	When using Search Builder, the search result set updates continuously as search conditions are changed		
104	Ability to search for items that contain specific keywords and with a specific date or within a specific date range		
105	Ability to search for items based on read/unread status		
106	Ability to search for items with specific recipients in the To/Cc fields, from a specific sender, based on subject		
107	Ability to search for content inside attachments		
108	Ability to search for Contacts in a Shared Address Book		
109	Ability to search for items that were sent to or received from a specific domain		
110	Ability to search for items that include a specific Tag(s)		
Calendar			
111	The web mail interface shall have an integrated calendar providing the following features: shared calendar, to-do lists, event scheduler and reminders.		
112	Ability to schedule meetings and view attendees' free/busy information, configure a resource to auto-respond to scheduling requests based on availability		
113	Ability to set an explicit time zone for an appointment and automatic display of appointments/schedules in the users current time zone		

#	Requirement Title	Compliance (Y/N)	Remarks
114	Ability for a user to view multiple calendars overlaid in the same view, which each calendar optionally represented by a different color; when viewing multiple calendars, option to view that indicates the degree of conflict at each potential time slot		
115	Ability to create recurring meetings and exceptions to recurring meetings		
116	Option to enable an alert popup for upcoming appointments		
117	Ability to create an appointment and/or drag an appointment's boundaries inline in calendar views		
118	Ability to quickly mark Accept/Tentative/Decline from calendar views		
119	Declined appointments display faded so that the user remains aware of their occurrence		
120	Ability to print calendars in day, week, work week, or month views and see a print preview		
121	Hovering over an appointment in calendar view displays additional appointment details		
122	Option to display a miniature calendar at all times; Right-clicking on the minimal displays a menu of actions to take on the associated date (e.g. add appointment, search for messages)		
123	Ability for a user to create multiple calendars within a single account		

3.3.3.18 Internet Payment Gateway (IPG)

The IPG will be provided by the GoSL and the bidder needs to integrate the same with all relevant solution components.

#	Requirement Title	Compliance (Y/N)	Remarks
1	IPG Integration should be implemented.		

3.3.3.19 Application Servers and Web Servers

#	Requirement Title	Compliance (Y/N)	Remarks
1	The proposed product/ solution has to be on premise and no cloud based solution/ product will be accepted.		
2	**Architecture** The product/ solution shall be completely Java EE Compliant – with Web and Full profile both support stand-alone mode with server management console, support third party integration of LDAP, support third party integration of messaging infrastructures		
3	**Compatible Web Services Technologies as per latest J2EE standards** a. Java API for RESTful Web Services (JAX-RS) b. Enterprise Web Services c. Java API for XML-Based Web Services (JAX-WS) d. Java Architecture for XML Binding (JAXB) e. Web Services Metadata for the Java Platform JSR f. Java API for XML-Based RPC (JAX-RPC) g. Java APIs for XML Messaging h. Java API for XML Registries (JAXR)		
4	**Compatible Web Applications Technologies as per latest J2EE standards** a. Java Servlet b. JavaServer Faces c. Facelets as JSF View Handler d. JavaServer Pages /Expression Language e. Debugging Support for Other Languages f. Standard Tag Library for JavaServer Pages (JSTL)		

#	Requirement Title	Compliance (Y/N)	Remarks
5	**Enterprise Application Technologies as per latest J2EE standards** a. Contexts and Dependency Injection for Java (Web Beans) b. Dependency Injection for Java c. Bean Validation d. Enterprise JavaBeans e. EJB Interceptors f. Java EE Connector Architecture g. Java EE Connector Architecture h. Java Persistence i. Common Annotations for the Java Platform j. Java Message Service API k. Java Transaction API (JTA) l. JavaMail		
6	**High Availability** The product/ solution shall provide a. Out-of-the-box Clustering, Caching, Session Replication, Fail-Over & Load Balancing support. b. The Solution should provide Central and single management console for all cluster nodes. c. Failover and load balancing for JNDI, RMI, and all EJB types d. Support for Transaction recovery during application server failover		
7	**Monitoring and Administration** The product/ solution shall provide: a. Key functionalities like Reliability, Availability, Scalability and Performance) combined with easy manageability features b. Simplified, integrated, centralized administration, management and monitoring tools. There shall be a unified configuration & management		

#	Requirement Title	Compliance (Y/N)	Remarks
	c. Distributed management tool for asynchronous remote multi- domain and multi-server management. Shall also provide runtime performance monitoring and diagnostic tool. Tools for transaction configuration and monitoring. d. It should support analysis of heap dump, memory leaks and threads.		
8	**Operations and Management** The product/ solution shall provide: a. Ability to keep history of change and rollback configuration of the Application Server b. Proposed Application Server shall be certified on leading JVM's, and all major Operating Systems		
9	**Scalability** The solution shall provide: a. Vertical scalability (on SMP machines) and Horizontal scalability (across clusters and non-cluster of machines) b. Mechanism for on-demand resource allocations - dynamic clusters (ability of the server to dynamically add new ma- chines or remove them to / from the cluster when workload changes). It shall also be capable of managing extra-large in- stalls of hundreds or thousands of servers and JVMs from a single console or command line. c. The system shall support Scalable architecture to support clustering at each layer i.e. Web server, Application server for Fault Tolerance & Load Balancing.		
10	**Security** The solution shall provide: a. Capability to have separate administrative roles and limit scope of actions (superuser, monitor, configurator, operator) b. Secure administration of a clustered server environment		
11	**Webserver Specifications** a. Shall support integrated Web server solution with request queuing and caching b. Shall support load balancing		

#	Requirement Title	Compliance (Y/N)	Remarks
	c. Shall have the ability to store web server configuration data in XML or plain text. d. Shall support web-based administration e. Supports industry standard Lightweight Third-Party Authentication (LDAP), OAuth, Kerberos, and RSA token authentication f. Shall support integration with certificate services		

3.4 Minimum Technical Specification for Infrastructure and Security

Mandatory Conditions

a. All Servers shall be from the same OEM

b. All Network Switches, routers and transceiver modules shall be from the same OEM

c. All Servers and Network devices shall be connected with 25GbE or higher.

d. External and Internal Firewalls should be different brand

3.4.1 Infrastructure

3.4.1.1 Blade Servers

#	Description	Compliance (Y/N)	Remarks
1	Blade server should be proposed with the latest generation x86 Intel/AMD processors Should be quoted with minimum 2 x 16 Core processors with minimum 2.8Ghz of clock cycle		
2	OS support: 64-bit Microsoft Windows Server Enterprise Edition(latest) / Red Hat Enterprise Linux / SUSE Linux Enterprise Server (latest), Oracle Linux (Latest) Hypervisor Support - Citrix XenServer/VMware vSphere ESXi/KVM/ All servers will be based on x86 architecture Shall be certified for proposing virtualization / Operating systems		

#	Description	Compliance (Y/N)	Remarks
3	Blade server should be quoted with minimum 1024 1TB memory, expandable up to 8TB, 4800/5600 MHz DDR4/DDR5 DIMMS		
4	The blade server should support min 6 no's of SAS/SSD/NVMe disk drive and should be quoted with minimum 2 x 480GB M.2 Boot drive in RAID 1 All the capacity disks and power supplies to be hot-swappable		
5	The Blade server should support Converged Network Adapters. The Converged Network Adapters should aggregate both the Ethernet and FC connectivity on a single fabric providing 100Gbs bandwidth per blade		
6	All servers to be connected to Ethernet and SAN with redundancy.		
7	4 year 24x7 remote break-fix assistance and next business day advance hardware replacement from OEM.		
8	The management solution should provide the capability to manage the blade servers across multiple chassis , rack servers from the same unified console. It should provide the complete administration including operating system installation and firmware management from the single console with a unified view of all the blade servers, server identities, configuration details, monitoring and alerting System shall support embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated phone home support		
9	System remote management shall support browser based Graphical Remote Console along with Virtual Power button, Remote boot using USB / CD/ DVD Drive. It should be capable of offering upgrade of software and patches from a remote client using Media / image/folder; It shall support		

#	Description	Compliance (Y/N)	Remarks
	server power capping and historical reporting and shall have support for multifactor authentication.		

3.4.1.2 Rack Servers

#	Description	Compliance (Y/N)	Remarks
1	OS support: 64-bit Microsoft® Windows Server Enterprise Edition / Red Hat® Enterprise Linux / SUSE® Linux Enterprise Server Oracle Linux Hypervisor Support - Citrix® XenServer® VMware vSphere® ESXi, KVM, All servers will be based on x86 architecture Shall be certified for proposing virtualization/Operating systems		
2	Server should be quoted with latest generation x86 Intel/AMD processor Server should be configured with minium of 2 x 32 Cores 2.8GHz latest generation Intel/AMD processors		
3	Memory (RAM): Min. 1024 GB scalable up to 8TB of Memory with DDR5 memory DIMMS		
4	12Gbps SAS RAID controller with 4GB Cache supporting RAID 0,1, 5, 6,10, 50, 60 supporting capacity drives configured in system.		
5	SSD : Minimum 2 x 1.2 TB SSD/NVME		
6	Disk bays: Support for min 20 small form factor hot plug SAS / SCSI/SSD/NVMe hard drives in disk drive		

#	Description	Compliance (Y/N)	Remarks
7	At least 4 x 10/25 Gbps Ethernet ports or more		
8	Server should support 64Gbps FC ports. Min 4 ports per storage controller		
9	Rear: 1 USB ports (Ver 3.0 or higher); RJ-45 Ethernet;; two RJ-45 Ethernet; Front: One USB (Ver 3.0)/KVM Connector		
10	Graphics controller: Supports display resolutions up to 1920 x 1200 16bpp @ 60H		
11	Security: Power-on password / admin password / Should have a cyber resilient architecture for a hardened server design for protection, detection & recovery from cyber attacks Should protect against firmware which executes before the OS boots * Hardware based Root of Trust * Signed firmware updates * Secure default passwords * Secure alerting		
12	Cooling fans: hot-swapable and redundant fan f		
13	Power supplies: Hot plug redundant AC power supply		
14	Management feature to identify failed components even when server is switched off.		
15	Rack Mountable 2 U		
16	It shall provide Secure Sockets Layer (SSL) 256-bit and above encryption and Secure Shell (SSH) Version 3 and support VPN for secure access over internet.		

#	Description	Compliance (Y/N)	Remarks
17	Shall be able to manage systems through a web-browser		

3.4.1.3 Blade Chassis

#	Description	Compliance (Y/N)	Remarks
1	Blade enclosure Should occupy between 7-12 RUrack height, supporting a minimum 8 half height/4 Full height modular server per blade chassis.		
2	Blade enclosure should support all x86 based Intel/AMD processor blade servers		
3	Chassis should have sufficient number of redundant converged modules with 100Gbps ports to provide a minimum FCoE uplink bandwidth of 100 Gbps per blade server for a fully populated chassis for converged Traffic.		
4	The chassis should support redundant modules for connectivity. The overall solution should support aggregation of multiple chassis for connectivity.		
5	The enclosure shall be populated fully with power supplies of the highest capacity available with the vendor. Power supplies should support N+N / N+1 redundancy configuration, where N is greater than 1. . Chassis should be configured with Titanium certified Power supply.		
6	Each blade enclosure should have a cooling subsystem consisting of redundant hot pluggable fans or blowers enabled with technologies for improved power consumption and acoustics		

#	Description	Compliance (Y/N)	Remarks
	The chassis cooling should be modular so that future enhancements can potentially handle open- or closed-loop liquid cooling to support higher-power processors.		
7	4 years comprehensive support and maintenance		
8	Management/controlling software's having to be from the OEM.		
9	The management solution and the switches that provides the connectivity to LAN and SAN environment should be provided		
10	Blade chassis management solution may be provided internal / external (SaaS or appliance based) , to the chassis and must provide single console for managing up to 10 chassis.		
11	The same management solution should also be capable to manage Rack Servers along with Blade Servers and it should provide the visibility to virtualization infra of the leading hypervisor as well as to the SAN environment of leading OEMs like NetApp, Hitachi, Pure storage, etc.		
12	The management appliance/solution should be deployed in High Availability and should provide the administration of rack & blade servers across chassis from the same console.		
13	The management solution should provide Role based Access Control and remote management capability. The management software can be used to create resource pools based on a hierarchal structure and have the blade resources assigned to the respective resource pools		
14	Firmware upgrade/downgrade should be possible for all the components in the infrastructure including the server, chassis management modules , converged switch, other modules from the same console that is used to manage the individual blades The management solution should provide email notification/alerts. It should also provide API to integrate with 3rd party solution.		
15	Administrators have the flexibility to define power policies so that the power can be limited to a specific server and have the		

#	Description	Compliance (Y/N)	Remarks
	flexibility to define power policies so that the power can be limited to a specific server		
16	Server management system should provide an alert in case the system is not part of OEM Hardware Compatibility list		
17	The proposed management solution should provide security & advisory details via same unified dashboard and Supports multiple level of authentication methods including TACACs+/ LDAP/ RADIUS/AD		

3.4.1.4 Storage: Enterprise Grade Object Storage Solution

#	Description	Compliance (Y/N)	Remarks
1	Proposed object storage must be enterprise-class appliance-based solution with high resiliency, no single point of failure, and enterprise-grade integrated hardware and software from a single OEM.		
2	Delivered as a pre-integrated appliance with minimum 4 active nodes; supports 500TB usable on Day-1 and scales to 1PB within one year.		
3	Proposed solution is a commercial enterprise-grade platform, not open source.		
4	Shall be integration via S3-compatible interfaces for Kubernetes workloads		
5	Solution should have GUI-based management console and RESTful APIs provided.		
6	Solution should have GUI-based management console and RESTful APIs provided.		
7	Storage solution should support MOSIP platform via RESTAPI integration		
8	Storage solution should support MOSIP platform via RESTAPI integration		
9	Proposed object storage should be able to consume storage capacity from the provisioned erasure coded storage nodes,		

#	Description	Compliance (Y/N)	Remarks
	block (SAN) storage, file (NAS) storage, public cloud storage or an S3 compatible storage.		
10	Must support multi-tenancy, with capacity quotas, access policies, and namespace configuration per tenant.		
11	Architecture must support independent scaling of capacity and compute (separation of access and storage nodes).		
12	Solution shall have data protection and WORM, and service-level policies		
13	Must support encryption at rest and in transit using AES-256, SSL/TLS, SSH keys, and certificate-based access control.		
14	Erasure coding must provide protection against 6 or more disk failures and at least 1 node failure, with rebuilds occurring within the same site to preserve WAN bandwidth.		
15	Solution shall consider rack awareness and failure domains while implementing		
16	Object storage must support multiple replication topologies: active-active, active-passive, one-to-many, many-to-one, ring, and chain.		
17	Object storage must support multiple replication topologies: active-active, active-passive, one-to-many, many-to-one, ring, and chain.		
18	Storage hardware shall be certified or approved by Object storage solution provider (OEM)		
19	Solution shall be provided at least 4 nodes with Read Only allowed after losing: Single Node.		
20	Nodes shall be placed with Rack awareness		
21	Special Note: Shall be in optimum throughput network 25GbE or higher (bidder shall calculate and propose network devices and speed accordingly)		

3.4.1.5 SAN (Storage Area Network)

#	Description	Compliance (Y/N)	Remarks
1	Proposed storage should deliver min 150,000 IOPS at 8KB block size from day 1 with 80% Reads and 20% write		
2	The system shall be a scale-out, all-flash NVMe architecture with a modular controller design featuring Dual Active-Active symmetric controllers to ensure high availability and load balancing. Storage should support cluster scale out architecture		
3	Storage should have enterprise class dual ported high performance NVMe TLC SSD drives with the capacity 30TB or less capacity of each drive		
4	Proposed storage should he All Flash that supports high performance NVME SSD Drives that supports high density and high endurance (>0.5+) with capacity 30 TB less		
5	The proposed array must be scalable to at least double of the disks to be required for meeting the solution requirements.		
6	All necessary licenses required to enable supported RAID levels, data/volume replication, DC/DR provisions, and array management features must be provided for the full supported storage capacity of the array. The solution must support RAID levels such as RAID 6 with dual parity support		
7	Must support multiple host interfaces including Fibre Channel (up to 64 Gbps), iSCSI (10/25 Gbps), and NVMe/TCP (up to 100 Gbps		
8	The proposed array shall have no single point of failure, with fully redundant and hot-swappable components. It must support non-disruptive hardware replacement, firmware upgrades, and guarantee 100% availability with built-in redundancy and dynamic drive protection.		

#	Description	Compliance (Y/N)	Remarks
9	The storage system shall have a minimum of 256 GiB cache memory per system to ensure low latency performance. The proposed array must ensure cache data integrity during manual shutdowns or unexpected power outages by automatically destaging cached data to non-volatile media such as flash or disk.		
10	The proposed storage should support all the popular enterprise operating systems.		
11	Offered Storage array shall support heterogeneous storage virtualization (native/external) for vendors like, but not limited to, EMC, HP, IBM, Hitachi, Netapp etc. Storage should be supplied with Unlimited capacity of virtualization license for existing storage. In case of non-native/external component used, it should be supplied in redundant mode with no single point of failure.		
12	The proposed all-flash storage array shall deliver consistent high performance across its entire capacity without requiring auto-tiering between different storage media types.		
13	The proposed array must support storage provisioning based on service level. There should be an option to configure and allocate storage space based on service level i.e. response time required for an application.		
14	The proposed array must provide continuous monitoring and movement of sub-LUN data chunks to provide real-time performance improvements		
15	The storage should be configured with Software/ Hardware Controller based Encryption for data security.		
16	The storage should be able to provide Quality or Service (QOS) to ensure bandwidth is allocated to desired servers or ports, storage should be capable of restricting IOs or throughput to LUNs or Volumes.		

#	Description	Compliance (Y/N)	Remarks
17	The proposed storage must provide an audit service to record activities including host-initiated actions, physical component changes, attempts blocked by security control. Audit log should be secure and tamper-proof.		
18	The proposed array must have capability to create target less snapshot for space efficiency, easy administration and minimal performance impact on production volumes		
19	The proposed array must support full copy clones for backup and reporting purposes.		
20	The proposed storage solution should support snapshot capabilities, ensuring efficient data protection and recovery. It must include the necessary software licenses		
21	The Proposed storage system should support Active-Active Storage configuration across two sites replicating to each other for same LUN/volume for zero RPO/zero RTO configuration.		
22	The storage should support both Synchronous and Asynchronous Data Replication to remote site		
23	The proposed storage array should support Three-Data-Center (3DC) replication, ensuring robust disaster recovery and high availability		
24	The proposed storage array should support Three-Data-Center (3DC) replication, ensuring robust disaster recovery and high availability		
25	The proposed array remote replication solution should support consistency group feature to ensure consistency of the data distributed across multiple devices of an application within an array or across homogenous arrays.		
26	The proposed array remote replication solution should ensure data consistency on the remote storages		

#	Description	Compliance (Y/N)	Remarks
27	Storage management software should be able to Orchestrate and Automate storage configuration operations		
28	Storage management software should be intuitive, browser-based user interface that configures and manages array		
29	Storage management software should be able to manage access controls, user accounts and permission roles		
30	Storage management software should provide interface to allow end users to replace disk drives		
31	Storage management software should provide interface/wizards to perform configuration operations like create LUNs present LUNs to host, set LUN attributes etc.		
32	Storage management software should be able to perform and monitor local and remote replication operations		
33	Storage management software should be able to send notifications for alerts generated in the end to end infrastructure i.e. virtual machines, Host OS, hypervisors, SAN devices, Storage devices		
34	Storage management software should be able to monitor alerts		
35	Storage management software should be able to monitor the service level objectives of application		
36	Should support system management console. Solution should provide: 1. Performance Analytics (Minimum 01 year Historical data & Real-time), 2. Replication monitoring, 3. Management Utilities.Logging. All Licenses required for the features described shall be provided for unlimited capacity.		
37	The storage system should have support for multi-path configuration for redundant path to connected hosts. Any		

#	Description	Compliance (Y/N)	Remarks
	Licenses (unlimited/frame based) required for this should be provided with Storage.		
38	Proposed replication solution should ensure data consistency on the remote storages		
39	The solution shall support inline data reduction with a minimum guaranteed effective ratio of 2:1.		
40	The proposed replication solution must support multi host and multi-array enterprise consistency in an open system environment. Should ensure data consistency for mission and business critical application data that spans across multiple LUNs and Raid groups		

3.4.1.6 SAN Switch

#	Description	Compliance (Y/N)	Remarks
1	The proposed director or chassis based solution must have complete redundancy in case of failure including hot swappable control plane module/supervisor, fabric modules, fan modules, power supplies, software modules on the OS.		
2	The switch(or director platform) must be able to provide up to 96 number - 64Gbps FC or 10-Gbps full line-rate autosensing Fibre Channel physical ports from day1. System should be scalable to support upto 384port or more.		
3	The switch(or director platform) should be able to support 64G FC speeds on all its ports at line rate from day1		
4	With the combination of 64-Gbps Fibre Channel switching module and supervisor switching modules it should be capable of enabling up to 4 terabits per second (Tbps) at the aggregate level		

#	Description	Compliance (Y/N)	Remarks
5	The switch must have non-blocking architecture and be capable of dropping bad / corrupt frames at the ingress of the switch		
6	The switch must support the following modules types: • 8/16/32/64 Gbps FC Module • 10 Gbps and FCoE Module • 10G ports of FCIP		
7	All FC ports for device connectivity should be 8/16/32/64 Gbps auto-sensing Fibre Channel ports.		
8	The switch module must support switching across the entire 48-ports on a module/linecard as single switched domain. The latency between any two ports chosen within the module or across modules needs to be consistent.		
9	The switch must be able to support non-disruptive software upgrade.		
10	The switch must be able to support stateful process restart.		
11	The switch must support port aggregation of up to 16 physical Fibre Channel ports into a single aggregated link. The aggregated ports must NOT be consecutive ports on a line card and should support distributed model.		
12	Switch should provide comprehensive tool set for analysing, troubleshooting, and debugging storage networks. Power-on self-test (POST) and online diagnostics to proactively monitor system health. Identify the exact path and timing of flows with capabilities such as Fibre Channel traceroute. Capture network traffic using Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) without any limitation.		

#	Description	Compliance (Y/N)	Remarks
13	When operating at 64Gbps FC speed with FEC turned on, the switch(or director platform) should offer consistent switching with same latency across the ports.		
14	Proposed switch or via solution should have the capability to provide FC analytics natively on switch ports or via external monitoring agent. The analytics solution should help measure via GUI end2end traffic from host to storage along with Disk Access Latency, Exchange completion times, SCSI related errors etc.. All licenses need to be provided from day one		
15	When analytics is turned on parameters such as disk access latency, exchange time completion, rx/tx rates, etc need to be shown for end to end traffic from server to storage and back.		

3.4.1.7 Tape Library

#	Description	Compliance (Y/N)	Remarks
1	Should have sufficient speed backup to Tape Library in High Availability for backing up data from the SAN without any user intervention.		
2	Should support latest technology-based library with Latest LTO tape drives, rack mountable with redundant power supplies.		
3	Cartridges should provide native/raw data capacity of 12 TB, max compressed speed of 360 MB/s		
4	Solution should include LTO 8 Media Cartridges with Cleaning Cartridges, Barcode labels shall also be provided		
5	It should support tape-based data encryption with the longest and most secure keys - 256 bits.		

#	Description	Compliance (Y/N)	Remarks
6	It should support web based remote manageability to allow monitoring and managing of the library		
7	Web based interface should give - Status information, health, configuration and operations, reporting, error and status logs, Library and drive firmware upgrade capabilities, Diagnostic tests and information, Cartridge movement for maintenance and management purposes, Security and access control.		
8	It should support SNMP for device monitoring, HTTPS web console, IPv6		
9	Device should have link path failover features, power and cooling fans redundancy		

3.4.1.8 VTL – Virtual Tape Library

#	Description	Compliance (Y/N)	Remarks
1	Should be able to interface with different server platforms and operating systems simultaneously via NFS v3, CIFS and FC.		
2	Should support LAN, SAN & NDMP backup solutions simultaneously		
3	Must support Inline data duplication technology at block level using variable block length technology		
4	Must support VLAN tagging.		
5	Must support both LAN D2D backup and VTL backup at the same time		
6	Must support single management pane for multiple storage arrays for ease of management		

#	Description	Compliance (Y/N)	Remarks
7	Must have the ability to perform different backup or restore jobs simultaneously		
8	Must support for deduplicated and may support encrypted Replication of data over Local or Wide Area Networks		
9	Must support 10Gb Ethernet connectivity		
10	Must support point-in-time copies of a LUN or volumes with minimal performance impact		
11	Must supports communications and data transfers through 2x4GB/2x8GB FC SAN, 4 x 1 Gb/4x10Gb Ethernet LAN		
12	Should support capacity on demand feature that allows the storage allocation associated with a virtual tape cartridge to be consumed upon write, and not creation		
13	Should support auto support remote health check for OEM to monitor the system health.		
14	Should support at least 10TB/hr backup throughput.		
15	VTL should support single storage/de-duplication pool and load balancing across multiple tape libraries configured in the proposed VTL.		
16	Should support different retentions for primary and DR backup storage		
17	Must support global and target based deduplication which should also support deduplication at backup server level.		
18	Must protect against lost data in power fail and software crashes		
19	Must support Data compression using lz, gz or gzfast		
20	Must support selective replication to sub share level replication, must support schedule throttle of network		

#	Description	Compliance (Y/N)	Remarks
	bandwidth depending on the utilization of the WAN bandwidth		
21	Must support simultaneous replication process while backup is running		
22	Replication Should support bi-directional, many-to-one, one-to- many, and one-to-one replication		
23	Should support recovery from replica.		
24.	Must support ACL for CIFS/NFS/telnet/http/https/ftp/ssh		
25	Should support Link Aggregation Control Protocol (LACP)		
26	Should have SNMP and command line support.		
27	Should support IP Aliasing.		
28	Should support 256 bit AES encryption at rest.		
29	Should support retention lock feature which ensures that no data is deleted accidently.		
30	Should have inbuilt NDMP tape server.		
31	Must support RAID 6 technologies		
32	Should be able to interface with different server platforms and operating systems simultaneously via NFS v3, CIFS and FC.		
33	Should support LAN, SAN & NDMP backup solutions simultaneously		
34	Must support Inline data duplication technology at block level using variable block length technology		
35	Must support VLAN tagging.		

3.4.1.9 Network – Core Router

#	Description	Compliance (Y/N)	Remarks
1	Hardware: 1) Routers should support modular LAN and WAN connectivity options including Ten Gigabit Ethernet, Gigabit Ethernet, 40Gbps and 100Gbps (Minimum 12x 1/10G SFP+ interfaces and 4x QSFP28 interfaces - At least 2 out of 4 QSFP28 interfaces should support 100Gbps speed from day one for LAN side connectivity 2) Multi-core Processor, internal redundant field replaceable power supply (from Day1). 3) Physical separation between control and data planes processor to support seamless field upgrade/replacement without interrupting running processes and services. 4) Inline hardware accelerated encryption for high-throughput IPsec and MACsec. 5) Minimum 64 GB of on-board DRAM/RAM for data plane and control plane processes. 6) 2x LAN side interfaces to be populated with 100Gbps multi-mode transceiver modules. WAN side modules to be considered as per design needs.		
2	Performance: 1) Minimum IP forwarding throughput of 190Gbps/higher. 130Gbps/higher IPSEC Bandwidth, 30Gbps/higher IMIX/EMIX encryption throughput. 2) 4000/more IPSEC tunnels. 3) 8000/more VRF segments. 4) Minimum 4M/more IPv4 & IPv6 routes. 5) 30M or more firewall sessions.		
3	Layer 2 , Layer 3 Security and other features: 1) static Routes, OSPFv2, OSPFv3, BGP4, MBGP, BFD, Policy based routing, IPv4 and IPv6 tunnelling. 2) IKEv1, L2TP, IKEv2, GRE and IPSEC. 3) Router should support Zone Based Firewall feature. 4) Support Traffic Optimization feature built in the router operating system or an external appliance for the same functionality can be provided. 5) 802.1p class of service and marking, classification, policing and shaping. 6) AES-256 and AES-GCM. 7) Hierarchical QoS should be supported both at Physical and sub-interface level. 8) Support deep packet inspection to identify applications at layer-7 and should be able to define QoS and access control based on application. It should be possible to identify at least 1000 common		

	applications by Device. 9) IGMP v1/v2/v3 and PIM multicast routing.		
4	Manageability features: 1) SSHv2, SNMPv2c, SNMPv3 and NTP. 2) support AAA using RADIUS and TACACS+. 3) Support for IP SLA or equivalent and best path selection for metrics like delay, latency, jitter, packet loss to assure business-critical IP applications from Day1. 4) Support monitoring of network traffic with application-level insight with deep packet visibility into web traffic, RTP-Based VoIP traffic.		
5	Certifications: 1) UL 60950 or IEC 60950 or CSA 60950 or EN 60950 Standards for Safety requirements of Information Technology Equipment. 2) EN 55022 Class A/B or CISPR22 Class A/B or CE Class A/B or FCC Class A/B Standards for EMC (Electro Magnetic Compatibility) requirements. 3) Certified for EAL 3/NDPP or above under Common Criteria Certification. 4) IPv6 Certified/IPv6 logo ready.		
6	OEM Services: 4 year 24x7 remote break-fix assistance and same day advance replacement hardware delivery.		

3.4.1.10 Network: Core Switches - LAN

#	Description	Compliance (Y/N)	Remarks
1	Core Switch should meet/exceed following hardware features/capacity. 1) 1U to 3U and rack mountable in standard 19" rack. 2) 8 GB RAM and 8 GB Flash and 80MB Packet buffer. 3) Hot swappable 1:1 redundant internal power supply and redundant fan. 4) Minimum 3Tbps of switching fabric and minimum 1Bpps of forwarding rate. 5) Loaded with 6x 100Gbps transceiver, 24x 10Gbps transceiver and 8x 1/10Gbps Base-T copper module. Both fiber modules should have duplex LC connector to work with multi-mode fiber supporting minimum 300 meters for 10Gbps link and 100 meters for 100Gbps link.		

#	Description	Compliance (Y/N)	Remarks
2	Core Switch should meet/exceed following performance parameters. 1) 80K MAC Addresses and 1K VLANs. 2) 25K ACLs, 30K Multicast and 80K IPv4, 80K IPv6 Routes. 3) Application visibility and traffic monitoring with minimum 60 K sflow/jflow/netFlow entries. 4) 200Gbps/more bidirectional stack throughput.		
3	Core Switch should support following Layer 2 , Layer 3, Security and other features. 1) Virtual Switching/Stack/Equivalent features allows links that are physically connected to two different switch to appear as a single port channel. 2) IEEE Standards of Ethernet: IEEE 802.1D, 802.1s, 802.1w, 802.1x, 802.3ad, 802.1ae (256-bit and 128-bit AES), 802.3x, 802.1p, 802.1Q, 1588v2. 3) AES-256 support with MACSEC-256 encryption algorithm on hardware. 3) BGP, MPLS, IS-IS, VRF, VXLAN, NAT, OSPF Routed Access, Policy-Based Routing (PBR), PIM SM, and Virtual Router Redundancy Protocol (VRRP). 4) 802.1p class of service, marking, classification, policing and shaping. Should support strict priority queuing. 5) port security, DHCP snooping, Spanning tree root guard, First Hop Security. 6) IPv6 support in hardware, providing wire rate forwarding for IPv6 network. 7) 802.1x authentication and accounting, IPv4 and IPv6 ACLs and Dynamic VLAN assignment.		
4	Core Switch should support following manageability features. 1) In Service Software Upgrade to provide an upgrade of the entire platform or an individual task/process without impacting hardware forwarding. In Service Software Upgrades to support upgrades, downgrades, and configuration rollbacks. 2) SSHv2, SNMPv2c, SNMPv3, IGMP, Netconf/YANG. 3) Configuration rollback:		

#	Description	Compliance (Y/N)	Remarks
5	Core Switch should have following certifications. 1) IPv6 certified. 2) UL 60950, IEC 60950, CSA 60950, EN 60950 Standards. 3) EAL 2/NDPP or above under Common Criteria Certification.		
6	OEM Services: 4 year 24x7 remote break-fix assistance and same day advance replacement hardware delivery.		

3.4.1.11 Access Switches LAN

#	Description	Compliance (Y/N)	Remarks
1	Access Switch should meet/exceed following hardware features/capacity. 1) 1U rack mountable in standard 19" rack. 2) 2 GB RAM and 2 GB Flash along with 6MB buffer 3) Internal field replaceable unit redundant power supply from day 1 4) Minimum 128/176Gbps of switching fabric and minimum 95Mpps/130Mpps of forwarding rate according to 24/48 port switch performance 5) 24/48 10/100/1000 Base-T ports and additional 4 nos. SFP+ uplinks ports loaded with 2x10Gbps SR transceiver. Both modules should have duplex LC connector to work with multi-mode fiber for minimum 300 meter distance) 6) All 24/48 port should support PoE (802.3af) and PoE+ (802.3at) with a PoE power budget of 740W/1440W		Include CPP
2	Access Switch should meet/exceed following performance parameters. 1) 16K MAC Addresses and 1K VLANs. 2) 1K ACLs, 1K Multicast and 3K IPv4, 1K IPv6 Routes, 128 STP Instances 3) Traffic monitoring with minimum 15K sflow/jflow/netFlow entries. 4) 80Gbps/more bi-directional stack throughput.		
3	Access Switch should support following Layer 2 , Layer 3, Security and other features.		

#	Description	Compliance (Y/N)	Remarks
	1) Switch should have dedicated slot for modular with dedicated stacking throughput and should support up to 8 switches in a stack 2) IEEE Standards of Ethernet: IEEE 802.1D, 802.1s, 802.1w, 802.1x, 802.3ad, 802.3x, 802.1p, 802.1Q 3) AES-128 support with MACSEC-128 encryption algorithm on hardware all ports. 3) Static routing, RIP, REP PIM, OSPF, VRRP, PBR and QoS. 4) 802.1p class of service, marking, classification, policing and shaping and eight egress queues. 5) IPv6 Binding Integrity Guard, IPv6 Snooping, IPv6 RA Guard, IPv6 DHCP Guard, IPv6 Neighbor Discovery Inspection and IPv6 Source Guard. 6) 802.1x authentication and accounting, IPv4 and IPv6 ACLs and Dynamic VLAN assignment. 7) Should be SDN ready with VXLAN and VRF		
4	Access Switch should support following manageability features. 1) Switch should support management features like SSHv2, SNMPv2c, SNMPv3, NTP, RADIUS and TACACS+		
5	Access Switch should have following certifications. 1) UL 60950, IEC 60950, CSA 60950, EN 60950 Standards. 2) EAL 2/NDPP or above under Common Criteria Certification.		
6	OEM Services: 4 year 24x7 remote break-fix assistance and next business day advance replacement hardware delivery.		

3.4.1.12 Network Management System (NMS) for Core and Access (Routers and Switches)

#	Description	Compliance (Y/N)	Remarks
1	The NMS will be hosted on-premises. NMS solution to provide a single pane of glass to discover, configure, provision, monitor,		

#	Description	Compliance (Y/N)	Remarks
	manage, analyze and troubleshoot the network using the features and functionalities defined below.		
2	Self learning capabilities like discovering the devices, getting onboarded using Plug and play and creating a topology automatically. Network discovery using LLDP, SNMP, IPDT, ARP Entries for host discovery. Provide complete inventory of network devices along with firmware details, also should support upgrade and downgrade of the firmwares.		
3	Templates for devices configurations. RMA workflows defined to replace the faulty devices with similar device and push right firmware, configuration and licenses to provide automation. RMA Process should be automated and it should automatically replace the device in NAC, Certificate Server and NMS database		
4	Capabilities to Integrate with SNMP, SYSLOG, DHCP, DNS, sflow/NetFlow Servers to capture the network data.		
5	Capabilities to Integrate with SNMP, SYSLOG, DHCP, DNS, sflow/NetFlow Servers to capture the network data.		
6	Application visibility using Deep Packet Inspection and also should provide visibility for known and custom applications along with SAAS based cloud applications.		
7	Support integration with Ticketing system (ITSM) to open and close the tickets automatically. Support integration with 3rd parties using North bound REST APIs.		
8	To provide POE dashboard for Endpoint devices that are pulling too much power, as well as switches that are approaching overload, are flagged. Granular visibility shows the available power on any switch for quick installation of IoT endpoint devices		
9	To provide Weekly and daily report to executives giving a summary of how their network is performing with insights into network devices, clients, and applications. Following reports to be supported - Device CPU, Memory utilization, Interface Utilization, AP, AP Radios, Rogue AP/WIPS - Threat details, Client performance, Executive summary of Client, Network and Applications		

#	Description	Compliance (Y/N)	Remarks
	performance, Network discovery inventory, Compliance, EOL and Licenses.		
10	Capabilities to alert/alarm the IT team when the issues detected over the network e.g. reachability issues, device health, link utilization and network issues and it should be categorized against criticality and shown under category like P1, P2, P3 on the dashboard		
11	Capabilities using AI and ML to identify deviations and throughput drop relate issues across the network.		
12	Support automation to provide root cause analysis against poorly connected devices, applications, clients or communication issues for the problem and recommendations to fix problem over the network in couple of minutes using AI/ML and existing knowledge base.		
13	Capabilities to monitor the health of network devices, clients connected to the devices and application accessed over the network with latency, loss information		
14	Support Network services analytics to monitor network services like DHCP, DNS and AAA to check the health of these critical services by measuring latency, transaction count etc. Proactive monitoring to reduce overall issue ticket resolution time and eventually leads to lower ticket volume.		
15	Solution should have Intelligent packet capture capability which allows admin to access the data from network devices. Network admin should be able to lively capture the packets partially / fully or scheduled.		
16	Solution should provide dashboard to view the dynamic baselines created by AI/ML for key client onboarding KPI's like onboarding time, DHCP Time, Authentication Time and Association failures of clients.		

3.4.1.13 DC Software Defined networking (SDN) Fabric Architecture

#	Description	Compliance (Y/N)	Remarks
1	Fabric Definition: 1) Proposed fabric must be the CLOS network topology architecture defined using Spine, Leaf switches with VXLAN overlay. 2) Fabric Should allow workload mobility anywhere in the DC, across the Data Center sites. 3) fabric should be able to sustain multiple link and device (Leaf & Spine), Controller failures. 4) fabric should be able with use full cross sectional bandwidth (any-to-any) across all provisioned uplink ports using equal cost multi pathing. 5) Solution should provide latency and drop analysis between end points connected to fabric with reason of drop. 6) The proposed architecture should provide a single pane for provisioning, monitoring, and management to deploy stretched policies across DC and DR.		
2	Hardware and Interface Requirement: 1) Leaf switches to Spine connectivity should use uplink port using line rate 100G only. 2) Leaf and spine switches quoted should be non-oversubscribed and perform at line rate. 3) All switches including Spine and leafs should be of line rate including access and uplink ports non-blocking. 4) All switches & proposed Fabric must support for 1000 VRF/Private network without any additional component upgrade or design change		
3	Fabric Features: 1) Fabric must support various Hypervisor encapsulation including VXLAN and 802.1q natively without any additional hardware/software or design change. 2) Fabric must auto discover all the hardware and auto provision the fabric based on the policy. 3) fabric architecture must be based on hardware VXLAN overlays to provide logical topologies that are abstracted from the physical infrastructure with no performance degradation. Fabric must support VXLAN Switching/Bridging and VXLAN Routing. 4) Fabric must support Role Based Access Control in order to support Multi - Tenant environment. 5) Fabric must integrate with different virtual machine manager viz. VMware vCenter, Nutanix AHV Prism, Kubernetes, Redhat OpenShift and manage virtualise networking from the single pane of Glass - Fabric Controller/SDN Controller for visibility of VM/Container at the controller level. 6) Fabric must integrate with L4 - L7 Physical and virtual appliances using single pane of glass - Fabric Controller / SDN Controller. 7) Fabric must provide deeper		

#	Description	Compliance (Y/N)	Remarks
	visibility into the fabric in terms of latency and packet drop between any two endpoints on the fabric. 8) Solution should provide L2 & L3 extension across sites. 9) Fabric must act as single distributed layer 2 switch, Layer 3 router and Stateless distributed firewall etc.		
4	Fabric Security Features: 1) Fabric must have zero trust policy model for connected systems or hosts to help in protecting against any kind of attacks like Unauthorized Access, Man - in - the - middle - attack, Replay Attack, Data Disclosure, Denial of Service. 2) Fabric must provide RBAC policies and support AAA using Local User authentication, External RADIUS, External TACACS+, External LDAP, External AD. 3) Fabric /SDN controller should provide micro-segmentation rules and policies for workloads connected to DC fabric for east-west traffic . It must support segmentation of VM based attributes like hostname, OS, VM Tags. 4) Fabric must support Micro Segmentation for the Virtualize and Non - Virtualize environment (BareMetal, Container). 5) Fabric must support true multi - tenancy. 6) Fabric must act as a State-less distributed firewall with the logging capability. 6) Fabric must be capable of dynamically insert physical and virtual L4 - L7 (FW,LB) services between multiple segment using policy base traffic redirect.		
5	Fabric management: 1) Fabric must provide Centralised Management Appliance or SDN Controller - Single pane of glass for managing, monitoring and provisioning the entire Fabric within Data Center & across all Data Centers. 2) Fabric must Auto discover all the Spine and Leaf switches and auto provision them based on the Fabric policy using Centralised Management appliance or SDN Controller. 3) Fabric must be capable of dynamically insert physical and virtual L4 - L7 (FW,LB) services between multiple segment using policy base traffic redirect for East-West traffic. 4) Centralised management appliance or SDN Controller should not participate in Data plane and control plane path of the fabric. 5) Solution should support bug, PSIRT etc visibility. 6) Solution should support device views, interface stats, config snapshot diff view. 7) Solution should support periodic snapshot of configuration which will help to rollback in case of any issue post configuration in fabric. 8) Support mechanism to quickly suggest utilization of configured and learned resources in		

#	Description	Compliance (Y/N)	Remarks
	terms of VLAN, routes, end points etc for better capacity planning. 9) Provide visibility of end point (virtual, BM and container) connected to fabric including VM and Hypervisor details with virtual port. 10) Provide instant visibility into any applicable bugs, security advisories and field notices for running hardware and configuration. 11) Support a single consolidated view of all the objects including links, devices, their relationships, the real-time status of their utilization, and a quick at-a-glance assessment of the current status of the entire system or any subset of the system for better event corelations. 12) Flow telemetry should support hardware acceleration so that it is not impacting CPU performance. 13) Centralised management appliance or SDN Controller must communicate to south bound devices using open standard protocol i.e. OPFLEX / OPENFLOW / OVSDB etc. or using Device APIs. 14) Centralised management appliance or SDN Controller must run in "N + 1" redundancy to provide availability as well as function during the split brain scenario. 15) In Event of all Centralised management appliances or SDN Controllers fails, the fabric must function without any performance degradation and with the current configuration. 16) Centralized management appliance or SDN Controller provide dynamic device inventory of the Fabric as well as current network topology of the fabric. It must also validate the cabling connectivity and generate alarms in case of wrong or faulty connectivity. 17) Centralised management appliance or SDN Controller must support multi tenancy from management perspective and also provide Role Based Access Control per tenant for the tenant management.		
6	All infrastructure required by fabric controllers to support the listed features and scale, should be provided by the bidder		

3.4.1.14 Data Center Spine Switch

#	Description	Compliance (Y/N)	Remarks
1	Hardware/Design: 1) The core/spine layer switches should have hardware level redundancy (1+1). 2) The switch should have redundant CPUs from day 1 and should not have any single point of failure like switching fabric, power supplies and fans. 3) Non-blocking architecture, all proposed ports must provide wire speed line rate performance. 4) Support hot insertion and removal of different parts like modules/power supplies/fan tray etc. 5) should have adequate power supplies for the complete system usage with all slots populated and used, providing N+1 redundancy. 5) Support Graceful Restart for OSPF, BGP etc. and should support uninterrupted forwarding operation to ensure high availability during primary controller failure		
2	Performance and Scale: 1) Min of 36 non-blocking interfaces populated with 100Gbps multimode fiber Transceivers. 2) Chassis should be capable of supporting 400Gbps from day1 without change in the base chassis components (supervisor, fabric, power supplies etc). 3) minimum 3.6 TBPS of switching capacity. 4) should support intelligent buffer management with a minimum buffer of 40MB. 5) Should support minimum 1000 VRF instances with route leaking functionality, minimum 500K IPv4 LPM routes, 100K multicast routes, minimum 500K of MAC addresses, minimum of 28Tbps switch bandwidth and 150MB Packet Buffer per line card.		
3	Network Virtualization Features: 1) Network Virtualisation using Virtual Over Lay Network using VXLAN. 2) support VXLAN and EVPN symmetric IRB for supporting Spine - Leaf architecture to optimise the east - west traffic flow inside the data center		
4	Layer2 Features: Spanning Tree Protocol (IEEE 802.1D, 802.1W, 802.1S), VLAN Trunking (802.1q), VLAN tagging (IEEE 802.1q), IEEE Link Aggregation and Ethernet Bonding functionality (IEEE 802.3ad) to group multiple ports for redundancy, layer 2 extension over VXLAN across all Data Center to enable VM mobility &		

#	Description	Compliance (Y/N)	Remarks
	availability, BGP EVPN Route Type 2, Type 4 and Route Type 5 for the overlay control plane.		
5	Layer3 Features: 1) Support non-blocking Layer 2 switching and Layer 3 routing. capable to function in line rate for all ports. 2) Complete STACK of IP V4 and IP V6 services. 3) Switch should support static and dynamic routing, segment routing and VRF route leaking functionality, 4) Multicast routing, multicast traffic reachable using PIM-SM, PIM-SSM & Multicast Source Discovery Protocol (MSDP). 5) should be able to re-converge all dynamic routing protocol at the time of routing update changes i.e. Graceful restart for fast re-convergence of routing protocols (OSPF, IS-IS, BGP).		
6	Quality of Service: 1) Switch system should support 802.1P classification and marking of packet using CoS (Class of Service) & DSCP (Differentiated Services Code Point). 2) Support for different type of QoS features for ream time traffic differential treatment using Weighted Random Early Detection & Strict Priority Queuing. 3) support to trust the QoS marking/priority settings of the end points as per the defined policy.		
7	Security: 1) Control plane Protection from unnecessary or DoS traffic by control plane protection policy. 2) Support for external database for AAA using TACACS+ & RADIUS. 3) Should support to restrict end hosts in the network. Secures the access to an access or trunk port based on MAC address to limits the number of learned MAC addresses to deny MAC address flooding. 4) Support MAC Sec (802.1AE) in hardware. 5) Role Based access control (RBAC) for restricting host level network access as per policy defined.		
8	Manageability: 1) Switch should support for sending logs to multiple centralised syslog server for monitoring and audit trail. 2) Should provide remote login for administration using Telnet, SSHv2, Flow path trace (ingress to egress switch), Latency and packet drop. 3) Monitor utilization of Operations like MAC/Route & Hardware resources like port utilization/ BW, Switch environmental like		

#	Description	Compliance (Y/N)	Remarks
	(CPU/memory/FAN/Power Supply), Interface statistics like CRC error. 4) Flow telemetry should support hardware acceleration so that it is not impacting CPU performance. 5) support for management and monitoring status using different type of Industry standard NMS using SNMP v3 with Encryption. 6) Should provide different privilege for login in to the system for monitoring and management.		

3.4.1.15 Data Centre Leaf Switch

#	Description	Compliance (Y/N)	Remarks
1	Hardware: 1) 1 RU fixed form factor, rack mountable with redundant Power units. 2) Minimum 48x 1/10/25Gbps SFP28 interfaces populated with 25Gbps transceiver modules for host connectivity and 6x 100G ports populated with 100Gbps modules for Spine connectivity. 3) console port for local management & management interface for Out of band management. 4) Minimum 20% of the ports per switch should be free for future utilization.		
3	Performance & Scale: 1) Support non-blocking Layer 2 switching and Layer 3 routing. capable to function in line rate for all ports. 2) should be able to re-converge all dynamic routing protocol at the time of routing update changes i.e. Graceful restart for fast re-convergence of routing protocols (OSPF, IS-IS, BGP). 3) Support minimum 1000 VRF instances with route leaking functionality, 1700K IPv4 LPM routes, minimum 3.6 TBPS of switching capacity (or as per specifications of the switch if quantity of switches are more, but should be non blocking capacity) and should support intelligent buffer management with a minimum buffer of 40MB. 4) Should support minimum 90k of MAC addresses		
4	Network Virtualization: 1) Support virtual Over Lay Network using VXLAN. 2) Support VXLAN and EVPN symmetric IRB for supporting Spine - Leaf architecture to optimise the east - west traffic flow inside the data center		

#	Description	Compliance (Y/N)	Remarks
5	Layer2 Features: Spanning Tree Protocol (IEEE 802.1D, 802.1W, 802.1S), Switch should support VLAN Trunking (802.1q), VLAN tagging (IEEE 802.1q), IEEE Link Aggregation and Ethernet Bonding functionality (IEEE 802.3ad) to group multiple ports for redundancy, Link Layer Discovery Protocol as per IEEE 802.1AB for finding media level failures, layer 2 extension over VXLAN across all Data Center to enable VM mobility & availability, DC Bridging i.e. IEEE 802.1Qbb Priority Flow Control (PFC), Data Center Bridging Exchange (DCBX), IEEE 802.1Qaz Enhanced Transmission Selection (ETS), Explicit Congestion Notification (ECN), BGP EVPN Route Type 2, Type 4 and Route Type 5 for the overlay control plane.		
6	Layer3 Features: 1) Support the complete STACK of IPv4 and IPv6 services. All Functionalities of Switch shall be IPv6 compliant and it should work on IPv6 Platform without any additional hardware/ software. 2) Switch should support static and dynamic routing, segment routing and VRF route leaking functionality, Segment Routing and Layer3 VPN over Segment Routing, multi instance routing using VRF/ VRF Edge/ Virtual Router routing and should support VRF Route leaking functionality. 3) Provide multicast traffic reachable using PIM-SM & PIM-SSM. 4) Multicast Source Discovery Protocol (MSDP) and IGMP v1, v2 and v3.		
7	Quality of Service: 1) Support 802.1P classification and marking of packet using CoS (Class of Service) & DSCP (Differentiated Services Code Point). 2) Support for different type of QoS features for real time traffic differential treatment using Weighted Random Early Detection & Strict Priority Queuing. 3) Rate Limiting - Policing and/or Shaping. 4) support to trust the QoS marking/priority settings of the end points as per the defined policy.		
8	Security: 1) Support control plane Protection from unnecessary or DoS traffic by control plane protection policy. 2) Support for external database for AAA using TACACS+ & RADIUS. 3) support to restrict end hosts in the network. Secures the access to an access or trunk port based on MAC address. It limits the number of learned		

#	Description	Compliance (Y/N)	Remarks
	MAC addresses to deny MAC address flooding. 4) VXLAN and other tunnel encapsulation/decapsulation should be performed in single pass in Hardware. 5) Support for Role Based access control (RBAC) for restricting host level network access as per policy defined. 6) support DHCP Snooping, dynamic ARP Inspection, IP Source Guard and unicast and/or multicast blocking on a switch port. 6) Support to suppress the flooding of frames destined for an unknown unicast or multicast MAC address out of that port. 7) Support broadcast, multicast and unknown unicast storm control. 8) LLDP, MAC Sec (802.1AE) in hardware and Spanning tree BPDU protection.		
9	Manageability: 1) Modular OS with dedicated process for each routing protocol. 2) Switch should support for sending logs to multiple centralised syslog server for monitoring and audit trail. 3) remote login for administration using Telnet & SSHv2. 4) support for capturing packets for identifying application performance using local and remote port mirroring for packet captures. 5) Switched Port Analyzer (SPAN) with minimum 4 active session and ERSPAN on physical, Port channel, VLAN interfaces. 6) Management and monitoring status using different type of Industry standard NMS using SNMP v1 and v2, SNMP v3 with Encryption. 7) Provide different privilege for login in to the system for monitoring and management. 8) Open APIs to manage the switch through remote-procedure calls (JavaScript Object Notation [JSON] or XML) over HTTPS after secure authentication for management and automation purpose. 9) Support monitoring of events and take corrective action like a script when the monitored events occurs. 10) Built-in tools to troubleshoot flow path issues, including latency and packet loss.		
10	Availability: 1) Provide gateway level of redundancy Ip V.4 and IP V.6 using HSRP/VRRP. 2) support for BFD For Fast Failure Detection.		

3.4.1.16 DC/DR Network Monitoring and Operations Dashboard

#	Description	Compliance (Y/N)	Remarks
1	The Solution must provide the capability to create and show a graphical representation of all Network Elements in the design.		
2	The Solution must be able to interface through open APIs with external ticketing systems, centralized Observability systems used in the NOC. Must integrate with 3rd-party systems through open APIs for additional reporting, with the minimum of time series databases and graphing applications		
3	The Solution must provide the capability to search endpoint on the network using MAC / IP / Subnets.		
4	The Solution should support flow analytics (NetFlow/sFlow/IPFIX) for visibility into traffic usage by end-points. Solution should provide flow analytics using hop by hop traffic statistics, latency and packet drop info for specific flows with reason of drop, which helps identify, locate and root-cause data path issues across fabric architecture.		
5	Solution must provide deeper visibility into the fabric in terms of latency and packet drop traffic profile, anomalies and performance parameters between any two endpoints on the fabric		
6	Solution should provide capability to proactively monitor network health over time by using time-synced data across multiple parameters to derive deeper understanding of issues and behaviours, consequently should help in knowing the impacted endpoints, applications, and flows due to network anomalies		
7	Solution should help to track per-hop information and behaviour. It should also help to verify software and hardware programming consistency across all available traffic paths between source and destination endpoints.		
8	Solution should be able to help in the Day-2 Operation that involves root cause analysis by providing below features:		

#	Description	Compliance (Y/N)	Remarks
	a) Locate virtual machines, bare-metal hosts, and other endpoints across the entire fabric. b) Gather sequence of events from past data and provide intelligent insights. c) Provide automated root-cause analysis of data-plane anomalies, such as packet drops, latency, workload movements, routing issues, ACL drops, and more by leveraging Flow Telemetry /Flow-Telemetry Events. d) Avoid network disruption when changing configurations by predicting the impact of the intended changes before deploying. e) Provide efficient capacity planning to maintain top network performance and provide fabric-wide visibility of resource utilization and historical trends.		
9	The Solution should provide information of bugs and field notices, also it should provide the details to stay secure and prevent unscheduled downtime.		
10	Solution should help to ensure establishing golden configuration and communication rules , and providing adherence to IT governance and security policies in the network.		
11	The Solution should provide the advanced reporting capabilities like exporting the anomaly and advisory summaries through email and PDFs, provide email alerts or notification. The solution should also provide capability to export and store flow-telemetry JSONs in external storage/servers for audit purpose.		Need to check for ODF compatibility
12	The solution should provide a full-featured Network threat analyser capability to detect threats emerging from inside the network (i.e., ones that have not passed through a perimeter FW/IPS). This includes the ability to establish “normal” traffic baselines through flow analysis techniques and the ability to detect deviations from normal baselines.		
13	Unsupervised and supervised machine learning along with probabilistic mathematics without predefined rules and signatures should be employed by the solution to detect significant anomalies and drifts in user, device or network activities and traffic that signal an attack.		

#	Description	Compliance (Y/N)	Remarks
14	The solution should be able to get threat intelligence from research team to make detections of malware activity with higher accuracy and efficacy including Botnets, C&C servers, Bogons, Tor Entry/Exit Nodes, Connections to bad reputation Nations and Dark IPs..		
16	The solution deployment must be capable of consuming both flow based for telemetry across the network and sensor based telemetry to monitor networks passively and generate telemetry for segments that are not natively flow capable.		
17	The solution should detect common anomalous events like Scanning, Malwares, Unexpected application services (e.g., tunnelled protocols, backdoors, use of forbidden application Protocols), Policy violations, etc.		
18	The solution should be able to investigate on-demand the cryptographic parameters for sessions between a server and its clients i.e. Number of encrypted connections made to servers that store critical data, TLS version, Cipher suite being used, Data volume and Key length to quickly determine vulnerable and out of policy TLS sessions.		
19	The solution should support the enrichment of a flow to provide information about source/destination - MAC/IP/Port numbers and country, application name, Bytes, Packets, RTT, SRT, URLs, TLS versions Client Side, TLS version and cipher in use from server side, Username, Proxy IP address, NAT device, action taken-allowed/denied, etc. are available.		
20	The solution should be able to combine/stitch the flow records coming from different network devices like routers/switches/firewall/endpoints/NAT gateway that are associated with a single conversation and present them as a single bi-directional flow record including traffic traversing NAT devices.		
21	The solution should provide application bandwidth utilization graph for various applications which should include bandwidth consumption for top hosts and trends on network bandwidth utilization.		

#	Description	Compliance (Y/N)	Remarks
22	The solution should have capability to assign risk and credibility rating to alerts and hosts and present critical high fidelity alerts prioritized based on threat severity with contextual information on the dashboard.		
23	The solution should be capable of providing visibility of east-west traffic in an encapsulated Software Defined Network fabric by decapsulating the overlying VxLAN headers to track endpoints.		
24	The solution should integrate with a Network Access Control (NAC) solution to alert the admin, provide mitigation actions like quarantine / block / apply custom policies both automatically on the endpoint to block further spread of the malware/worm across the network without affecting legitimate traffic on the network.		

3.4.1.17 Server Load Balancer

#	Description	Compliance (Y/N)	Remarks
1	Platform should provide application acceleration, reducing load on websites/Application and performing load balancing as well as other features (SSL offload, proxy/reverse proxy, content routing, L4/L7 firewalling and more)		
2	Solution should support hardware-based SSL acceleration.		
3	Solution should have dual power supply from day 1		
4	Solutions should support active-active and active-backup high availability from day 1		
5	Solution should support network-based failover for session mirroring, connection mirroring and heartbeat check		
6	Solutions should support full configuration and session sync.		
7	Solutions should be able to synchronize of the ruleset, configured policies objects in both units		

#	Description	Compliance (Y/N)	Remarks
8	Solution should support Static NAT, Hide NAT, and Dynamic NAT for flexibility and scalability		
9	Should support VLAN and port Trunking support		
10	Support integration with SDN technology like Cisco ACI, Nutanix, OpenStack, and Ansible		
11	Solution should have NVGRE and VXLAN Support		
12	Should have IPv6 Support for SLB, interfaces, routing, and firewalling		
13	The solution should supports layer4 and layer 7 load balancing for well-known protocols like HTTP, HTTPS, TCP, UDP, FTP, RADIUS, RDP, SIP, DNS and more		
14	The solution should supports the following load balancing methods: a. Round-Robin b. Weighted Round-Robin c. Least Connections d. Fastest Response e. Host f. Host Domain		
15	Solutions should provide application & server health checks for well-known protocols like ICMP, TCP, TCP_ECHO, HTTP, HTTPS etc.		
16	The solution should support application (JavaScript, xml) and text (CSS, html, xml, custom plain) compression/ decompression for web site acceleration		
17	Solution should support SSLv3, TLSv1.0, TLSv1.1, TLSv1.2, TLSv1.3		

3.4.1.18 Global Load Balancer

#	Description	Compliance (Y/N)	Remarks
1	Automatic failover between primary and secondary Data centers to ensure speedy disaster recovery in the event of an outage/failure.		
2	Global load balancer (GLB) should ensure high availability and consistent performance of applications and websites from DC and DR.		
3	GLB should be able to measure client load and ensure that requests are distributed for distribution across both DC and optimal performance.		
4	The GLB should support both Active - Passive and Active/active load balancing between Primary and secondary DC		
5	The device should be able to detects that DC site failure and should be capable of initiating operations from secondary DC (DR) automatically.		
6	Should have required capacity to support DC and DR requirements for project duration		
7	The Device should be capable of real-time health monitoring to enable immediate detection of outages and ensure high availability.		

3.4.1.19 Network Access Control

#	Minimum Technical Specifications/ Requirements	Compliance (Y/N)	Remarks
1	The solution should offer comprehensive visibility of the network by automatically discovering, classifying, and controlling endpoints connected to the network to enable the appropriate services per endpoint.		
2	The solution should be appliance-based hardware application capable of interfacing to all networked devices without impacting existing throughput or performance. It should		

#	Minimum Technical Specifications/ Requirements	Compliance (Y/N)	Remarks
	provide a highly powerful and flexible attribute- based access control solution that combines authentication, authorization, and accounting (AAA); profiling; posturing and guest management services on a single platform.		
3	Support comprehensive visibility of the network by automatically discovering, classifying, and controlling endpoints connected to the network to enable the appropriate services per endpoint.		
4	The solution should enforce security policies by blocking, isolating, and repairing noncompliant machines in a quarantine area without requiring administrator attention. The solution should also include a manual override in case the endpoints should not be blocked. The bidders shall submit a detailed plan to DRP for deploying this solution in phases across the endpoints at locations, NoC, SoC, Data Centers etc.		
5	The solution should be able to carry out a network-based profiling by targeting specific endpoints (based on policy) for specific attribute device scans, resulting in higher accuracy and comprehensive visibility of components present on the network including IT, OT and IoT devices.		
6	The solution should be able manages endpoint access to the network with the endpoint Protection Service, which enables administrators to specify an endpoint and select an action - for example, move to a new VLAN, return to the original VLAN, or isolate the endpoint from the network entirely through a GUI.		
7	The solution should have predefined device templates for a wide range of endpoints, such as IP phones, printers, IP cameras, smart phones, tablets, IoTetc.		
8	Should support Includes a built-in web console for monitoring, reporting, and troubleshooting to assist helpdesk and network operators in quickly identifying and resolving issues. Offers comprehensive historical and real-time		

#	Minimum Technical Specifications/ Requirements	Compliance (Y/N)	Remarks
	reporting for all services, logging of all activities, and real-time dashboard metrics of all users and endpoints connecting to the network.		
9	The solution should have integrated LDAP/Radius server with Certificate Authority. If not available natively bidder can propose additional component.		
10	Solution should support allow end users to interact with a self-service portal for device on- boarding, providing a registration vehicle for all types of devices as well as automatic supplicant provisioning and certificate enrolment for standard PC and mobile computing platforms.		
11	Should provide a Registered Endpoints Report which provides information about a list of endpoints that are registered through the device registration portal by a specific user for a selected period of time. The report should provide the following details such as Logged in Date and Time, Portal User (who registered the device), MAC Address, Identity Group, Endpoint Policy, Endpoint Policy ID and Device Registration Status.		
12	should support a wide range of access control mechanisms, including downloadable access control lists (dACLs), VLAN assignments, URL redirect/ or tag's.		
13	Solution must support Non 802.1x technology on assigned ports and 802.1x technologyon open use ports.Solution should support MAB and can further utilize identity of the endpoint to apply the proper rules for access.		
14	Solution should have capability to administrate devices through TACACS+ from day one. It should come with prebuilt command set profiles for deny all commands, allow all commands and show only commands with ability to define custom command sets with options to list the permitted command or negate option to not allow any other command that is not listed in the command set.		

#	Minimum Technical Specifications/ Requirements	Compliance (Y/N)	Remarks
15	The solution should provide granular compliance checks for Windows, MAC and Linux minimally supporting the following: - Check operating system , service packs , hotfixes - Check process, registry, file & application - Check for Antivirus installation , Version , Antivirus Definition Date - Check for Antispyware installation , Version , Antispyware Definition Date - Check for windows update running & configuration - Ability to run custom scripts and policies "		
16	The solution should automatically enforce security policies by blocking, isolating, and repairing noncompliant machines in a quarantine area with appropriate notifications to the administrator		
17	The hardware appliance should come with minimum 4 x 10G SFP interfaces, 64GB RAM and 1TB Disk. Each appliance should have redundant hot swappable power supply and fan module/tray.		
18	The solution should support Federal Information Processing Standard (FIPS) 140-2		

3.4.1.20 Miscellaneous Hardware: Rack

#	Description	Compliance (Y/N)	Remarks
1	42U Rack with USB KVM Switches with LCD monitor. Power panels and connectors shall support dual source and power panels shall include power meters.		

3.4.1.21 Miscellaneous: Installation and Configuration

#	Description	Compliance (Y/N)	Remarks
1	Servers, Network and devices to be install and configure as per the Employers requirement at the time of deployment.		

#	Description	Compliance (Y/N)	Remarks
2	Cat 6 and Multimode fiber with LC connectors to be used for cabling.		

3.4.2 Infrastructure Platform and User Experience, Monitoring Platforms

3.4.2.1 Virtualization Platform

#	Description	Compliance (Y/N)	Remarks
1	Provide a highly-available administrative console for management of the virtual data center platform to conduct activities such as onboarding/managing/updating hosts, virtual machines, storage and networks.		
2	Provide the ability to create new virtual machines from scratch or based on templates (created from fully configured virtual machines) Software shall support Open-Source Container Solution		
3	Provide the ability to hot-add CPU and memory and hot-plug disks and NICs (provided the same is supported by the guest operating system).		
4	Enable consolidation of VMs on fewer hosts and automatically power down unused capacity to reduce power/cooling requirements. It shall also leverage deep process power state of the CPU at the host level to further optimize power & cooling requirements.		
5	Provide the ability to boot from iSCSI, FCoE, Fibre Channel SAN , locally attached USB storage and network PXE boot.		
6	Provide support for heterogeneous guest operating systems such as Windows (Desktop & Server OS) and Linux (at least Red Hat, SUSE, Ubuntu and CentOS) and Solaris x86.		

#	Description	Compliance (Y/N)	Remarks
7	Provide the ability to expand virtual disks (boot and non-boot disks) without downtime and provide options for locating new virtual disks for existing workloads on different tiers of storage for both Windows and Linux workloads.		
8	Provide I/O prioritization for virtual workloads to ensure that business critical VMs are not affected due to congestion by other VMs on the same host.		
9	Provide a highly-available platform with built-in clustering capability leveraging both network & storage communication for cluster heartbeats. Failure of the management network shall not result in downtime for the workloads.		
10	Solution shall provide zero downtime hosts patching with maintenance mode to move running workloads to other hosts on the platform with a consistent audit trail of the patching process.		
11	Provide continuous availability for critical application workloads in the event of server failures by creating a live shadow instance of a virtual machine that is always up-to-date with the primary virtual machine thus enabling fault tolerance with zero downtime.		
12	Provide a centralized interface from which virtual machine access switching for the entire data center can be configured, monitored and administered.		
13	Support configurations of 802.1q VLANs which are compatible with standard VLAN implementations from other vendors.		
14	Shall continuously monitor utilization across virtual machines and should intelligently allocate available resources among virtual machines		

#	Description	Compliance (Y/N)	Remarks
15	Support an option to securely boot workloads using the UEFI (Unified Extensible Firmware Interface) when available in hardware to ensure that only signed drivers & OS loaders are loaded while booting.		
16	Support AES-128 and AES-256 encryption (in conjunction with any KMIP 1.1 compliant KMS server) of the workloads when at rest on storage without modifying the Guest OS.		
17	Solution must intelligently learn the environment behavior; based on usage patterns, preemptively rebalances workloads before demand spikes.		
Storage			
1	Have in-built software defined storage capability integrated within the hypervisor itself and shall work without the need for any specialized dedicated controller virtual appliance.		
2	The software defined storage solution shall support the capability of increasing the storage capacity by simply adding another hard drive in the physical node instead of adding another physical server in the cluster. Cluster scalability minimum up to 50 Nodes shall support.		
3	The solution shall be able to accelerate read/write disk I/O traffic with built-in caching on server-side flash devices to optimally minimize the storage latency.		
4	Provide highly efficient VM-centric snapshots and clones with support for up to 28 snapshots/ clones per VM and leveraging the unique Software defined storage file system.		
5	Limit IOPS consumption per VM to better manage performance SLAs for different workloads.		
6	Provide end-to-end software checksum of data enables automatic detection and resolution of silent disk errors and ensures data integrity. Data Consistency Scanning/Scrubbing shall run in the background.		

#	Description	Compliance (Y/N)	Remarks
7	Solution shall support all flash more than 98K IOPS per host with consistent sub-millisecond response times.		
8	Shall support stretched clusters that span across two geographic locations.		
9	Solution health service includes preconfigured health check tests to monitor, troubleshoot, diagnose the cause of cluster component problems, and identify any potential risk.		
10	Solution shall provide self-healing and data re-balancing		
11	shall perform block-level deduplication and compression to save storage space.		
12	shall provide data at rest encryption at both cache layer (journaling) and capacity disks (layer)		
Management Platform			
1	The virtualization management software shall provide the core administration interface as a single Web based interface. This interface shall be flexible and robust and shall simplify the hypervisor control through shortcut navigation, custom tagging, enhanced scalability, and the ability to manage from anywhere with Internet Explorer or Firefox-enabled devices.		
2	The management software shall provide the means to perform quick, as-needed deployment of additional hypervisor hosts. This automatic deployment shall be able to push out update images, eliminating patching and the need to schedule patch windows.		
3	The virtualization shall have capability to simplify host deployment and compliance by creating virtual machines from configuration templates.		

#	Description	Compliance (Y/N)	Remarks
4	Storage related and OS cluster related information has to initiate from the relevant sources and can be integrated through RESTful APIs.		
5	Virtualization management console shall provide capability to monitor and analyze virtual machines, and server utilization and availability with detailed performance graphs.		
6	Virtualization management console shall maintain a record of significant configuration changes and the administrator who initiated them.		
7	Virtualization management console shall provide the Manageability of the complete inventory of virtual machines, and physical servers with greater visibility into object relationships.		
8	Virtualization management software shall support user role and permission assignment (RBAC).		
9	Provide a single unified management console for the management of the entire environment including virtualized environment as well as software defined storage environment to simplify the manageability of the entire solution.		
10	Virtualization management shall allow you to deploy and export virtual machines, virtual appliances in Open Virtual Machine Format (OVF).		
11	Virtualization management software shall include provision for automated host patch management with no VM downtime.		
12	The management solution shall provide predictive analytics capabilities to understand baselines and model capacity and demand for accurate forecasting of infrastructure requirements.		

#	Description	Compliance (Y/N)	Remarks
13	The management solution shall give explanations and recommended solutions to performance, capacity and configuration problems. It shall be possible to associate workflows with alerts to automatically initiate corrective measures at critical thresholds.		
14	The management solution shall be able to collect and analyze all types of machine-generated log data, for example, application logs, network traces, configuration files, messages, performance data and system state dumps.		
15	Solution shall provide smooth governance and compliance policies		
Security			
1	Solution shall provide logic firewalls to protect workloads(VMs)		
2	Shall provide full features load balancer with SSL termination capabilities		
3	Platform Solution shall be capable to protect individual workload – irrespective of the workload's network subnet or VLAN.		
4	Platform Shall be able to define security policies and controls for each workload based on dynamic security groups, which ensures immediate responses to threats inside the environment and enforcement down to the individual virtual machine.		

3.4.2.2 Backup and Security

#	Description	Compliance (Y/N)	Remarks
	Analyst Rating: Backup software proposed should be in Gartner's leader quadrant for last five years in Gartner Magic Quadrant report for Data Protection / Backup Software.		
	Licensing: The proposed Backup software must offer instance based licenses with no restrictions on type of arrays (protecting heterogenous storage technologies), front end production capacity or backup to disk target capacity restrictions. Licenses and associated hardware should be supplied having License for min. 250 VM's should be included and backup appliance should be provided with 500TB capacity from Day1.		
	Reporting Capabilities: 1) Backup software should have Capability to do trend analysis for capacity planning of backup environment, extensive alerting and reporting with pre-configured and customizable formats. Any specialized reporting modules needed must be quoted along with associated hardware to achieve this functionality. All necessary hardware resources required to run this module should be supplied. 2) Proposed solution should support 24x7 real-time monitoring, with at-a-glance and drill-down views of health, performance and workload of the virtual hosts. 3) Proposed solution should have security and compliance dashboard inbuilt with the product. 4) Proposed solution should support automated action for popular alarms (automated or semi-automated), with at-a-glance and drill-down views of health, performance and workload of the virtual hosts.		
	Data Protection of Container Workload : 1) Backup software should have the ability to take application consistent backup at granular level for micro-services. 2) Proposed solution should be capable to take backup on object storage if required. Proposed solution should have inbuilt DR capability as well. 3) The proposed solution should support backup, recovery, Disaster recovery and application mobility of container based applications. 4) Solution should support various Kubernetes distributions through native API integration. Solution should support		

#	Description	Compliance (Y/N)	Remarks
	movement of container based workloads between clusters for Test / dev or cluster upgrade purposes.		
	Security &Compliance: 1) The proposed solution should have on demand scans available for malware attacks. 2) The backup Software must have inline detection & in guest detection via guest indexing against any malware attacks. 3) The proposed backup software should have four eyes approval for any backup deletion.		
	Backup support for hypervisors and Applications: 1) Backup software should be a Hardware Agnostic software and it should support snapshot integration with hypervisors like VMware, Hyper-V, Nutanix AHV nad RHEV and support de-duplication on any storage target. It should be able to backup data to tapes (like LTO) as well for long term retention. 2) The proposed backup software should provide Instant recoveries for any backup to Vmware or Hyper-V Virtual machine. It should also support the Instant VM recovery for AHV workloads as well. 3) Backup software should support file level recovery from any backup of any VM or physical server. It should support a full system recovery in case of a system crash, either on a physical system or virtual machine or as a Cloud Instance(AWS, Azure or Google). 4) The Proposed backup Software should supprot Syslog and Service Now integration. 5) Backup software should support instant database recoveries of MS SQL and Oracle from the backup files. 6) Backup software should support Multi factor authentication for accessing Backup console and console auto log-off functionality.		
	RPO/ RTO and Recovery Assurance: 1) Backup software must have a feature of data validation, whereby a workload (VM with OS and application) is powered-on in a sandbox environment and tested for its recoverability. 2) Recovery verification should automatically boot the server from backup and verify the recoverability of VM image, Guest OS and Application Consistency and then publish automated reports to be used in		

#	Description	Compliance (Y/N)	Remarks
	backup / recovery audits. 3) Backup software should provide Backup and Replication capabilities in one console only and also allow users to integrate with RBAC capabilities of the hypervisor, so that users can initiate backup and restore only those VMs to which they have access, without administrator intervention, thereby delivering self serve capabilities. 4) Proposed backup software should be able to Hardened the Linux Repository. This service will prevent backup copies of data from any corruption or ransomware attacks. 5) The software should support Group Managed Service Accounts which should have an option to users to allow change passwords after every 30 days and allows for complex password policy. 6) The proposed backup should have object storage backup. 7) Proposed backup software should have the ability to perform staged restores to enable admins to comply to regulations by selectively deleting files / records which should not be restored from the backup copies. 8) Backup software should support instant file share recovery in NAS storages to allow users to access files fast after disaster.		
	Backup and Replication Performance and SLA: 1) The proposed Backup software must allow to configure the maximum acceptable I/O latency level for production data stores to ensure backup and replication activities do not impact storage Availability to production workloads. 2) Backup software should provide Recovery of Application Items, File, Folder and Complete VM recovery capabilities from the image level backup within 15Mins RTO. 3) The software should be Network-efficient, Secure backup data replication with variable-length encryption at the source, along with compression and encryption to ensure that backups are optimized for WAN transmission. This should be ensured with or without need of any other 3rd party WAN Accelerator requirements.		
	Disaster Recovery Capabilities: 1) Replication in the software should be a VM level replication and must replicate the VM level data with or without backing it up at the source site. It should also		

#	Description	Compliance (Y/N)	Remarks
	include failover and failback capabilities and should be able to perform automatic acquisition of network addresses at the destination site. 2) The Proposed solution should support Continous replication at VM level. The RPO must be less than 5 Seconds and it must deliver Application consistency. 3) Backup and replication software must deliver maximum investment protection by supporting replication of workloads between dis-similar systems like hyperconverged infrastructure to stand alone servers and storage running similar hypervisors across sites, thereby creating a Disaster recovery environment for production qworkloads irrespective of the underlying hardware. 4) Backup software should have ability to backup data from one server platform and restore it to another server platform to eliminate dependence on a particular machine and for disaster recovery purposes. This bare metal recovery capability should be built in for the physical servers and should even work on the dissimilar hardware. 5) Backup software should have the ability to backing up a Cloud VM running in AWS or Azure and restore it as a valid VM workload back onto a Vmware server farm.		

3.4.2.3 Cloud Native Backup and Restore

#	Description	Compliance (Y/N)	Remarks
1	Cloud native applications (k8s) backup and restore Solution shall support in place restore and restore into separate namespace		
2	Solution shall be capable of application discovery i.e. Automatically pulls all meta data information and objects associated with each application like it, Persistent volumes, Secrets, Config-maps, Services etc.		
3	Solution shall have policy driven automation and end-to-end security		

#	Description	Compliance (Y/N)	Remarks
4	Shall be able to manage multiple k8s(Kubernetes) clusters from single pane (Enterprise Dashboard)		
5	Solution shall provide volume snapshots and App consistent backup and application cloning		
6	Solution shall provide Dedup and compression		
7	Shall provide exclude/include filters		
8	Solution shall be support infrastructure portability		
9	Solution shall provide logging integration capabilities		
10	Solution shall support DR and HA		
11	Shall provide Monitoring and alerting features		
12	Shall have authentication and RBAC capabilities		
13	Backup offload/Target storage solution/appliances shall be proposed by Bidder. Backup target device should have deduplication. Data domain or Object Storage or equivalent Backup retention period will be 8 months		
14	Target backup solution shall be in HA or redundancy mode		
15	Target backup shall be highly efficient for network-based replication to disaster recovery sites		

3.4.2.4 Disaster Recovery

#	Description	Compliance (Y/N)	Remarks
1	Proposed solution shall be capable of providing disaster recovery		
2	DR Site should be 100 % capacity of DC Site.		

3.4.2.5 Enterprise Container Application Platform

#	Description	Compliance (Y/N)	Remarks
1	Shall be able to run modern stateful apps more efficiently with lower TCO		
2	The container platform shall support the deployment and orchestration of multiple container formats (docker, cri-o etc.) for preventing any technology lock-in.		
3	Shall be simplified deployment and management		
4	The platform shall provide and support the adoption of DevSecOps		
5	The platform shall provide an Integrated registry and also should be able to integrate with external registries like Git, bitbucket etc.		
6	The platform should provide Enterprise authorization and authentication by integrate identity infrastructure—including Lightweight Directory Access Protocol (LDAP), open authorization (OAuth) and open ID connect (OIDC), and use a fine-grained permissions system to map to organizational structure and grant access to whole teams to manage specific repositories		
7	The platform shall have the capability to run both stateful and stateless applications		
8	The platform shall provide an auto-scaling capability for automatically running an appropriate number of container instances as per load requirements.		
9	The platform shall have inbuilt automated application container build capability – from source code to a runnable container image		
10	The platform shall provide application/container version management, auto-build of new application container instance in test environment basis on application code new version commit. Rollback to an earlier version.		

#	Description	Compliance (Y/N)	Remarks
11	Platform shall support polyglot technologies as runtime platforms for applications such as – Java, PHP, Python, Ruby, Perl, Node.js, Mysql, PostgreSQL, MongoDB, MariaDB etc.		
12	The platform shall provide CI/CD tools and also should support Integration with external CI/CD tools has to be part of the solution.		
13	The platform shall provide container instance auto-healing capability.		
14	Platform must have service Mesh that provides networking capabilities at the application layer so that application components can discover services and communicate.		
15	Platform shall support running Server-less workloads.		
16	Platform should provide a consistent, security-focused, and zero-configuration development environment.		
17	Platform should automate your container builds with integration with GitHub, Bitbucket, and more. Robot accounts allow for automatic software deployments.		
18	Platform shall provide container runtime, container orchestration, container management and container monitoring capabilities.		
19	Platform shall provide centralized logging capability (including applications logs from container instances) for audit, logs analysis & ease of management purpose.		
20	Platform must provide User-friendly Web Console for both Administrator and developer to manage and deploy applications respectively. Further, they should also be able to perform operations through CLI as well		
21	Platform should have the ability to collect and view metrics at the individual container and application level		

#	Description	Compliance (Y/N)	Remarks
22	Container should be able to allocate quotas for teams/projects in terms of CPU, Memory, Number of Pods and other Kubernetes resources that a team can consume		
23	Platform should support the Operator Framework or equivalent.		
24	Platform must provide tools to collect diagnostic information about your environment.		
25	Should be certified to Federal Information Processing Standards (FIPS)		
26	It should be able to provide network bound disk encryptions and should be able to provide encryption for local storage. It should also be able to do integration TPM/TPM (v2).		
27	Proposed container platform solution should be provided similar capabilities and capacities in DR Site as well and both the platforms should be in active-active state Container applications shall be able to deploy on both site In HA manner		

3.4.2.6 Staging Environment

#	Description	Compliance (Y/N)	Remarks
1	Staging environment sizing shall be calculated and proposed by Bidder as per the proposed production solution.		
2	Environment shall be physically isolated from production.		

3.4.2.7 Container Runtime Security and East west Traffic Inspection and Attack Mitigation Solution

#	Core Components	Compliance (Yes/No)	Remarks
Kubernetes integration			

#	Core Components	Compliance (Yes/No)	Remarks
1.	The solution shall support Kubernetes deployment on Private Cloud Native Kubernetes		
2.	The solution shall support Ubuntu 16.04, 18.04,20.04 RHEL/CentOS 7.3, 8.0 Kubernetes Host VM OS		
3.	The solution shall support CNI Spec 0.3.0 and higher, which support CNI chaining (e.g., Calico, Flannel, Weave)		
4.	The solution support Docker and CRI-O Container Runtime		
5.	The solution shall have separate Management plane and Data Plane		
6.	The solution shall support automated deployment using the following: - Helm Chart		
DevSecOps support			
1	Kubernetes integration configuration of the solution shall be specified in a YAML file so that it can be easily integrated into infrastructure deployment files for fast, repeatable deployments		
2	The solution shall run as a daemon set, allowing single command from within Kubernetes to deploy firewalls on all nodes in a cluster at once.		
3	The solution shall support threat prevention and sandbox services to block exploits, prevent malware, and stop both known and unknown advanced threats		
4	The solution shall support content inspection and SSL Decryption, preventing sensitive information from leaving your network.		
5	The solution shall support URL Filtering using machine learning to categorize URLs and block access to malicious sites that deliver malware or steal credentials		
6	The solution should support allowing access to specific GitHub repositories. FQDN and block access to the rest of the GitHub repository.		

#	Core Components	Compliance (Yes/No)	Remarks
7	The solution shall support policies defined by application, user, content, native Kubernetes labels, and other metadata to deliver flexible policies aligned with business needs		
8	The solution shall support application-level visibility, detection and protection, including: - application visibility across all ports - URL Filtering - real-time network visibility and suspicious/malicious traffic detection for in-line protection- application white-listing with user-based policies.		
General			
1	Provide single holistic platform for protecting hosts, containers and server-less functions		
2	Use defense-in-depth approach to protect the containers across their lifecycle by using continuous vulnerability management, compliance checking and enforcement, runtime defense and cloud native firewall		
3	Generate a map automatically and dynamically showing all the containers and process running and how they are inter connecting with each other		
4	Group the containers by namespaces in the map		
5	The map shall show vulnerability status, compliance status and runtime state such that the security posture of the application is instantly obtained		
6	Sensors shall run only a single instance of the agent on each VM and Kubernetes/ Docker worker node without adding any files or binaries to the containers being protected		
7	Provide a scalable platform for managing policies centrally that are enforced on thousands of nodes.		
8	auto-upgrade support for agents deployed on host and container runtime environments		
9	The offered solution shall be self-container with API server, Front end UI, Internal certificate management,		

#	Core Components	Compliance (Yes/No)	Remarks
	Database and other components bundled as single software.		
Vulnerability Management			
1	Provide continuous vulnerability management across the entire container		
2	Utilize behavioral metrics about current runtime environment to assign risk score to vulnerabilities such that vulnerabilities with highest risk can be identified		
3	Support vulnerability scanning of images in registry and repository.		
4	Provide layer by layer vulnerability analysis and pinpoints vulnerability data at each image layer.		
5	Allow definition of policies for admission control to stop images not matching the corporate vulnerability polices from being run in production environment		
6	Provide flexibility to apply different policies to different images based on container name, image name, host name and labels		
7	Highlight risk factors introduced by each vulnerability		
8	Shall be able to also take information from runtime environments and correlate vulnerability risk to them and provide risk score for top vulnerabilities in the production, UAT environment		
9	Provide plugin and command-line interface for integrating with Jenkins and other CI/CD tools such that vulnerability scan can be performed during the build process		
10	Allow definition of policies to alert and block severe vulnerabilities from moving forward in the development pipeline		
11	Report the result of vulnerability scan done in CI/CD tools on the centralized console		
12	The agent shall be able to scan the host operating system on which the containers are running and provide details of all known vulnerabilities		

#	Core Components	Compliance (Yes/No)	Remarks
13	Shall support vulnerability detection across the OS layer, application framework and custom packages.		
14	There shall be cli utility provided for performing the vulnerability scan from the terminal and also ability to be incorporated in a script for custom pipelines		
Compliance and Hardening			
1	Tool shall be officially certified for implementing the Docker, Kubernetes, and Linux CIS Benchmarks		
2	Include pre-built templates for ~~HIPAA~~, PCI, ~~GDPR~~, and NIST SP 800-190, along with 400+ certified checks for the AWS, Docker, Kubernetes, and Linux CIS Benchmarks		
3	Allow definition of policies to not just alert non-compliance but also enforce the recommendations of selected compliance Checks		
4	Provide flexibility to apply different policies to different resources based on container name, image name, host name, labels and function names		
5	Provide plugin and command-line interface for integrating with Jenkins and other CI/CD tools to enforce compliance across before the containers are being run in runtime environment		
6	Shall be extensible with support for custom compliance checks via OpenSCAP, XCCDF, and Bash scripts		
7	Support automated whitelisting of known images source to easily create a secure image baseline		
8	Provide mechanism to run images from trusted image source based on base layers, image groups, or repository		
9	Shall allow TRUST policy to be created to allow, by policy, which registries, repositories, and images to trust, and stop images from running if they are deemed non-trusted		
10	Granular policy controls prevent unauthorized images from progressing through the CICD pipeline		

#	Core Components	Compliance (Yes/No)	Remarks
11	There shall be cli utility provided for performing the Compliance and Hardening scan from the terminal and also ability to be incorporated in a script for custom pipelines		
Runtime and environment protection			
1	Learn the behaviour of each running container and build runtime model automatically		
2	Provide visibility of running containers in the terms of processes running, ports being listened, outbound connections made, domain names lookup by DNS and file system access		
3	Update runtime model of containers automatically for new application releases		
4	Detect anomalies in running workloads based on automatically generated runtime models on processes, network activities and file system access		
5	Block suspicious activities based on runtime model learned, malware database and advanced threat protection feeds		
6	Provides a unified protection framework to protect cloud native applications across different environments such as managed Kubernetes platform, self-operated Kubernetes platform, OpenShift and etc.		
7	Store forensic data as part of any security incident and displays the incident, kill chain, and data timeline for seamless incident response		
8	Shall have host OS behaviour modelling capabilities using the process and file system actions that understands the tasks that OS services need to do as a baseline		
9	Provide FIM - File Integrity monitoring Monitor files and directories against read, write, and metadata changes with alert and prevent capabilities		
10	Provide behavioural-based anomaly detection - host intrusion detection and protection for the underlying host OS		
11	The tools shall provide host and container forensics capabilities to help after action analysis of host system		

#	Core Components	Compliance (Yes/No)	Remarks
	behaviours to determine the sequence of events that lead to an incident		
12	Provide Incident forensics, logging with alert to simplify SOC Incident Response		
L4 -L7 firewall capability			
1	Perform zero-touch machine learning to automatically build network topology across hosts, containers, and server-less apps		
2	Learn new communication patterns automatically for new application releases		
3	Provide threat detection and Layer 4 protection		
4	Layer 3 firewall shall automatically model traffic flows between container micro services so teams can view traffic flows while automatically blocking anomalies without requiring manual rule creation and management		
5	Automatically detect Istio connections and traffic flows, with ability to report and quarantine entities based on the network metadata, observed behavioural anomalies, and Istio-specific compliance checks for compliance and hardening		
Architecture and Integration			
1	The tool shall provide flexibility of deploying on a Virtual machine environment and also on OpenShift or Kubernetes container environment		
2	The tool shall have extensive logging and telemetry capability		
3	The tools shall have extensive API capability and shall offer all the above features as and API		
4	The tool shall have an intuitive UI to provide rapid forensics and investigative capabilities		
5	Integrations with Active Directory, OpenLDAP, and SAML		
6	Secrets management integration with AWS System Manager Parameter Store, AWS Secrets Manager, Azure		

#	Core Components	Compliance (Yes/No)	Remarks
	Key Vault, CyberArk Enterprise Password Vault, and HashiCorp Vault		
7	Support for containers running on Linux as well as Windows host OS for containers		
8	Support for vulnerability scanning of underlying Linux host as well as Windows hosts		
9	Support for syslog based raw forensic log export		
10	Alerting integration with developer and operations tools like Jira, Slack, Pagerduty, SOAR platforms		
11	Open integration support for alert using Webhook		
12	Shall support Docker container registry, Quay and Harbor container registries		

3.4.2.8 Application Performance Management(APM) and Full Stack Observability

#	Description	Compliance (Y/N)	Remarks
1	Functional Requirements of APM and Observability Module:		
1.1	Offered Application Performance Management/Monitoring tool license tool should be provided with total visibility - from the URL to the line of code. Two sets of performance metrics are required to be closely monitored: 1) Performance experienced by end users (both front end and back end) of the application. 2) Performance metrics to measure the computational resources used by the application for the load, indicating whether there is adequate capacity to support the load, as well as possible points/locations of a performance bottleneck.		
1.2	APM tool should also broadly cater to the following requirements: 1) Monitoring to meet the three functional dimensions of digital experience monitoring (DEM); application discovery,		

#	Description	Compliance (Y/N)	Remarks
	tracing and diagnostics (ADTD); and application analytics (AA). 2) Applying data-driven analytics and ML technology to enhance the effectiveness of monitoring.		
1.3	APM tool should help monitor all the components at all layers for an optimal, application delivery and helps to improve the end user experience at the last mile. The tool strives to detect and diagnose complex application performance problems to maintain an expected level of service.		
1.4	APM tool should aim at providing comprehensive monitoring at all levels, including synthetic monitoring as well as end-user experience monitoring and provides analytics for issue tracking, auto ticketing etc.		
1.5	APM solution should provide end to end view into the business transaction monitoring and analytics for an enterprise application which also ingest transaction data either from logs or DB, correlate it with performance data of other infrastructure components and provide unified end to end real time visibility into the performance of business transaction for an application.		
1.6	The proposed solution should cover following aspect of digital experience monitoring (DEM): 1) Availability and performance monitoring which should support the optimization of operational optimisation and bahaviour of digital agents, human and machine with enterprise application and services. 2) Real User monitoring (RUM) for web and mobile based application along with synthetic monitoring capabilities to be able to effectively track the quality of user experiences perceived by end users from various geographic locations.		
1.7	The module should offer a single interface with its native intelligence to assist the IT Operations team in reducing overall MTTI and MTTR and provide the root cause analysis of an issue		

#	Description	Compliance (Y/N)	Remarks
	for faster remediation. It should also offer event correlation and de-duplication to reduce the unwanted noise across IT landscape.		
1.8	The module should offer a single interface with capabilities to consume data from multiple sources in the infrastructure, correlate and contextualise these data-points and provide a single glass view to pin-point the issue. It should also offer predictive analytics capabilities helping team to predict the outages well in advance so that team can act before it starts impacting the end users.		
1.9	End to End Monitoring: 1) Solution should provide hop by hop path visualization from fixed enrolment centres to the data centre right from the "end point/node to the network and application" to triage application & network performance issues. 2) Solution should provide the following metrics while testing the application - Availability, connect time, DNS time, response code, response Time, SSL time, Wait Time 3) Solution must support routing layer test and measure the metrics like routing path changes, reachability, and BGP updates. It should have their own BGP collectors to measure the UDI prefix performance monitoring over internet. 4) Solution should provide the layer three hop by hop visibility with network KPIs like forwarding loss, latency, jitter for faster troubleshooting 5)		
2	Full Stack Observability:		
2.1	The solution should address use cases including: 1) End-to-End Service Visibility. 2) Event Analytics. 3) Incident Investigations and Workflow. 4) 4) Problem Analysis. 5) Log Management. 6) It should be a single and integrated product for Logging, Service Monitoring and Event Analytics. 7) Single user interface for all system functionality including searching, reporting, rule building, and system administration. 8) Single, common data		

#	Description	Compliance (Y/N)	Remarks
	store for all ingested data. 9) Single search or report that can encompass all the ingested data. 10) Ability to perform "normative statistical analysis" to determine what is normal and what is not across the enterprise. 11) Offer visibility into application or service context to prioritize incidents based on business impact. 12) Ability to support troubleshooting and root cause analysis with drill down into raw data and events. 13) Offers machine learning to highlight anomalous activity based on historical trends or patterns. 14) The solution should provide out-of-the-box machine learning to group related operational events to reduce alert noise. 15) Ability to combine multiple key performance indicators to proactively detect irregularities. 16) Ability to visualize the entire technology stack from bare metal through the business layers. 17) Ability to visualize operational KPIs across the same timeline to enable root cause analysis. 18) Ability to do cross-data source correlations.		
3.1	1) Platform should be a single product that can take care of data ingestion and searching. 2) Should have out of the box AI powered features. 3) Platform should be able to monitor data from number of systems without the restrictions on format of the data. The platform should also be able to ingest logs and alerts from other monitoring tools in the environment. 4) Platform should be able to correlate the logs and alerts from various data sources. Showcase patterns, do the alert suppression to avoid multiple incident creation. 5) Platform should be able to create the service mapping and the dependencies of services which are affected during an outage. Platform should also be able to assist the analyst do the root cause of the incidents. 6) Platform should be able to help teams collaborate and reduce the MTTI, various teams needs to have role based access to various logs. 7) Platform should be able to take corrective actions as part of self-healing, actions like running a script, enabling/disabling services, delete files etc. 8) Platform should be able to use AI and ML capabilities for alert identification and predictive modelling		
4	Application Performance Management (APM)		

#	Description	Compliance (Y/N)	Remarks
4.1	The proposed solution must comprehensively cover the following 5 dimensions of application performance management: 1) End-user experience monitoring by capturing data on how end-to-end performance impacts the user, and identifies the problem. 2) Discovery of application architecture, modelling and mapping in run-time by discovering the software and hardware components involved in application execution, and their communication paths and establishing the potential scope of problems. 3) User defined transaction profiling by examining user-defined transactions, as they move across paths to identify the source of the problem. 4) Deep-dive in-context component monitoring to conduct deep-dive inspection of the resources consumed by, and events occurring within, the application components. 5) Application analytics including technologies such as behavior learning engines – to crunch the data generated, discover meaningful and actionable patterns, pinpoint the root cause of the problem, and ultimately anticipate future issues that may impact the end user. The proposed solution must be able to deliver all the above mentioned outcomes as part of one integrated user interface with no requirement to launch or access separate tools/screens. The information flow among all the modules should be in-context, correlated and seamless without the need to manually correlate and analyse data among multiple disparate tools.		
4.2	The proposed solution should provide subscription licensing models and must offer On-Premise deployment (without requiring any external connection outside customer network) option		
4.3	The proposed APM platform must support both Linux and Windows flavours for deployment of its core components (such as management server) and should not require any kind of "root access" or "root privilege" to deploy agents in the monitored applications.		

#	Description	Compliance (Y/N)	Remarks
4.4	The proposed solution should have out of the box support for automatic baselining wherein the solution can automatically learn the behaviour of monitored applications and set baseline thresholds automatically for all the monitored metrics, including: i) Application metrics. ii) Server metrics. iii) End User Metrics. iv) Custom Metrics. v) Business Metrics. vi) Database Metrics. The solution must also provide an option of fixed as well as rolling time periods to calculate these thresholds. There should not be any limit to number of metrics being auto baselined.		
4.5	The proposed solution must provide an auto-discovered dynamic visual representation of the application topology comprising of components and activities in the monitored application environment. The discovered topology visualization (map) must clearly depict the following information: i) Type of connection between components (synchronous/asynchronous). ii) Calls per minute between components. iii) Round trip time of the request between components (including network and backend time). iv) Baseline indicators for requests between components. The solution should also provide options to manage/configure/customize the visualization (map) to suit the monitoring needs.		
4.6	The proposed solution must automatically discover end-to-end, cross-component processing paths used to fulfil a request for all services provided by the monitored application, without requiring any changes to the existing application code. After discovering the transactions, the solution should be able to further categorise the transactions into below buckets automatically, based on their behaviour: i) Normal. ii) Slow. iii) Very Slow. iv) Stalled. v) Errors. The solution must be able to automatically segregate and sort these transactions based on load, errors, response times, health violations as well as percentage contribution to overall application average response time.		

#	Description	Compliance (Y/N)	Remarks
4.7	The proposed solution must trace and capture every single transaction, calculate the per minute performance (average) and send the results to the platform. The solution should then be able to detect poorly performing transactions against an automatically created baseline and dynamically profile to provide deep code level visibility. The solution should also be able to provide a mapped flow of the problematic transaction with details of participating components and time spent for request completion at each component layer as an end outcome.		
4.8	The proposed solution must provide diagnostic code level details for problematic transactions including sequential method execution details with method type, class name, method name and line number. The solution should further provide execution time per method with thread state and exit calls to remote services or database instances if any. The solution should also have an option to trigger collection of these diagnostic sessions on-demand for selected transactions, when required.		
4.9	The proposed solution should provide an option to drill down directly from any problematic transaction to: i) the server instance which was executing that transaction and provide visibility into health of the server and other transactions getting executed in that node. ii) related DB instance in-context with the queries that are being executed. iii) in-context OS level metrics. iv) correlated application logs from available log files.		
4.10	The proposed solution should also have an option to identify network performance bottlenecks and app/network-interaction bottlenecks using an agent that resides on the application instance without needing any kind of network tapping or data capture appliances. The solution should be able to detect load balancers, TCP endpoints etc. and depict it on a dynamic network map.		
4.11	The proposed solution should provide end to end visibility across all web, mobile including detailed end-user experience analysis to specifically determine: i) geographically where the heaviest		

#	Description	Compliance (Y/N)	Remarks
	application load is originated from, depicted in a geo-map. ii) geographically where are the slowest end-user response times occurring. iii) Variation in application performance by location, client type, device, browser and browser version, and network connection for web requests. iv) Variation in application performance by application and application version, operating system version, device, and carrier for mobile requests. v) Variation in application performance by slowest web/Ajax requests, and the problem isolation correlated and in context to the backend application server calls. vi) Variation in application performance by slowest mobile network requests and problem isolation correlated and in context to the backend application server calls. vii) Variation in application performance by errors and crashes on mobile and its root cause. viii) Variation in application performance by web resource performance.		
4.12	The proposed solution should provide website/application monitoring and triage the performance issue related to application or network		
4.13	The proposed solution must be able to track web and mobile user sessions to analyse any user's behaviour based on user's unique ID. There must be a provision to query for a segment of users with similar behaviour, such as from a specific geo location or visiting a specific page or using a particular device etc. The solution should also support a seamless ingestion of raw session data to an analytics engine to perform slicing and dicing on the data.		
4.14	The proposed solution should have a robust analytics engine that can ingest application performance, custom and business data from multiple sources such as: i) Application transactions. ii) End user browser requests and sessions. iii) End user mobile requests and sessions. iv) Application logs. This analytics module should have a provision to query the ingested data through UI and also a full-fledged query language to perform advanced analytics to provide insights into application performance impact on a process flow through		

#	Description	Compliance (Y/N)	Remarks
	business journey mapping, impact analysis of an issue over a period of time on users, regions and functionalities, release analytics, conversion of business KPIs to trackable metric, experience level management etc.		
4.15	The proposed solution should be able to provide in context database monitoring, supporting wide array of RDBMS as well as NoSQL. The solution should be able to report. a) top database activities (e.g. Top SQL, Top Users, Top Programs); b) database activity profile over-time (identify patterns); c) Collect and store all database wait events and correlate with SQL/Stored Procedures; d) Collect and store SQL/Stored Procedure Key Performance Indicators (CPU, Count, Reads/Writes). e) Collect and store database instance level statistics (table size, row count, indexes) f) Collect and store database server/host Key Performance Indicators (CPU, Memory, …). g) breakdown of latency of stored procedure components. h) Collect SQL Explain & Execution plans. i) Collect and store performance data on database Objects (Schemas, tables, indexes).		
4.16	The proposed solution should have capabilities to Monitor containerized application & microservices metrices without changing container image. The solution should also be capable of pulling information from the orchestration layers like kubernetes/openshift and present relevant metrics like pod metrics, node metrics, deployment metrics, endpoint metrics etc.		
4.17	The proposed solution should provide contextual monitoring of OS level metrics and provide auto correlation to the application performance. The server OS level monitoring should include general server visibility, process, volume and network metrics. There should be seamless correlation between server and application metrics through UI on the same screen without having to switch UIs.		
4.18	~~The proposed solution must have a robust alert and respond engine that leverages multiple data inputs into analysis (app~~		

#	Description	Compliance (Y/N)	Remarks
	~~performance data, machine data, analytics data and user provided data), uses Boolean logic to combine multiple conditions through AND / OR logic, has capability to disable rule evaluation temporarily for predetermined maintenance windows, can trigger alerts or notifications when rules are violated (email, SMS or custom), can utilize complex logic to combine different metrics into one trigger/alert.~~		
4.19	The proposed solution should provide mechanisms (API based or other methods) to take data feeds from various infra providers - cloud platforms, software defined data center and networking platforms as well as send data feeds and trigger actions into hybrid cloud management platforms, application resource scalability and optimization platforms and service management platforms. It should facilitate auto remediation of problems based on alert triggers and pertinent action workflows through these integrations.		
4.20	The proposed APM solution must also offer an integrated synthetic monitoring module to measure the performance (namely availability and response time) of client/browser based application (including single and multi-step transactions) using both cloud hosted and private managed agents helping to track the SLA related to the critical applications.		
4.21	The platform should offer automatic Runtime Application Self-Protection (RASP) for modern applications, keeping both users and the digital business secure by detecting vulnerabilities at runtime and defending against attacks to prevent breaches on real time basis without having a need to deploy any extra agent. The module should offer following capabilities around application security: 1. Monitor common vulnerabilities in OWASP Top 10 along with providing the related CVE details of vulnerability detected in application runtime and provide recommendation related to remediation of these vulnerabilities.		

#	Description	Compliance (Y/N)	Remarks
	2. Harvest threat intelligence feeds from multiple sources including open source databases like NIST NVD and other OEM threat feeds assisting team in identifying any potential risks. 3. Flag any risk through API ecosystem and correlate these security context with business transactions through risk score helping team to prioritise and respond to security risks and reduce overall organisational risk profile. 4. Detects and block attacks on near real-time basis along with providing details around summary of attacks (like entry point, vulnerability used, attack type etc.) for an easy hand off between security and application owner team. 5.Define policies around what runtime behaviours to ignore, detect, or block basis the runtime behaviour like Command execution, File system access, Headers in HTTP transactions, Web transactions, Network or socket access etc. One can create and configure runtime policies to specify an action to mitigate the attacks and vulnerabilities.		

3.4.2.9 Enterprise Monitoring system

#	Description	Compliance (Y/N)	Remarks
1	The Monitoring Solution should provide End to End Monitoring of Complete IT Infrastructure including: • Network Monitoring • Server Monitoring • Application Monitoring • End User Experience Monitoring • Database Monitoring • Virtualization Platform Monitoring • Storage Monitoring		

#	Description	Compliance (Y/N)	Remarks
2	The proposed solution should be capable to provide hybrid monitoring architecture through agent/agentless approach		
3	The Platform must support Event Correlation Alerting (ECA) integrations to trigger automated creation of incidents, problems, and changes based upon alarms and events correlation		
4	The proposed monitoring solution should provide capability to integrate with hardware monitoring platforms.		
5	The proposed monitoring solution should possess the inherent capability to leverage API's and SDK's to enable integration and monitoring.		
6	The proposed monitoring solution should have capability to configure actions-based rules for set of pre-defined alarms/alerts enabling automation of set tasks.		
7	The Platform must include an event correlation automatically fed with events originating from managed elements, monitoring tools or data sources external to the platform. This correlation must perform: a. Event Filtering b. Event aggregation c. Event Masking		
8	The Reporting Portal should be Completely web based with ability to define Accounts and Users for Role Relevant Views		
9	The proposed solution should provide the ability to create custom dashboards with ability to aggregate metrics from all monitored devices and should provide drill down functionality to other defined dashboards within the tool.		
10	The proposed solution should provide the ability to monitor and generate alarms for setting threshold for pre-defined Service level agreement for monitored metrics. The		

#	Description	Compliance (Y/N)	Remarks
	proposed monitoring solution should provide functionality to sync with online library for latest updates and support for new functionalities.		
Server Monitoring System			
1	The Solution should monitor heterogeneous operating systems for both physical and virtual environments OS including but not limited to Windows 32/64 bit, All Major Flavours of Linux, Solaris, Unix etc.		
2	The solution should be able to monitor non-SNMP devices (e.g. using WMI, Telnet, SSH etc.)		
3	The solution should monitor all server files, up to the lowest granularity.		
4	The solution should monitor File System Mounts for presence / absence / functionality		
5	The solution should generate alarms based on what is currently mounted compared with what is configured on a defined compliant system.		
6	The solution should support monitoring any ASCII based log files.		
7	The solution should support monitoring of Windows Event Logs and provide correlation of events for these.		
8	The solution should support monitoring of performance counters in Windows/Linux environment.		
9	The solution should support monitoring of services/processes in a Windows / Linux environment.		
10	Processes monitoring should also have ability to track CPU and Memory consumption of the monitored process for alerting and reporting/trending purpose.		

#	Description	Compliance (Y/N)	Remarks
11	The solution should report on services not in the expected state and optionally start or stop them.		
12	The solution should support the monitoring of processes & taking automated actions		
13	The solution should support monitoring new processes that come up on a server.		
14	The solution should support monitoring CPU performance over defined user defined time periods of time		
15	The solution should support monitoring Availability and performance of memory, including upper and lower thresholds and types of usage		
16	The solution should support monitoring Local and Attached Disk capacity and provide delta change in used capacity		
17	In Windows/UNIX/Linux environments the solution should support monitoring Alerts & Log Messages, including regular expression matching.		
18	In Windows/UNIX/Linux environments the solution should support monitoring Performance counters for IO		
19	In Windows/UNIX/Linux environments the solution should support monitoring Running services and in-progress jobs		
20	The solution must monitor the availability, health, and performance of Distributed File Services namespace and replication.		
21	The solution should monitor uptime/ downtime of servers		
22	The Solution should support monitoring new processes that come up on a server		
Network Monitoring System			

#	Description	Compliance (Y/N)	Remarks
1	The Solution should provide capability to monitor any device based on SNMP v1, v2c & 3		
2	The Solution should monitor bandwidth utilization.		
3	The solution should monitor utilization based on bandwidth.		
4	The Solution must be capable of monitoring the availability, health, and performance of core networking devices including but not limited to CPU, memory, temperature.		
5	The Solution should have the ability to issues pings to check on availability of ports, devices.		
6	The Ping Monitoring should also support collection of packet loss, Latency and Jitters during ICMP Ping Checks		
7	The Port Check for IP Services monitoring should also provide mechanism to define new services and ability to send custom commands during port check mechanism.		
8	The Solution should have the ability to receive SNMP traps and syslog.		
9	The Solution should automatically collect and store historical data so users can view and understand network performance trends.		
10	The solution should be capable of monitoring network delay/latency.		
11	The solution should be capable of monitoring delay variation		
12	The solution should be capable of monitoring packet loss, Packet QOS, Packet Errors on one or more ports		
13	The solution should allow users to access network availability and performance reports via the web or have those delivered via e-mail.		

#	Description	Compliance (Y/N)	Remarks
14	The solution should support auto-discovery of network devices		
15	The solution should have the ability to schedule regular rediscovery of subnets.		
16	The solution should provide the ability to visually represent LAN/WAN links) with displays of related real-time performance data including utilizations.		
17	The system should provide discovery of heterogeneous physical network devices like Layer-2 & Layer-3 switches, Routers and other IP devices and do mapping of LAN & WAN connectivity.		
18	The solution should provide capability to mask the default port speed for accurate % port utilization reporting		
19	The System shall support monitoring of Syslog		
20	The solution should provide capability to add an IP device or IP Range or IP subnet with functionality supporting multiple SNMP strings.		
21	The solution should provide capability to add devices from word or excel file by drag and drop functionality and auto configure based on pre-defined settings.		
22	The solution should allow easy configuration of polling frequency till per second scenario.		
Database Activity Monitoring			
1	The solution should monitor multiple database servers and multiple versions of each server including:		
1.1	Oracle / SQL Server / Informix / DB2 / Sybase / MySQL etc. including database proposed by MSP.		
2	The Solution should Provide SQL Response Time for Monitoring Custom Queries		

#	Description	Compliance (Y/N)	Remarks
3	The Solution should provide response time Monitoring for custom queries through JDBC Mechanism to allow monitoring unsupported databases		
4	Database Space Monitoring for both file group and transaction log (Warning threshold, Critical threshold as well as file group/log full)		
5	Performance monitoring - capture of DB Engine related performance counters as well as threshold alerting		
6	The solution must support SQL Agent monitoring - failed jobs, long running jobs		
7	The solution must support Database Health and Settings - Check database status (offline, suspect), Check database options (auto grow, auto shrink, auto close etc.)		
8	The solution must support monitoring of Replication, DB Mirroring and Log shipping if applicable		
9	The solution must be able to report & check for last recent Full database backup and last recent Transaction Log backup		
10	The solution must monitor for Blocking (exceeding duration) and Deadlocks		
11	The solution must be able to run power shell, VBScript, cmd and VBScripts to perform tests on the database and have the results put into the solution as performance data and or alarms		
12	Inclusion of SQL statements within the Solution should be a standard “easy-to-use” function achieved without programmatic intervention.		
13	The solution should support auto-discovery of database instances.		

#	Description	Compliance (Y/N)	Remarks
14	The solution should support the creation and management of reusable test templates that contain a specific pre-defined set of database checkpoints/measurements.		
15	The solution should support the use of schedules and time filters for database monitoring.		
Virtualization Monitoring System			
1	The solution should provide support for leading virtualization platform like VMware, HyperV, Zen, IBM PowerVM, KVM etc.		
2	The solution should support monitoring of virtualized environment through management interface		
3	The solution should provide capability to monitor events generated by the hypervisor to generate alarms and alerting functionality		
4	The solution should provide capability to create monitoring template and auto configure any newly detected virtual machine.		
5	The solution should provide a configurable interface to view performance metrics related to virtualization infrastructure		
6	The solution should provide capability to monitor the availability to Web API's of application		
7	The proposed solution should be integrated with centralised monitoring tool to enable aggregation of alarms and alerts.		
8	The proposed solution should allow reporting through unified reporting console along with other infrastructure devices being monitored.		
Storage Monitoring System			
1	The proposed solution should be able to monitor leading enterprise storages through standard interfaces		

#	Description	Compliance (Y/N)	Remarks
2	The proposed solution should be able to monitor In depth metrics and performance data for supported storage platforms		
3	The proposed solution should automatically discovers storage configuration and auto-applies monitoring by template		
4	The proposed tool should be able to monitor other storage devices through SNMP		

3.4.2.10 SLA Monitoring System

#	Description	Compliance (Y/N)	Remarks
1	**General:** The solution most support Service Level Agreements Lifecycle Management including Version Control, Status Control, Effectively and audit Trail.		
2	**General:** The solution must provide a flexible framework for collecting and managing service level templates including Service Definition, Service Level Metrics, Penalties and other performance indicators.		
3	**Service Delivery:** The solution must have the ability to define and calculate key performance indicators from an End to End Business Service delivery perspective.		
4	**Contract Management:** The solution must support dependencies between supplier contracts and internal or external contracts.		
5	**Bonus & Penalty:** Support for Defining and Calculating service Credit and Penalty based on clauses in SLAs. Support for Defining and Calculating service Bonuses based on clauses in SLAs		

#	Description	Compliance (Y/N)	Remarks
6	**Alerts:** The solution must support delivery mechanisms to indicate/notify whether SLA targets are being achieved or violated.		
7	**Business Impact Analysis:** The solution must make it possible to find the underlying events that cause the service level contract to fail.		
8	**Dynamic Calculations:** The solution supports dynamic service level targets to reflect obligations importance and priority over time.		
9	**Audit Trails:** Full electronic audit trails available for both system and user transactions.		
10	**Reporting:** Report module and SLA Management module must be integrated to provide ease-of reports configuration and execution.		
11	**ITIL**: The solution supports ITIL standards.		

3.4.2.11 IT Service Management

#	Description	Compliance (Y/N)	Remarks
1	The proposed helpdesk solution must provide flexibility of logging, viewing, updating and closing incident manually via web interface.		
2	The web interface console would also offer power-users tips.		
3	The proposed helpdesk solution must provide seamless integration to log incident automatically via system and network management.		
4	The proposed helpdesk solution must provide classification to differentiate the incident via multiple levels/tiers of		

#	Description	Compliance (Y/N)	Remarks
	categorization, priority levels, severity levels and impact levels.		
5	The proposed helpdesk solution must be able to provide flexibility of incident assignment based on the workload, category, location etc.		
6	Each escalation policy must allow easy definition on multiple escalation levels and notification to different personnel via window GUI/console with no programming.		
7	The escalation policy would allow flexibility of associating with different criteria like device/asset/system, category of incident, priority level, organization and contact.		
8	The proposed helpdesk solution must provide web-based knowledge database to store useful history incident resolution.		
9	The proposed helpdesk solution must contain built-in knowledge tools system that can provide grouping access on different security knowledge articles for different group of users.		
10	The proposed helpdesk solution must have a strong Business Objects based reporting module built in it.		
11	The proposed helpdesk solution must integrate with EMS event management and support automatic problem registration, based on predefined policies		
12	The proposed helpdesk solution must be able to log and escalate user interactions and requests.		
13	The proposed helpdesk solution must provide status of registered calls to end-users over email and through web.		
14	The proposed helpdesk solution must have an updateable knowledge base for technical analysis and further help end-users to search solutions for previously solved issues.		

#	Description	Compliance (Y/N)	Remarks
15	The proposed helpdesk solution must have the ability to track work history of calls to facilitate troubleshooting.		
16	The proposed helpdesk solution must support tracking of SLA (service level agreements) for call requests within the help desk through service types.		
17	The proposed helpdesk solution must support request management, problem management, configuration management and change order management.		
18	The proposed helpdesk solution must be capable of assigning call requests to technical staff manually as well as automatically based on predefined rules, and should support notification and escalation over email, web etc.		
19	Knowledge tools and Configuration Management Data Base (CMDB) should be integral built-in components of Helpdesk and should be accessible from the same login window to enable seamless access.		
20	The proposed helpdesk solution must allow the IT team to see the Configuration Items (CI) relationships in pictorial format, with a specified number of relationships on single window.		
21	Workflow must provide the ability of being Non-linear workflow with decision-based branching and the ability to perform parallel processing. It should also have a graphical workflow designer with drag & drop feature for workflow creation and updation		
22	The proposed helpdesk solution must have an integrated CMDB for better configuration management & change management process. CMDB should have be able to scale as per the requirements of the project for creation of CI families, CI Classes and CI Relationship Types out of the box. Both helpdesk & CMDB should have same login window for seamless access.		

#	Description	Compliance (Y/N)	Remarks
23	The proposed helpdesk solution must have a top management dashboard for viewing the helpdesk KPI in graph & chart formats.		
24	The proposed helpdesk solution must support remote management for end-user & allow analysts to do the desktop sharing for any system located anywhere, just connected to internet.		
25	Remote desktop sharing / integrated		
	Helpdesk tool should be out-of-the-box, agent-less & all activities should be automatically logged into the helpdesk ticket.		
26	The proposed helpdesk solution must allow IT teams to create solution & make them available on the end – user login window for the most common requests.		

3.4.2.12 Project Management Tool

#	Description	Compliance (Y/N)	Remarks
1	**Dashboards:** The dashboards should provide a quick and complete view on every aspect of the project, in a form that is easy to grasp and understand. It should be available on a real time basis and allow for customizations to create different dashboards for different stakeholders based on the provided input parameters		
2	**Gantt chart:** A Gantt chart or any related tool for visual interpretation of the milestones, dates and activities for the project is needed. The Gantt chart or related tool should be able to add tasks to people and monitor the status of each project task. The tool should also be able to add the dependencies for each task to be initiated i.e. a task can only start if a particular task is completed		

#	Description	Compliance (Y/N)	Remarks
3	**Project scheduling:** A Project Management tool should also be able to Schedule the tasks as required by the concerned officials, which can be updated as required and can be viewed by each team member. The project schedule should allow not just managing team schedules, but also team workloads		
4	**Project reporting:** The tool should be able to create a report on every project feature which can be customized to provide the data as required. The reporting should allow to track planned and actual progress of the different ongoing activities in place. The reports should be able to download in CSV, Excel, PDF and other common formats		
5	**Project & task tracking:** This can be used to track the tasks so that officials can ensure the tasks are completed on time. The tasks can also be collaborated and shared to the respective task owners.		
6	**Defect logging and tracking:** The tool may have a built-in defect logging and tracking module capable of tracking the defects from different stages of testing i.e. unit testing / integration testing etc., should be capable of capturing priorities/ impact (critical / major/ minor). This module should also be capable of generating MIS reports		
7	SI shall propose infrastructure requirement as part of the proposal, if it is an on-premises solution or it can be a cloud-based tool		
8	SI shall propose role-based license requirements for the Development team. In addition to these, 20 officials need to be given full access. All officials should be able to generate reports. No named licenses to be issued, access can be rotated between any users		
9	The tool should be supported by a mobile application		

3.4.2.13 Container Orchestration Platform

#	Description	Compliance (Y/N)	Remarks
1	Provision and deploy a Kubernetes based container platform solution to host Business applications. SI shall provide the required support for deployment of applications on the container platform.		
2	Deploy most up-to-date, stable and enterprise ready release with relevant tools and should allow workloads to be moved between environments like Dev , testing , Pre-Prod Prod etc.		
3	Manage end to end security and monitoring for containerized platform deployed by the SI.		
4	Should integrate with LDAP/AD for user authentication and role management.		
5	Should integrate with LDAP/AD for user authentication and role management.		
6	Should allow creation of a customized cluster in a single click and also allow both vertical and horizontal scaling of a cluster.		
7	Deploy container orchestration solution as Kubernetes cluster deployment service. It should include operational tasks to increase and decrease worker nodes in existing Kubernetes cluster		
8	Do patch updates and upgrades of Kubernetes cluster version without taking application downtime		
9	Setup multiple Kubernetes clusters for different environments i.e. Production /Dev/Test as per the requirement. Each cluster should support multi-tenancy and would have multiple tenant applications.		
10	Deploy Operations Management tool to monitor complete Kubernetes objects like Namespaces, Clusters, Replica Sets, Nodes, Pods, and Containers and ensure continuity and responsiveness of the application services by recreating failed / unresponsive nodes. Tool should help in		

#	Description	Compliance (Y/N)	Remarks
	troubleshooting by highlighting any performance issues and send alerts for the objects that are monitored.		
11	Implement in-depth analytics for the North-South traffic flows including latency/end-to-end timing analysis of flows, application performance monitoring, client and log analytics and dynamic health scoring		

3.4.2.14 Software Code Version Management System

#	Description	Compliance (Y/N)	Remarks
1	The tool must be able to Initialize or create a new and empty repository for each project. It should have Distributed repository model.		
2	The tool must support adding a file (import) to the main repository to begin managing version control		
3	The tool should have an Easy-to-understand naming convention and comprehensible naming convention.		
4	The tool must have a consistent mechanism for tracking and making changes, commits, synchronization, and merges		
5	The tool should have Smooth reversion, backup, and restoration capabilities		
6	The tool must record historical record of who, when, and what changes were made (viewing the differences in two files)		
7	The tool should support Concurrent file sharing with automated merge capabilities		
8	The tool should be able to identify conflicts for cooperative resolution		
9	The tool should be able to make improvements by branching individual work before merging files		

#	Description	Compliance (Y/N)	Remarks
10	The team should be able to revert to a previous state		
11	The tool should Provide unique revision with each commit		
12	The tool should trigger and deliver automated and regular updates to the team on changes		
13	It should have sandbox capability in order to test large changes before committing		
14	Short- and long-term undo or revert (in order to restore the last version in the event of a mistake)		
15	Check-in and Check-out		
16	Include a check-in message to notate changes		
17	Save changes and backup code consistently and frequently.		
18	Manage appropriate controls to allow proper, productive access.		
19	Ensure developers can easily pull up necessary documents		
20	Define team, individual, and read-only access to streamline document availability and allow users to perform their functions in a timely manner		
21	Support Agile teams with the ability to work simultaneously toward the overall team goals and timeline in order to quickly move a project towards success and maintain the goal of Agile development.		

3.4.2.15 Performance Testing Tool

S. No.	Description	Compliance (Y/N)	Remarks
1	The testing tool should integrate with agile and DevOps tools, making it easy to combine with continuous integration and continuous development frameworks such as Jenkins, Maven to name a few of these tools.		
2	It should also support the shift-left testing by enabling shortening of the build and test cycles, thus helping to save testing time.		
3	The testing tool should support recording communication between two tiers of the system and should efficiently playback the automatically created script.		
4	The tool should also support along with HTTP, other important and common protocols.		
5	Sometimes, load testing is reduced to pre-production testing using protocol-level record/playback as the main feature.		
6	There are certain applications where recording cannot be done, in such cases, API calls from the script may be an effective option. Thus, the usage of API testing scripts and web services scripting should be supported by the load tools taken into consideration.		
7	The tool should support testing of all kinds of mobile apps such as Native, Hybrid, Web and Secure applications.		
8	The tool should automate functional tests simulating user actions with the automated record and playback options		
9	Tools should have a built-in ability to manage test execution and enable test data to be made available.		
10	Load tools should support coordination between virtual users with respect to synchronization points, protocols, and varied network connections.		

S. No.	Description	Compliance (Y/N)	Remarks
11	The tool should be able to support with respect to scaling of users and handle large volumes of information		
12	The testing tool should support new technologies and integrate easily with DevOps CI/CD and other platforms within the existing testing ecosystem.		
13	The tool should be able support distributed testing and load scheme customization to simulate the actual fluctuations of peak load and drops.		
14	The tool should be able to capture the key metrics such as detected defects, response times, the number of requests, metrics from a database, and other system components to define the overall performance level and design fit-for-purpose improvements.		
15	The testing tool should be easily integrable with the enterprise monitoring tools to capture the performance of the application system resources with the variation in loads		

3.4.3 Security

The following list of security solutions provides a summary of the solutions to be procured and deployed for the SL-UDI program. The detailed specifications are provided below**.**

Note: As a policy decision, no data from the SL-UDI program shall go on the cloud for any purpose whatsoever. All security solutions below shall be deployed locally in the data centers of SL-UDI and no data shall go on the cloud.

Note: Vendor is free to quote individual / stand-alone solution or an integrated solution (with multiple security solutions in a box) that meets the stated requirements

3.4.3.1 Data Leak Prevention (DLP) with High Availability

#	Description	Compliance (Y/N)	Remarks
1	The agent should monitor content traversing across the endpoint by I/O channel (USB, bus, Bluetooth, LPT, etc.) and Application Access.		

#	Description	Compliance (Y/N)	Remarks
2	The solution should notify the end user of a policy violation using a customizable pop-up message and should capture content that violates a policy and store it in an evidence repository.		
3	The solution should be able to enforce policies while the endpoint system is disconnected from the network and the endpoint agent should log all violations and reports into the central database when a connection to the network is established.		
4	The solution should be able to Identify mass storage device by vendor specific identification numbers.		
5	The solution should be able to Identify content using regular expressions, key words, hash functions and pattern matching.		
6	The solution should be able to Identify content based on location and allow creation of policies based on Users and Groups.		
7	The solution should support the deployment of agents using the Central Management Console or common software deployment methods for management.		
8	The agent should protect itself from unauthorized removal or configuration change or service stoppage.		
9	The solution should have an option to Encrypt / Quarantine / Monitor / Delete sensitive files found during discovery.		
10	Solution should have Ability to exclude by application process name in removable storage device rules		
11	Solution should support device control for endpoints		
12	The solution should allow encryption using strong algorithms as per industry best practices of the complete hard drive sector by sector.		

#	Description	Compliance (Y/N)	Remarks
13	The solution should support encryption of extended partitions. The configuration for full disk encryption is controlled from the management console by selecting the drive letter that you intend to encrypt regardless of the partition type.		
14	The solution should record the encryption status of each hard drive		
15	The solution should support the encryption of removable media. (CD/DVDs, flash drives, external hard drives, etc.)		
16	The solution should be able to inspect HTTP traffic and HTTPs traffic		
17	The solution should be able to prevent content getting posted or uploaded to specific geo-destinations.		
18	The solution should be able to enforce policies by URLs, domains, or URL categories either natively or by integrating with a Web Security solution		
19	The solution should be able to monitor FTP traffic.		
20	The solution should have achieved at least EAL 2. The solution should be FIPS 140-2 Compliant.		
21	The solution should support the recovery of the password for a remote user.		
22	The solution should integrate with the proposed SIEM solution.		
23	The communication between all components of the Solution should be encrypted.		
24	The solution should integrate with the proposed LDAP and PAM/PIM solution.		

#	Description	Compliance (Y/N)	Remarks
25	The proposed solution should be managed from a centralized management server used to manage the DLP solutions.		
26	The solution should support Per User or User Group Policy and Multilevel Administration Privilege.		
27	The solution should support backup of DLP rules and settings.		

3.4.3.2 Anti-Advanced Persistent Threat (APT) with High Availability

#	Description	Compliance (Y/N)	Remarks
1	The solution should support selective analysis of files which are deemed suspicious based on internal capability. Entire solution and all its components should be on-premises with no data including meta data leaving the buyers data centre		
2	Solution should have ability to capture all traffic including encrypted on perimeter, inspect and analyze all protocols, analyze all the files (pdf, doc, xls, xlsx, jpg, jpeg etc.) for embedded code and binary codes.		
3	The solution should support deep packet inspection of TLS/SSL encrypted traffic (including HTTPS) and provide a throughput of minimum 30Gbps		
4	The Sandbox solution must be able to work with network , endpoint security systems , email and web security systems.		
5	Direct integration with the existing/proposed IPS, Endpoint, SIEM, log management, next generation firewalls, etc.		
6	Full malware lifecycle analysis must be supported so as to fully capture and understand the behaviour of the malwares. need for security expertise to interpret reports. And must be able to support of analysis of file size of up to 100MB.		

#	Description	Compliance (Y/N)	Remarks
7	The solution should provide capability to identify new APT families and threat sources through global feeds and available knowledge sources.		
8	The solution may have capability to identify the payload information of APT including the origination and code information.		
9	The solution should provide detection, analysis and repair capability against APT and SSL based APT-based attacks. Solution should be able to intercept SSL traffic and capable to intercept major PKI encryption algorithms.		
10	Solution should be capable of integration with SIEM for logging, reporting, and correlation.		
11	Proposed solution should have inline blocking mode capability to support real time analysis with 100Gbps interface support		
12	The solution should be able to schedule reports and also provide the flexibility to generate on-demand reports like daily/weekly/monthly/ yearly/specific range (day and time) etc.		
13	The solution should provide detection and analysis capability against APT-based attacks on network, log and endpoint systems. Real time and Offline threats should be detectable and preventable.		
14	The solution should allow user to manually interact with the sample within the analysis environment while the analysis is taking place.		
15	~~The sandbox solution must Makes integration fast and easy with sandbox representational state transfer (REST) API & Provides integration for a number of third-party products, including gateways, proxies, and security information and event management (SIEM) platforms~~		

#	Description	Compliance (Y/N)	Remarks
	The solution should have capability for API based integration using REST/other transfer mechanisms with third-party products such as gateways, proxies, and SIEM platforms, etc…		
16	The solution should support secured (encrypted) backup of Anti APT rules and settings		
17	Solution should provide granular reporting with following details as minimum description, risk score of individual detections, pcap files, network activities, disk activities, process activities etc.		
	A video/image/PCAP/Equivalent of the malware analysis should be made and be able to have playback and download capability for further analysis. curity expertise to interpret reports.		
	The solution should be delivered as an appliance and supported directly by OEM to provide safe and highly secure on-premises static and dynamic malware analysis and maintain the integrity & confidentiality of data.		
	The solution must have a user interaction tool that provides a safe environment to dissect malware without the risk of infecting your network. Built into the appliance, analysts are able to interact with the sample while it is being analysed including opening applications, clicking through dialogue boxes, and even reboot this virtual machine if needed.		
	The solution should have capability to Analyse more than 800+ highly accurate and actionable advanced behavioural indicators.		
	The solution should have capability to automatically derives threat scores from proprietary analysis and algorithms that consider the confidence and severity of observed actions, historical data, frequency, and clustering indicators and samples. Prioritizes threats with confidence to reflect each sample's level of malicious behaviour. Improves the prioritization of threats, which enhances the efficiency and accuracy of malware analysts, incident responders, security engineering teams, and products that consume sandbox feeds.		

#	Description	Compliance (Y/N)	Remarks
	The solution should provide easy-to-integrate normalized feeds in a number of standardized formats – such as eg JavaScript Object Notation (JSON), Structured Threat Information Expression (STIX), and comma-separated values (CSV) - and as Snort rules		

3.4.3.3 Privileged Access Management (PAM) / Privileged Identity Management (PIM) with High Availability

#	escription	Compliance (Y/N)	Remarks
1	The proposed solution must be deployable on-premises.		
2	The proposed solution must support a manual installation method on the organizations standard O/S images.		
3	The proposed solution must support an automated installer on the organizations standard O/S images.		
4	The proposed solution must be hypervisor agnostic and not rely on physical or virtual appliances.		
5	The proposed solution cannot rely on non-standard or proprietary components such as non-commercially available databases or network protocols.		
6	Describe the proposed solutions full architecture stack for on-prem		
7	The proposed solution must include components to distribute workloads across an environment.		
8	The proposed solution shall define scale-out architecture of properties such that new hardware may be added as per requirement.		
9	Describe the proposed solutions high-availability architecture for on-prem		
10	Describe the proposed solutions disaster recovery features for on-prem		
11	The proposed solution must support a wizard driven upgrade process and be performed without vendors professional services.		
12	The proposed solution must support the following types of accounts for password changing out-of-the-box: • Active Directory (All Account) • Windows Local User & Administrative Accounts (2008 R2+)		

#	escription	Compliance (Y/N)	Remarks
	• Unix Local Users & Administrative Accounts (Any Distribution) • Network System Accounts (Cisco, Juniper, Blue Coat, Enterasys, etc.) • Hypervisors (Hyper-V, VMware, Xen, etc.) • Out-of-Band Management Systems (iDrac, HP iLO, etc.) SSH Keys & Dependencies w/ and w/o Passwords • Database Accounts (ODBC, MySQL, MS SQL, IBM, SAP, Oracle, PostgreSQL, etc.) • VMWare ESX/ESXi Accounts • LDAP Accounts (OpenLDAP, Oracle Directory Server EE, etc.)		
13	The proposed solution must support an easy to use and intuitive scripting framework which allows the application owners to extend credential management functions to internal personal without vendors professional services.		
14	The proposed solution must have a native integration with Active Directory and support LDAP(s).		
15	The proposed solution must integrate with Security Groups within the proposed directory services as a component of the role-based access control.		
16	The proposed solution's Directory Services Integration must allow for a configurable synchronization schedule to automate onboarding new users.		
17	The proposed solution must support Integrated Windows Authentication for access to the platform.		
18	The proposed solution must support Local authentication & Local role-based access control groups.		
19	The proposed solution must support any SAML 2.0 Identity Provider for Single Sign-on.		

#	escription	Compliance (Y/N)	Remarks
20	The proposed solution must support any RADIUS-based multi-factor authentication solution.		
21	The proposed solution must support out-of-the-box integrations with DUO, FIDO2, RADIUS, and any TOTP solution.		
22	The proposed solution must support IP Address whitelisting for access users.		
23	The proposed solution must support masking available login domains during the login process from the user.		
24	The proposed solution must support a custom informational banner at the login screen without CSS modifications.		
25	The proposed solution must be configurable to enforce HTTPS through HSTS.		
26	The proposed solution must support a single pane of glass for policy configuration across an entire deployment.		
27	The proposed solution's policy configuration must include the ability to configure password management settings, security settings, and location for workload assignment.		
28	The proposed solutions must support applying policies at an account level and/or folder level.		
29	The proposed solution must support the following security workflows: a. Justification for Access (user must submit a reason/comment before accessing) b. Access Approval -- single approval c. Access Approval -- multi-step approval. Please describe how this workflow is configured in your platform. d. Account Check Out & Check In (one-time password and exclusivity) e. Account Check Out with the ability to run uploaded scripts (PowerShell, SSH, SQL) during the Pre and Post Check Out process		

#	escription	Compliance (Y/N)	Remarks
30	The proposed solution's Check Out must support manual, forced, and an automatic time-based Check In process.		
31	The proposed solutions justification and approval workflows must support optionally validating case/tickets with an external ticketing system during the justification and approval process.		
32	The proposed solution must support custom ticket system integrations.		
33	The proposed solution must provide workflow and policy management for the request, provisioning and decommissioning of discovered and newly created service accounts.		
34	The proposed solution must include a tamper-proof, robust, audit of all activities within and against the platform.		
35	The proposed solution's audit must provide the who, what, where, and when of activity.		
36	The proposed solution must support forwarding logs to any SIEM platform.		
37	The proposed solution must support keystroke capturing for Linux, Unix, and Windows Operating Systems.		
38	The proposed solution must support the cross-searching of keystrokes and allow for export to a CSV file.		
39	The proposed solution must support reviewing the audit trail under a single pane of glass portal.		
40	Email notification for password access, password rotation, etc.		
41.	Email notification for Account Lockout		
42	Email notification for Forcing Access Approval on all accounts		
43	The proposed solution must provide all reporting functions within the single pane of glass portal without the need for external reporting platforms.		

#	escription	Compliance (Y/N)	Remarks
44	The proposed solution must include several pre-configured out-of-the-box reports.		
45	The proposed solution must allow for built-in reports to be customized directly from the single pane of glass interface without the need for vendor professional services.		
46	The proposed solution must provide the capability of generating custom reports directly from the single pane of glass interface without the need for vendor professional services.		
47	The proposed solution provides an audit trail for service account workflow and governance enforcement		
48	The proposed solution must support transparently connecting a user from the web portal to a target resource through RDP, SSH, or application.		
49	The proposed solution must support monitoring a session without notifying the connected user.		
50	The proposed solution must support sending a message to the connected user.		
51	The proposed solution must support terminating an active user session.		
52	The proposed solution must provide pre-configured applications for session launching (RDP, SSH, PowerShell, SSMS, etc.).		
53	The proposed solution must provide the ability to natively add custom application session launchers to be configured from the single pane of glass interface without the need for vendors professional services.		
54	The proposed solution must not require middleware applications such as Autofit, AutoHotkey, or other Windows GUI automation platforms to add custom application session launching.		
55	The proposed solution must support launching to sessions without disclosure of the password.		

#	escription	Compliance (Y/N)	Remarks
56	The proposed solution must support the automatic recording of sessions with and without notification to the user.		
57	The proposed solution must support capturing Windows application events during sessions.		
58	The proposed solution must support cross-searching for executed Windows processes, e.g., opening PowerShell, or MMC.		
59	The proposed solution must provide a method of aggregating the recording agents into logical collections.		
60	The proposed solution must provide a method of whitelisting commands issued to SSH-based resources.		
61	The proposed solution must support offloading recordings to a SAN, NAS, or other network shares while still being encrypted.		
62	The proposed solution must include an automated account discovery function.		
63	The proposed solution's account discovery function must allow for scheduling down to an hourly basis.		
64	The proposed solution's account discovery function must provide an easy to understand discovery results view to visualize accounts across the environment.		
65	The proposed solutions account discovery function must provide out-of-the-box support for Active Directory Accounts, Windows Accounts, Linux Accounts, Unix Accounts, Hypervisor Accounts.		
66	The proposed solution's account discovery function must support rules to automate onboarding of all discovered accounts.		
67	The proposed solution's account discovery function must be extensible to other platforms not supported out-of-the-box. Please describe in detail how your platform can meet this requirement.		

#	escription	Compliance (Y/N)	Remarks
68	The proposed solution's account discovery provides the ability to discover service accounts and enforce governance and ownership.		
69	The proposed solution must offer an extensive web services API with create, read, update, and delete functions.		
70	The proposed solution's web services API must support Integrated Windows Authentication and OAuth Authentication.		
71	The proposed solution's web services API must support IP address whitelisting.		
72	The proposed solution's web services API use must be auditable by the PAM platform.		
73	The proposed solution must offer SDK or programming libraries for inclusion within the source code of internally developed software.		
74	The proposed solution's SDK/libraries must support IP address whitelisting.		
75	The proposed solution's SDK/libraries must be auditable by the PAM platform.		
76	The proposed solution's SDK or CLI client must offer a configurable encrypted caching strategy.		
77	The proposed solution's SDK or CLI client audit must be accessible within the platform.		
78	The proposed solution's SDK, CLI client, or other API components must not be Java based.		
79	The proposed solution must have a direct integration with common vulnerability scanner solutions for offloading credentials required in authenticated scans.		
80	The proposed solution support out-of-the-box integration with common ticketing systems for use in workflow validations.		

#	escription	Compliance (Y/N)	Remarks
81	The proposed solution must protect data at rest.		
82	The proposed solution must protect data in transit.		
83	The proposed solution must provide a user audit report; allowing admins to visualize what accounts an offboarded individual touched.		
84	The proposed solution must provide an easy method to rotate the accounts disclosed in the user audit report mentioned previously.		
85	The proposed solution must support offloading the management of the master encryption key to Hardware Security Module.		
86	The proposed solution must offer a built-in scheduled backup function capable of saving to a SAN, NAS, or other network location.		
87	The proposed solution must support zero information disclosure error messages to prevent logs from displaying sensitive information.		
88	The proposed solution must support configuration to allow for non-standard ports.		
89	The proposed solution must support a customizable password complexity and rules policies engine		
90	The proposed solution must support allowing our standard organizational Group Policy Objects to be enforced on all components of the platform architecture.		
91	The proposed solution must support checking for known security breaches of sites whose logins are stored in the password manager, for which you haven't changed your password since the breach occurred.		
92	The solution must provide a single-pane of glass interface for all access and configurations for all functions, e.g., administration, auditing, reporting, vaulting, access policies, privileged sessions, discovery, and API.		

#	escription	Compliance (Y/N)	Remarks
93	The solution must not require browsers plugins (Flash, Java, etc.) for any function of accessing, initiating, reviewing, administration, or management .		
94	The proposed solution's user experience must be the same for all users but only be restricted by roles and permissions to streamline training and adoption.		
95	The proposed solution's administration and user experience must be intuitive.		
96	The proposed solution's account segregation should mimic a systems file system explorer to streamline training and adoption.		
97	The proposed solution's account segregation hierarchy must support an inheritance model for resources and policies.		
98	The solution should be able to manage and interact with multiple remote sessions for both Remote Desktop Protocol (RDP) and SSH in a unified environment.		
99	The solution should be able to manage multiple sessions active at once, using different connection protocols and a variety of privileged accounts.		
100	The solution should be able to launch and configure sessions across multiple environments with credentials automatically injected into sessions as needed.		
101	The solution should be able to provide an end to end record of privileged user access and provide a collaboration between teams to view live and send messages		
102	The solution should provide custom terminal banners after a successful login with available commands to be displayed.		
103	The solution should have the ability to start a terminal connection and launch using a single line and include 2FA for access.		
104	The solution should be able to utilize built in capabilities such as the up and down arrows for have command history.		

#	escription	Compliance (Y/N)	Remarks
105	The solution should not require more hardware or additional licensing for these terminal connection features.		
106	The proposed product should be able to seamlessly integrate with the existing solution and support all the Operating Systems including but not limited to Windows, Unix, Linux, Solaris, etc.		
107	The proposed solutions should be able to integrate with applications including but not limited to web applications, thick clients, etc.		
108	The proposed solutions should be able to integrate with security devices including but not limited to Firewall, IPS/IDS, etc.		
109	The proposed solutions should be able to integrate with network devices including but not limited to switches, routers, etc.		
110	The proposed solutions should be able to integrate with databases including but not limited to MySQL, Oracle, HBase, MSSQL, etc.		
111	The proposed solution should be agentless.		
112	The solutions should provide a single platform to access all the integrated devices		
113	The solution should have the capability to monitor session activities in real time and should maintain audit logs of the same		
114	The solutions should be capable of providing real time dashboard and reporting		
115	The solution should be common criteria compliant		
116	The solution should contain a password vault which should enable an administrator to define different password formation rules for target accounts on different target systems and supports the full character set including special characters that can be used for passwords on each target system.		
117	The solution should set unique random value anytime a password is changed.		

#	escription	Compliance (Y/N)	Remarks
118	The solutions should provide a single console for all administrative tasks		
119	The solution should be capable of user and group level access with multi-level administrative access		
120	The solution should restrict privileged activities on a windows server (e.g. host to host jumps, Power shell, cmd/telnet access, application access, tab restrictions etc.) from session initiated with PIM.		
121	The solution should be able to restrict usage of critical commands and/or tables for database access through SSH, Database Client utilities (TOAD, SQL developer) on any combination of target account, group or target system and end-user.		
122	The solution should have maker-checker control built-in for all administrative functions (password changes, system		
123	The solution can restrict target-account-specific entitlements of end users individually or by group or role.		
124	The solution can restrict end-user entitlements to target accounts by days and times of day.		
125	The solution must support parallel execution of password resets for multiple concurrent requests.		
126	The solution should provide fully automatic failover from a single active instance to a backup/standby instance with a fully replicated repository.		
127	The solution should automatically archive session recording data to external storage/ media based on time and available space.		
128	The solution should be scalable in terms of the system administrators, target systems and the concurrent session.		
129	The solution should be scalable in terms of the system administrators, target systems and the concurrent session.		

#	escription	Compliance (Y/N)	Remarks
130	The solution should integrate with the proposed Enterprise Management Solution.		

3.4.3.4 Two Factor Authentication with High Availability

#	Description	Compliance (Y/N)	Remarks
1	Two factor authentication tokens will be used to provide two layer of authentication for the departmental officers accessing SL-UDI's business application and should be software token based. It will be the bidder's responsibilities to work with different solution providers to deploy the solution and provide support for integration.		
2	The solution should cater to at least 200 departmental users.		
3	The solution should support authentication with password less authentication methods by using biometric authentication based on FIDO2 standards The proposed solution should not be cloud based.		
4	The solution must support integration with the existing infrastructure which acts as the presentation layer and the proposed/existing directory services		
5	The solution should cater to users accessing the departmental application through internal network and the users accessing the application through VPN		
6	The solution shall generate a one-time password for every access request with an expiry time configurable, that would synchronize with the proposed Authentication Server.		
7	Customer user directories from the existing directory should be synched with Authentication Server using a lightweight		

#	Description	Compliance (Y/N)	Remarks
	synchronization agent. All communication between this agent and the directory server should be encrypted.		
8	The solution must support a PASSCODE (combination of a 4 – 8 digit numeric/alphanumeric PIN and a pseudorandom token no.) using AES or 3DES or oAUTH or latest compliant algorithm		
9	The solution must have authentication support based on the current Universal Coordinated Time (UCT) and a supported time buffer.		
10	The solution must provide encrypted communication between the components including the primary and failover servers with the encryption key to change every few minutes.		
11	The solution must provide support to define access based on time of day, day of week or by group or user-defined access		
12	The solution must have provision available to write a custom query (SQL Statement) and generate the reports based on queries in .CSV, .HTML formats		
13	The solution should have inbuilt RADIUS Server		
15	Software token should be free and support multiple mobile devices.		
16	Should have support for customization like: User messages, token related (SMS or software) alerts etc.		
17	The solution should be a. Able to create and provision user accounts b. Provisioning manually via the management console c. Bulk importing of users via CSV file to the management console		

#	Description	Compliance (Y/N)	Remarks
	d. Automated synchronization against an identity repository.		
18	The solution should provide intelligent authentication by analysing log-in transactions and measuring risk by user and by device. Depending on the risk associated with a particular log- in transaction, solutions should have the capability to step up authentication using out-of-band or two-factor authentication techniques supported within the enterprise. The risk scores should take into account the following layers: The rules engine should establish rules from known fraud patterns that factor into the ultimate risk score of a particular log in. These rules should help to identify risky behavior as well as impossible log-in patterns. The rules must apply general policy around log-ins from forbidden countries or known risky IP/geo locations. The behavioral engine should store typical user behavior and must employ a heuristic engine to map subsequent log-ins against these known patterns of behavior. For each user, Intelligent Authentication should store patterns of behavior including OS, browser type, IP address, network, and geographic location to assess anomalies in a particular log-in event. The device engine should analyze the specific characteristics of the end user's device (PC, mobile or tablet) and must employ a heuristic engine to compare these characteristics on subsequent log-in transactions.		
19	The solution should integrate with the SIEM solution.		
20	The mobile applications should support provisioning using a QR code and it should not require a third party QR code scanner		

#	Description	Compliance (Y/N)	Remarks
	The proposed solution should provide a configurable lockout threshold for unsuccessful login attempts and the solution should support auto-lockout expiration for configurable time		
	The proposed solution should provide admins the ability to see which authentication devices are not protected with screen lock, including the option to view the list of users provisioned for those devices		

3.4.3.5 Web Gateway with High Availability

#	Description	Compliance (Y/N)	Remarks
1	Proposed Web Solution should be an on premise having Proxy, URL filter Caching, SSL Inspection, Anti-Virus, Antimalware, multiple detection engines.		
2	The solution should support different deployment modes.		
3	The solution must identify and block web pages with content including but not limited to: Malicious JavaScript / VB Script Malicious (or unauthorized) ActiveX applications Block Potentially Unwanted Programs (PUPs) Malicious Windows executable		
4	The Solution should integrate with SIEM, APT solution and the proposed/existing Ticket Management system for proactive detection and incident management.		
5	The solution must identify and block configurable search strings (like: porn, adult, hacking, download, shareware, etc.) and pattern.		
6	The solution should have gateway level Antivirus and malware protection.		

#	Description	Compliance (Y/N)	Remarks
7	The solution must provide file filtering for upload/download.		
8	The solution must support different types of compression algorithms and should be able to scan encoded and compressed files.		
9	The solution must have flexibility to monitor and block instant messaging (IM) based file transfer and other granular controls in applications granular controls in applications.		
10	The solution must be updated automatically with the new signatures from the web at customized user defined intervals.		
11	The solution must immediately block and alert the user if the content being downloaded/uploaded/accessed is found to contain virus/other malware over HTTP and HTTPS connections.		
12	The solution must be capable of dynamically blocking a legitimate website which has become infected and unblock the site when the threat has been removed.		
13	The solution should perform dynamic content inspection of web-based content being accessed from otherwise unblocked websites.		
14	The solution should provide creation of custom policies to be applied for specific user/s, IP's and group/s		
15	The solution should integrate with existing/proposed directory services.		
16	The solution should provide multiple administrator roles for configurable administrative functions.		
17	The Solution should have capability to provide detailed investigation reports including URL blocking summary, risk		

#	Description	Compliance (Y/N)	Remarks
	summary, application blocked summary and malware categories.		
18	All usage reports must be able to be run daily, weekly, monthly, or a configurable time span including previous day or previous seven days or previous month.		
19	The solution should have the capability to conduct web page analysis and restrict any malicious content (including images, videos etc.)		
20	The solution should be capable of detecting malicious activity in the network by a malware or other security threats.		
21	The solution should be able to detect encrypted and password protected files.		
22	The OEM should provide 24x7 technical support		
23	Solution should be capable of generating user access logs as well as activity logs.		
24	The solution should be able to integrate with the proposed Syslog and SIEM solutions.		
25	The solution should support Per User or User Group Policy and Multilevel Administration Privilege.		
26	The solution should support secured (encrypted) backup of Web Gateway rules and settings.		
27	Solution should enable Real Time Dynamic categorization that shall classify in real time in case the URL the user is visiting is not already under the pre-defined or custom categories database.		
28	The solution should support at least 2 industry known Anti Malware/Anti Virus engine that can scan HTTP, HTTPS and FTP etc. traffic for web based threats		

#	Description	Compliance (Y/N)	Remarks
29	The solution shall provide option to scan all ports at wire speed, detecting and blocking spyware activity trying to connect to the outside Internet. By tracking all 65,535 network ports and all protocols, the solution shall effectively mitigate malware that attempts to bypass HTTP and HTTPS etc.		
30	The solution should support following actions like allow, monitor, block, time-based access. Should also support displaying a warning page but allows the user to continue clicking a hypertext link in the warning page and creation of custom URL categories for allowing/blocking specific destinations as required by the		
31	The solution should allow administrator to define access to internet based on IP addresses, range of IP addresses, subnet and CIDR basis. It should also support to be forced for Authentication from Specific IP addresses, Subnet or CIDR's. The solution should be capable of blocking specific files downloads and based on size and per user group basis.		
32	Solution to maintain detailed proxy access logs that can be searched via filters, for easy location of any desired access of the user and to see how the product dealt with it.		
33	The solution should have facility to retain original source IP. When enabled, requests originating from a client should retain the client's source address and appear to originate from the client instead of the appliance.		
34	The policy editor must allow customisation the blocking page for each policy entry. The customisation must include the ability to define a custom message, insert a custom logo, or an administrator email address. The policy editor must allow to define a different blocking page for each identity and category of events (for instance a blocking page for security-related events, a blocking page for web filtering blocks, etc.)		

3.4.3.6 Code Review Tool

#	Description	Compliance (Y/N)	Remarks
1	Perform static and dynamic source code review of the application to identify security vulnerabilities.		
2	Review cross platform application developed in languages such as JAVA, ASP.Net, PHP, etc.		
3	Able to provide details of issues to file name and line number for precise identification of the issue.		
4	Able to track vulnerable function or variable throughout the source code.		
5	Able to identify vulnerabilities such as but not limited to OWASP Top 10, SANS 25, Buffer overflow, dangerous functions.		
6	Able to perform analysis of open source code modules used.		
7	Provide feature to validate the results and identify false positives.		
8	Provide recommendations and work around for the fix.		
9	Provide detailed reports as spreadsheet, PDF and HTML format, customizable as per the requirement and comparable to previous assessment.		
10	Should support periodic vendor updates for patches and attack signatures.		

3.4.3.7 Virtual Desktop Infrastructure (VDI)

#	Description	Compliance (Y/N)	Remarks
1	The Virtual Desktop Infrastructure (VDI) should cater to the following clients at the minimum – a. Desktops b. Laptops c. Tablets		

#	Description	Compliance (Y/N)	Remarks
2	Virtual Desktop Infrastructure (VDI) must have native clients for Windows 8, Windows 10, Macintosh, Linux, Chrome OS, Blackberry OS, IOS, Android and HP WebOS		
3	The solution should cater to users both on the intranet (LAN or WAN) as well as the internet.		
4	The solution should seamlessly scale up or down as per requirement with no/ minimal downtime for existing users.		
5	The solution should include a backup proposal with suitable hardware, licenses, implementation and support for the entire contract period. for VDI infrastructure.		
6	The solution should include the proposal for the best diskless thin client for the solution.		
7	The solution should ensure that mundane tasks related to creating / modifying / deleting of developer VMs should be with minimal administrative efforts.		
8	The solution should have Single / Minimum base images for all delivery methods of Virtual Desktops such as Full VM / Persistent and Non-Persistent VM/ Offline access VM etc.		
9	The solution should be capable of efficiently handling Planned or Unplanned down times with facility to handle Peak / Low workloads		
10	The solution should integrate and work with Backup solutions, Anti-virus solutions, Storage solutions, Network and Security solutions, SIEM Solution, PAM/PIM solution, IDAM solution, etc. and not deprive functionality benefits offered for Virtual Desktop Infrastructure.		
11	The solution should target efficient handling of resources like CPU, Memory, Storage IOPS, Network IOPS for Critical/ Non-Critical and Resource Hungry workloads and guarantee resources.		

#	Description	Compliance (Y/N)	Remarks
12	The solution should eliminate boot storm when all the users log in virtual desktops.		
13	The solution should offer security functions within and across Physical servers and Network components.		
14	The solution should not include network equipment like Load Balancer / WAN Optimizer.		
15	The solution should include the proposal of suitable hardware to meet the requirements to cater to 200 concurrent / named users.		
16	Hardware should be compatible with proposed VDI.		
17	Hardware proposed should ensure performance and availability to all 200 users.		
18	Hardware should be sized for a maximum of 300 users.		
19	Proposed hardware solution should have a blade center in both locations with FS SAN connectivity and High availability for VDI.		
20	Proposed solution should be able to add more blade servers to expand up to 300 concurrent / named users.		
21	Proposed solution should have SAN with FC connectivity and SAN switch with redundancy.		
22	Proposed SAN should have a minimum storage of 5TB (assuming 40 active sessions using 128 GB each) usable capacity with RAID 5 on each location and can have capacity to expand up to 50TB storage with RAID 5 on both the locations.		
23	Proposed SAN should have site to site replication capability.		

#	Description	Compliance (Y/N)	Remarks
24	Proposed solution should have to use existing network infrastructure in the organization.		
25	Proposed hardware should be able to support IPv4 and IPv6.		
26	The solution must include the supply of 200 concurrent / named user licenses to access desktop OS VM instances for scoped users.		
27	The solution must include a proposal for the software for the virtualization clients, backup and MS office.		
28	The software supplied should ensure that SL-UDI team has the rights to receive product updates and upgrades as they are released at no additional charge.		

3.4.3.8 Identity and Access Management (IDAM) with HA

#	Description	Compliance (Y/N)	Remarks
1	Solution should provide Single Sign-On solutions present in SL-UDI infrastructure including but not limited to applications developed in-house on platforms such as JAVA, Microsoft .Net, PHP, HTML5/JS, etc. The solution offered should not be restricted to above mentioned technologies. It should be possible to integrate the solution with the developments in other technologies.		
2	LDAPv3 compliant		
3	High Availability [no single point of failure]		
4	Scalability: Scalability to store minimum 1000 user records		
5	Replication across Multiple Nodes		
6	Multi-master replication: N-way multi-master replication for high-availability and disaster recovery		

#	Description	Compliance (Y/N)	Remarks
7	Schema management: Support creation of custom object classes and attributes to define entries specific to our needs		
8	Backup and restore: Support for online backup and restore		
9	Advance Security: Support for SSL/TLS		
10	IPv6 support for client access: Support for incoming connections from IPv6 clients		
11	Support for 64 bit Architecture		
12	Encryption: Supports different encryption methods of selected attributes		
13	Synchronization: Supports Synchronization of user data with other directory servers		
14	Monitoring: Support for SNMP protocol for real time monitoring		
15	Supports security policies to enforce rules related to password complexity, expiry, length etc.		
16	Logging and tracing of all operations performed. Provide report on who, what, when, and where the action was performed		
17	Developer Support		
18	RESTful API for self-service functionality e.g. user and password management		
19	Easy to Use GUI tools for administrators		
20	Should integrate with SIEM		
21	Password Authentication		
22	Risk Based Authentication		

#	Description	Compliance (Y/N)	Remarks
23	Windows Integrated Authentication		
24	Token or OTP (One Time Password) based authentication for multifactor. The token or OTP will be sent using SMS/Email or any other method		
25	Easily configurable 2-Factor authentication to choose the OTP sending mechanism		
26	Support for third party authentication service		
27	The solution should offer facility to include CAPTCHA functionality		
28	The solution should provide easy customization of UI to end user		
29	User access log should be maintained		
30	The Product must support Open Standards like SAML 2,		
31	Auth 2, OpenID Connect, WS-Security and WS Federation		
32	The Product must support Implementation of SAML 2 Identity Provider and SAML 2 Service Provider for authentications based on SAML2		
33	The Product must support Implementation of oAuth2 Authorization Server and Resource Server for authentications based on oAuth2		
34	The product should support secured communication between different components using SSL		
35	The Solution should support global idle session timeout, session timeout for idle sessions and single log-out		
36	Support for SSO to legacy applications		

#	Description	Compliance (Y/N)	Remarks
37	User ID Creation/Modification/Deletion: Creation and Modification of Users data manually or automatically based on event and/or workflow or script		
38	User ID Lock/Unlock based on event: Locking and Unlocking of Users manually or automatically based on event or workflow		
39	Mass Locking / Unlocking users		
40	Person/System user ID Support: user ids of person and system		
41	De-Duplication of user ids: duplicate user-ids should not be allowed		
42	User ID Merging: ability to merge identities in cases where multiple identities are created for a single person		
43	Delegated User Administration: allows user management to be distributed to users other than administrators, including providing multiple granular levels of identity administration permissions		
44	Delegation of Authority: allows users to assign a delegate while away from the office for example, while on vacation		
45	User ID Synchronization: synchronizes User Ids from IDAM system to and from other User ID stores		
46	User ID provisioning and de-provisioning based on event: provisioning and de-provisioning of users based on events such as approval and updating of all dependent target stores		
47	Notification/Alerts: the solution should facilitate administrator to configure real time alerts for events like configuration modification, intruder attack, fatal events etc.		
48	Group Management: allows creation/deletion of groups and addition/deletion of group members		

#	Description	Compliance (Y/N)	Remarks
49	Delegated Group Management: allows group creation, deletion and management to be performed by identified users based on authority delegation by administrators		
50	Nested Groups: allows groups to be members of groups.		
51	Dynamic Groups: supports addition/deletion of users to group dynamically based on rules or set of rules		
52	Password Policies: uses policies to enforce rules related to password complexity, expiry, length, password aging, password composition, password history enforcement etc.		
53	Password synchronization: synchronization of Passwords across managed systems		
54	Administrative password resets: allows a delegated administrator or helpdesk staff member to reset a password for an end-user		
55	Role lifecycle management based on Approval: supports creation/updation/ deletion/assignment/de-assignment of roles based on requests and / or workflow		
56	Reporting: who is assigned what roles and vice versa at any point of time		
57	Mass operation: supports mass assignment, de-assignment of roles		
58	Provide APIs for integration of Legacy Applications		
59	RESTFUL API: support for authentication, authorization, and identity services from web applications or native mobile applications using REST Clients		

#	Description	Compliance (Y/N)	Remarks
60	Solution should have activity trail of the following: a. Sign-on, Sign-off b. User: create, update, delete or disable accounts c. Role: create, update, delete or disable roles d. Password changes, resets, challenge response questions changes e. Synchronization events		

3.4.3.9 Hardware Security Module (HSM) with High Availability

#	Description	Compliance (Y/N)	Remarks
1	The solution should support Operating Systems including but not limited to Linux, Windows, Solaris, HP-UX, etc.		
2	The solution should be appliance based.		
3	The solution should support TCP/IP Network based appliance- Gigabit Ethernet connectivity with multiple Ethernet interfaces.		
4	The solution should comply to standards - UL, CE, FCC part 15 class B, RoHS2, WEEE.		
5	The solution should be compliant with FIPS 140-2 Level-3 or higher.		
6	The solution should support the standard algorithms as per the CCA Guidelines.		
7	Hash/message digest: Minimum SHA-2 family		
8	Cryptographic Symmetric: AES, 3 DES (2 Key and 3 Key)		
9	Cryptographic algorithms: Diffie-Hellman, RSA (2048-8192 bit), DSA (1024-3072).		

#	Description	Compliance (Y/N)	Remarks
10	Cryptography ECC: Full Suite implementation with fully licensed Elliptic Curve Cryptography (ECC), ECDSA and ECDH.		
11	Published API for various above functionalities for integrating with the Application software.		
12	Signing performance: Preferably at least 10000/sec for 2048-bit RSA keys.		
13	The solution should also support automatic synchronization of keys between HSM Systems.		
14	The solution should support minimum 30 unique logical partitions with each partition supporting minimum 50 keys of 2048 length		
15	Possibility to share keys between HSMs in different operating locations to enable load sharing and hardware fault tolerance.		
16	The remote administration of the HSM devices should be possible.		
17	Creation of multiple security domains should be possible.		
18	Should support NTP for time synchronization.		
19	The HSM should be able to log all the administrative activities, usage and application operations and should be able to integrate with the Syslog server and SIEM solution		
20	Should support SNMP.		
21	HSM should be capable of overall key management (creation, access, archival, destruction).		
22	The solution should support Per User or User Group Policy and Multilevel Administration Privilege.		

#	Description	Compliance (Y/N)	Remarks
23	The solution should support secured backup of HSM rules and settings on HSM docks.		

3.4.3.10 Anti-Distributed Denial of Service (DDoS) with High Availability

#	Description	Compliance (Y/N)	Remarks
1	DDoS solution should be a dedicated hardware appliance and not a licensed feature on Firewall or Load Balancer Appliance.		
2	Should have 4X10Gbps and 4X 40 Gbps SFP Interfaces. Interfaces should be populated with multi-mode fiber transceiver modules.		
3	System should have scalable inspection throughput of 5 Gbps scalable to 10 Gbps without additional hardware.		
4	Present license should be for 1 Gbps throughput.		
5	Should support latency less than <75 microseconds and should be clearly documented in the data sheet.		
6	SSL attack prevention Module/appliance System should Mitigate encrypted attacks and should have 4000 SSL CPS/TPS (1TPS = 1 CPS) with 2048 bit Key.		
7	In inline mode system must not modify MAC or IP addresses of passed frames.		
8	System should be designed with High availability		
9	The solution should support at least 2 million packets per second on each box from day 1.		
10	System should support Multiple Segment protection minimum of 6 Segments.		
11	System should support, In-Line, Out-of-Path deployments modes.		

#	Description	Compliance (Y/N)	Remarks
12	System should support following environments: a. Symmetric b. Asymmetric Ingress		
13	Solution should be transparent to control protocol like MPLS and 802.1 Q tagged VLAN environment. Also, it should be transparent to L2TP, GRE, IPinIP traffic.		
14	The system should be transparent to 'logical link bundle' protocols like LACP.		
15	Solution Should detect IPv6 Attacks		
16	Solution should mitigate IPv6 Attacks.		
17	The DDoS detection capability of the solution must not be impacted by asymmetric traffic routing.		
18	Should detect and Mitigate attacks at Layer 3 to Layer 7.		
19	Should support standard network maximum transmission unit (MTU).		
20	The system must allow protection parameters to be changed while a protection is running. Such change must not cause traffic interruption.		
21	System should Protect from multiple attack vectors on different layers at the same time with combination of Network, Application, and Server side attacks.		
22	Solution should provide protection for volumetric/Protocol and Application layer based DDoS attacks.		
23	Inspection and prevention is to be done in hardware.		
24	The system must have an updated threat feed that describes new malicious traffic (botnets, phishing, etc.).		

#	Description	Compliance (Y/N)	Remarks
25	The system should be capable to mitigate and detect both inbound and outbound traffic.		
26	Solution should provide real time Detection and protection from unknown Network DDOS attacks.		
27	System should have mitigation mechanism to protecting against zero-day DoS and DDoS attacks without manual intervention.		
28	System supports random, horizontal and vertical port scanning behavioural protection.		
29	System should support behavioral-based application-layer HTTP DDoS protection.		
30	System supports DNS application behavioural analysis DDoS protection.		
31	System must be able to detect and block SYN Flood attacks and should support different mechanisms. a. SYN Protection - Transparent Proxy/out of sequence b. SYN Protection - Safe Reset c. SYN Protection /TCP Reset.		
32	System must be able to detect and block HTTP GET Flood and should support mechanisms		
33	Should support following HTTP flood Mechanism: a. High Connection Rate b. High rate GET to page c. High rate POST to page		
34	System should detect and Mitigate different categories of Network Attacks: a. High rate SYN request overall b. High rate ACK		

#	Description	Compliance (Y/N)	Remarks
	c. High rate SYN-ACK d. Push Ack Flood e. Ping Flood f. Response/Reply/Unreachable Flood		
35	System should provide zero-day attack protection based on learning baseline / behavioural analysis of normal traffic; zero-day attacks are identified by deviation from normal behaviour.		
36	System provides behavioural-DoS protection using real-time signatures.		
37	System should Protect from Brute Force and dictionary attacks.		
38	System must be able to detect and block Zombie Floods.		
39	System must be able to detect and block ICMP, DNS Floods.		
40	Should support IP defragmentation, TCP stream reassembly.		
41	The system must be able to block invalid packets including checks for: Malformed IP Header, Incomplete Fragment, Bad IP Checksum, Duplicate Fragment, Fragment Too Long, Short Packet, Short TCP Packet, Short UDP Packet, Short ICMP Packet, Bad TCP / UDP Checksum, Invalid TCP Flags, Invalid ACK Number) and provide statistics for the packets dropped		
42	Should detect and Mitigate from Low/Slow scanning attacks.		
43	Should detect and mitigate from Proxy and volumetric Scanning.		

#	Description	Compliance (Y/N)	Remarks
44	System Should support dedicated DNS protection from DDoS.		
45	System should support suspension of traffic/ blacklisting from offending source-based on a signature/attack detection.		
46	System should support user customizable and definable filters.		
47	System should support anti-evasion mechanisms.		
48	System should have capability to allow custom signature creation.		
49	System protects from DDoS attacks behind a CDN by surgically blocking the real source IP address.		
50	Protection Against Encrypted Attacks		
51	System should have out-of-path / on device SSL inspection		
52	Proposed Solution should Protect against SSL and TLS-encrypted Attacks with a separate SSL Decryption module on device / out of Path.		
53	Proposed Solution should detect SSL encrypted attacks at Key size 1K and 2K without any hardware changes.		
54	High Detection and Mitigation Accuracy		
55	System supports Challenge-response (Layers 4 to 7) mechanisms without Scripts.		
56	System supports HTTP Challenge Response authentication without Scripts.		
57	System supports DNS Challenge Response authentication: Passive Challenge, Active challenge.		

#	Description	Compliance (Y/N)	Remarks
58	System should have capability to integrate with SIEM solution.		
59	Should have ready API for SDN environment integration/ Anti- DDoS system for attack mitigation in custom portal.		
60	System should support SDN controller/Anti-DDoS system with a vision and strategy to support future SDN enabled network.		
61	The system must support configuration via standard up to date web browsers. System user interface must be based on HTML.		
62	System should support CLI access over console port and SSH.		
63	The system must have a dedicated management port for Out-of- Band management.		
64	Management interfaces must be separated from traffic interfaces. System management must not be possible on traffic interfaces, management interfaces must not switch traffic.		
65	System must have supporting of tools for central monitoring.		
66	Management certificate must be possible to change.		
67	Proposed solution should have centralized management system.		
68	The system must support the generation of PDF and e-mail reports.		
69	Integration with RADIUS and TACACS+ or PAM/PIM solution		

3.4.3.11 Security Information and Event Monitoring (SIEM) with High Availability

#	Description	Compliance (Y/N)	Remarks
1	The solution should offer a single view of all the data captured from devices across all sites and the SIEM solution should be consistent in Gartner's Leaders Quadrant across last 5 years (2019-2024)		
2	The proposed solution must include Next Gen SIEM having features such assecurity Analytics, Big Data Analytics with necessary automation capabilities. To avoid maintaining multiple data repositories, proposed solution should have central data repository which should act as common data lake for SIEM, UEBA & SBDL		
3	The proposed solution must be able to support at least 8 out the following indicative list: Network: HTTP/HTTPS Referrer, User Agent, Cookie, Header, Data, URL IP: Domain, Endpoint. File Hash, Name, Extension, Path and Size Registry Hive, banner grabbing, Path, Key Name, Value Name, Value Type, Value Text, Value Data Process Name, Arguments, Handle Name, Handle Type Service Name, Description Certificate: Certificate Alias, Serial, Issuer, Subject, Start Time, End Time, Version, Handshake Type, Public key Algorithm, Signature Algorithm. Email: Email Address, Subject Body.		
4	The proposed solution must be able to handle 30000 EPS / 800 GB of data /logs per day from day one. without dropping or queuing of logs as per the requirement. There should not be limitations on the number of devices		

#	Description	Compliance (Y/N)	Remarks
	like servers, network devices, virtual machines or any other data source(s) that is required to be integrated. Solution must be able to scale up to peak of 40000 EPS / 1 TB /day on few instances without any performance degrade or loss of data/logs should be provisioned from day one considering peak usage and surge.		
5	The solution should be able to collect the logs in an agent/ agentless manner and store the same in real-time to a central log database from any IP Device. The raw logs should be time stamped, compressed to optimize storage utilization.		
6	The solution should collect the entire log sent by the devices by guaranteeing chain of custody for regulatory compliance.		
7	In order to make these logs tamper proof, the solution must store events in compressed archives that are tamper proof encoded.		
8	The solution should allow filtering log data based on log message payload like source and destination IP, ports, usernames, workstation address, domain etc.		
9	The SIEM log collector component must store the data locally if communication with centralized data storage is unavailable.		
10	The proposed SIEM solution must be fully integrated with the central repository of logs data without the need to duplicate the collected raw logs and the searchable data is for 180 days (6 months)		
11	The solution should provide support for IPv6.		
12	Solution should be able to provide correlation of all the data sources which are integrated and should have facility to change/modify the source of correlation		
13	The solution should be able to perform different correlations (but not limited to): Rule based, Historical based, Heuristics		

#	Description	Compliance (Y/N)	Remarks
	based, Behavioral based, etc., across different devices and applications		
14	The proposed solution must come with out-of-the-box integration and dashboards, reports, rules etc... to provides rapid insights and operational visibility into, Windows, Unix and Linux environments machine data: syslog, metrics and configuration files.		
15	The solution must provide a field extraction wizard that is used to create parsers and allow testing and validation with existing live or historical data within the system from the web interface. Old data should be parsed with new parser without re-ingesting or re-indexing the data.		
16	SIEM solution should be able to receive and consume global threat feeds automatically and manually.		
17	The proposed solution must be able to capture both the logs and network flow information.		
18	The proposed SIEM solution should include all required software and hardware components for log collection, web server or any kind of application software for its installation.		
20	The proposed system should encrypt the logs or the channel of logs transmission before sending them to the correlation engine. The System should also compress the logs before transmission to the log correlation engine.		
21	The solution must not have any restriction on the number of rules to be created for correlation		
22	The SIEM solution should provide correlation against data collected from multiple devices across the network.		
23	The SIEM solution should be capable of obtaining security feeds from different sources and integrate the feeds for correlation and analysis.		

#	Description	Compliance (Y/N)	Remarks
24	Log Filtering –. Capability to filter logs by the source system, times, or by other rules defined by the SIEM administrator. Solution should be able to work seamlessly in an air gapped environment.		
25	The proposed solution must come with at least 1200/more out of the box correlation /detection rules to ensure and align with various industry security frameworks like MITRE, NIST, etc… allowing to readily monitor for potential threats across the systems.		
26	The product must provide the ability to limit bandwidth used for transmitting event data.		
27	The solution's reports should run fast on large data sets. Proposed solution should use next generation functionalities like creating set of data from the main index or data store. This will avoid running the queries on large index or full index and faster response for searching and reporting.		
28	The proposed solution must support a configurable replication factor of N where it can tolerate the failure of N-1 peer nodes or should handle failure of a node in the solution.		
29	Reports can be scheduled in a dynamic fashion with schedule windowing and prioritization to improve run priority of high value scheduled reports and manage concurrently running reports to meet the requirements of completing reports under 24 hours. The report should be parameterized, and the user should be able to scale and add the parameter as neededOut of box aging analysis of incident should be available.		

#	Description	Compliance (Y/N)	Remarks
30	The proposed solution must provide the following capabilities as a Security Analytics Platform: a. One single syntax that can be used universally for search queries, alerts, reports or dashboards, SIEM and preferably for SBDL also. b. Incident management technique to facilitate incident tracking, investigation, pivoting and closure c. Risk management technique to apply risk scores to any asset or user based on relative importance or value to the business d. Threat intelligence technique that automatically collect, aggregate, indicators of compromise from OEM threat feeds. The solution should have capability to alert in case duplicate indicators of compromise is added.		
31	The proposed solution must provide an interface that allows the same query string to be configured as an alert, report or a dashboard panel. Same query string should also be capable of being used for SBDL & SIEM.		
32	The solution must provide value in assisting in adhering to audit requirements, alerting of non-compliance and providing necessary reports that can be used during an audit.		
33	The solution must be capable of not only detecting attacks but must also provide a mechanism to respond and recommend mitigation of the attacks in real-time using various quarantine methods while providing the necessary audit trail.		
34	The solution should have an artificial intelligence-based recommendations engine that suggests remediation actions based on previous behavior patterns. The proposed solution should natively have ML capabilities and should not have separate engine/compute requirements for running ML model and the proposed solution must be		

#	Description	Compliance (Y/N)	Remarks
	able to execute automated corrective or follow-on actions via scripted alerts.		
35	Proposed solution should leverage the data in SIEM platform and not build its own data store and maps the fields in the data to User Entity Behaviour Analysis (UEBA)-specific fields.		
36	The system should support a Data Masking capability to remove sensitive data from the view of analysts, such as UID , social UDI number, credit card numbers, etc.		
37	The proposed solution must be able to achieve high availability for indexing cluster without the need of any third party software and the solution should be DR ready and must support the data replication natively without relying on other third party replication technologies on the operating system or storage level with near zero RPO and RTO. Like big data platforms solution should also allow admin to decide on replication factor within DC and replication factor for DR. DR should always be active and should be updated with artifacts for any incident analyst is working on.		
38	Solution shall Collect metrics and log data from a Kubernetes clusters and Virtual Machines as well from proposed virtualization platform		
39	The proposed solution must use a modular approach for storage requirement for all mission critical data it must use SSD High speed storage with minimum 4500 IOPS and any other searchable data must use SAS/SAN storage which must be atleast of 2500 IOPS, all other offline data can be stored for longer in archieve mode on low cost storage e.g.		

#	Description	Compliance (Y/N)	Remarks
	SAN/NAS, etc. and wherever possible leverage the existing infrastructure , compute or storage.		
40	The system must support alarm notification via: SNMP, SMTP, SMS (via Response configuration or client SMTP to SMS Gateway), alert automatically integrated with external help desk systems that accept notifications and presented in real-time as soon as data is collected, normalized, and analyzed; Triggled alerts after a single occurrence or multiple occurrences of an event within a given time period. Email can be sent to individual or group in the Alarm Notification.		

3.4.3.12 Patch Management Solution

#	Description	Compliance (Y/N)	Remarks
1	The solution shall operate without requiring the endpoints to belong to a Domain or Active Directory in SL-UDI		
2	The solution shall be capable of integrating with one or more Active Directory structures when it is present.		
3	The solution should be able to deploy the Patch management agent as well as the patches with the help of IP addresses.		
4	The Patch Management Solution must be appliance based. In case of non-appliance, the bidder has to supply the complete hardware, software, operating system, database software etc. It would be the responsibility of the Bidder to supply the solution complete in all respect.		
5	The offered Patch Management solution should not have any impact on the Wide Area Network and on working of SL-UDI's core applications.		
6	The offered Patch Management Solution should support centralized and or distributed architecture.		

#	Description	Compliance (Y/N)	Remarks
7	The offered solution should support the virtualized environment also.		
8	The Patch Management solution should support failover or redundancy.		
9	The Patch Management solution should be Agent based/Agentless		
10	Deployment of different sets of hardware should be facilitated across various zones in DC / DR. The servers should be deployed in the Desktop zone and the server zone. The patch management servers deployed in the desktop zone should be able to serve up to 2000 machines. Separate Patch management servers to be made available for external and internal zones. All the set up should have DC-DR set up.		
11	The offered solution should have the capability to discover the Assets operational across SL-UDI's locations i.e. Scan the network to produce a full inventory of IT assets and provide flexible ways to group and classify these assets.		
12	The solution should have the capability to whitelist the applications of its own and means for modifications on the whitelisted application according to SL-UDI requirement should be made available		
13	The solution should be able to block a particular software application or list of applications at the endpoints which may be categorized as unauthorized by SL-UDI.		
14	The solution should allow administrators to generate customized reports on Hardware and Software inventory information.		
15	The solution should discover the assets operational in virtual environment		
16	The Patch Management solution should support the heterogeneous environment i.e. multiple version of		

#	Description	Compliance (Y/N)	Remarks
	operating systems including but not limited to Microsoft, Unix, Linux, Mac OS, Sun Solaris etc.		
17	The Patch Management solution should not be machine or configuration dependent. The solution should work smoothly and independently irrespective of configuration and hardware.		
18	The Patch management solution should support the range of applications other than Operating System Patches including but not limited to Adobe, Mozilla, Real Networks, Java, Chrome etc. to apply the appropriate patches released by the respective OEMs.		
19	The Patch Management solution should have the ability to manage PCs, Laptops, Servers, Routers, and Printers etc. on the network.		
20	The Patch Management solution should support the Dynamic IP environment.		
21	The offered solution should support the centralized administration and support role based access control without much load on the network		
22	The latest fixes/ updates should be downloaded to the Patch Management server on the same day that the patch is made available on software vendors‟ websites.		
23	The solution should be able to determine if a patch has already been installed on a node. , even though it is assigned manually. It should have the capability to analyze the appropriate patches of the OS/ applications for the Desktop/ server in comparison to the latest available patches/ updates released by respective OEMs.		
24	The solution should be able to determine if a newer patch has been installed on a node in comparison to the latest available patches/ updates released by respective OEMs. If so, the solution shall treat the node as patched.		

#	Description	Compliance (Y/N)	Remarks
25	The solution should be able to detect the required patches according to individual node's configuration.		
26	Allow users to postpone the deployment of a patch for a period of time determined by the administrator.		
27	The solution should be able to determine patch dependencies prior to deployment of patches to the nodes.		
28	The solution should be able to delete the patch installation files from the nodes" hard disk automatically once the patch has been successfully applied.		
29	The administrator must be able to target the particular patch on all the machines with any specific properties. Machines with similar properties should allow patches to be applied to a select class of assets		
30	The Patch Management solution should support the IPs into groups 1. IP range 2. Network Groups 3. Arrangement of Assets into groups 4. Identification of assets having similar configuration and OS etc.		
31	Remediation/Patch Management		
32	The offered solution should support the event-driven remediation i.e. automatically initiate the process on receipt of a critical patch.		
33	The offered solution should support policy-based remediation actions.		
34	The solution should support VPN users.		
35	The solution should support virtual machines that are offline.		
36	The offered solution should support rollback of patches and service packs applied.		

#	Description	Compliance (Y/N)	Remarks
37	The Patch Management solution should have the capability for Remediation i.e. Continuously deploy, monitor, detect and enforce patch management policies.		
38	The solution should support easy integration with SL-UDI's enterprise Wide area Network (WAN) i.e. providing patch management, device discovery etc. as per the IP address/ range provided in the SL-UDI network but not dependent on host name/ domain.		
39	The solution should support the smooth integration with other security solutions such as SIEM, EDR, IPS, etc.		
40	The solution should support the Application Programming Interface.		
41	The Patch Management solution should have the facility to integrate easily with other security and configuration management systems.		
42	The solution should be able to deploy any software/ files through the patch management solution.		
43	The solution should be able to integrate with databases including but not limited to MSSQL, MySQL, HBase, etc.		
44	The offered solution should have the reporting capabilities.		
45	The solution should have the capability to generate report specific to one environment or should be capable of generating reports with an enterprise view.		
46	The solution should come along with standard reports and or can generate the customized reports as per business requirement.		
47	The solution should support the various reporting formats i.e. reports can be downloaded easily and or exported.		

#	Description	Compliance (Y/N)	Remarks
48	The offered solution should include the remediation information in the reports.		
49	The solution should have the ability to consolidate scan data and to produce a single report for the entire network.		
50	The solution should support the regulatory specific reports.		
51	The solution should be capable of producing alerts When a new host is discovered. When a host exceed		
52	The offered patch Management Solution should come along with all operational technical manuals along with other related documents.		
53	The Patch Management solution should be capable of generating real time reports on patches deployed, when, by whom, to which endpoints, etc.)		
54	The solution should be able to identify nodes that have various instant messengers and be able to uninstall them.		
55	The solution should be able to detect and remedy Security Best Practices.		
56	The solution should be able to remove and create network shares at any time.		
57	The solution should be able to detect and remedy IE Security Configurations		
58	The solution should be able to start and stop services on remote machine without user's knowledge.		
59	The solution should be able to Shut down or restart any machine targeted based on any retrieved properties.		
60	The solution should have the capability to have the Asset Inventory of Desktops, Laptops, and Servers etc. centrally.		

#	Description	Compliance (Y/N)	Remarks
	Asset Details should cover the OS installed, IP no, date of purchase, asset life etc.		
61	The solution should have the capability to manage the OS/ Application licenses across the desktops/ servers. For e.g.: the number of licenses deployed for MS Office, EDR solution etc. should be manageable.		
62	The solution should be able to identify nodes that have USB storage devices enabled and in use. In addition, should be able to prevent only USB storage devices from being used while allowing other USB devices such as keyboard or mouse to be used.		
63	Monitor the status of the clients reporting to Patch Management Solution. All aspects of Installation, De-installation, Configuration, Reconfiguration, relocation, enhancements, updates, upgrades, bug fixes, problem analysis, performance analysis, audits, on - site as well as off - site support of the PMS.		
64	Monitor and follow up the un-managed assets.		
65	Automate the patch pushing to all the clients as and when advised.		
66	Coordinating with OEM in fixing the system related issue and resolve on a time bound manner.		
67	Periodical global threat advisory and follow up on the implementation.		
68	Monitoring the Bandwidth while deploying the Patches.		
69	Testing the Patches before deploying.		
70	Submission of periodical reports.		
71	Any other work pertaining to Patch Management Solution		

3.4.3.13 Email Gateway with High Availability

#	Description	Compliance (Y/N)	Remarks
1	The email gateway offering should be secure appliance/software based solution with high availability implementation.		
2	The email gateway solution should be able to integrate with the existing mailing solution and it is bidder's responsibility to seamlessly migrate to the proposed solution.		
3	The gateway should support a comprehensive email security solution that integrates inbound and outbound defences against latest email threats such as Graymail Safe unsubscribing, snowshoe spam, viruses, Malicious URL Blocking, URL category based filtering, Robust anti-APT, DNS RBL verification, reputation filtering, DLP, Encryptions and phishing filtering utilizing a strong global threat intelligence capability		
4	The solution should be able to integrate with the existing / proposed PAM / PIM /Identity and SIEM solution		
5	The solution should use their own operating system and MTA on appliance. MTA system should be purpose built and optimized for Messaging Queuing which should maintain separate queues for each destination domain to avoid single queue issues		
6	The Directory harvest attack prevention should control the maximum number of bounces per hour due to invalid email recipients according to sender's IP address/range, domain and email reputation. The directory harvest attack prevention should allow administrator to define a limit on number of invalid recipient requests that can be accepted.		
7	The system sends a notification email to users, informing them of quarantined spam and suspected spam messages. This notification should contain a summary of the messages currently in the Spam quarantine for that user.		

#	Description	Compliance (Y/N)	Remarks
8	The solution should allow administrators to apply policies such as blocking known bad senders, throttling suspicious senders and allowing trusted senders based on reputation score assigned from reputation database.		
9	The reputation based scoring architecture should function at TCP conversation level and not after acceptance of email, to increase the overall performance and availability of the messaging infrastructure.		
10	The solution should support creation of customized sender groups and apply customized mail flow policies to each sender group.		
11	Should support Blacklists (IP, Domain, Reputation), Whitelists (IP, Domain, Reputation), Sender and Recipient address whitelist and blacklist		
12	The solution should be able to block, accept, throttle, reject and TCP refuse based on: Sender IP, IP range, Domain, Email Reputation score from reputation filtering, DNS List, Connecting host PTR record		
13	The solution should perform SMTP conversational bounce for invalid recipients (prevent Non-Delivery Report Attack), directory harvest prevention, and have ability to perform SMTP session control and traffic rate limiting (down to per recipient) according to sender's IP address/range, domain or email reputation.		
14	Statistics on Invalid Recipients, Stopped by Reputation, Spams and Viruses Detected, and Cleaned Messages (Per Domain and IP address)		
15	To combat misdirected bounce attacks, the solution should support bounce verification tag to replace envelope sender for all outgoing messages; if a bounce arrives that doesn't contain the tag, then it is discarded. Legitimate bounces should be delivered.		

#	Description	Compliance (Y/N)	Remarks
16	The solution should support multiple email domains on the same appliance. For each domain a specific destination mail server can be assigned for delivery.		
17	Solution should have Multi-layer Anti-spam filter: It should have capability to scan mails for spam with 3rd party SPAM engine before OEM Spam engine.		
18	The policy at SMTP conversation level should be able to perform reverse DNS domain lookup and assign policy per sender basis.		
19	The Mail Security gateway should combine sophisticated content based Anti-Spam technologies, IP reputation and RBL to effectively block spam.		
20	The solution should accurately filter more than 99% of spam.		
21	The solution should support defining custom threshold for the sender or IP reputation in addition to the default thresholds provided by the vendor. Specific actions for the mail delivery should be accordingly configured based on the threshold levels.		
22	The solution should support anti-relay. It should have the ability to configure domains for which the solution will accept or refuse email.		
23	The solution should support RBL lookup. It should support adding of multiple RBL list.		
24	The solution should have an option to allow/block mails by IP address, sender Domain address and sender email address.		
25	The solution should support scoring based threshold to detect spam. Based on severity a different threshold action should be configured.		

#	Description	Compliance (Y/N)	Remarks
26	The solution should provide protection against zero-day and targeted attacks. It should be able to dynamically analyse message attachments for malware without sending files to cloud		
27	The solution should offer various actions for spam detected: Monitor, Block, Annotate and Deliver, Quarantine and Forward.		
28	File attachment detection should include but not limited to: a. File Type b. File Size c. File Name d. File extension e. MIME Type		
29	The solution should have dual virus scanning available within the appliance. One of the AV engine should be from Gartner leader quadrant		
30	Automatic quarantine and release of quarantined messages not falling into new virus/worm characteristics upon outbreak rule update and before virus signature update.		
31	The solution should support outbound SMTP over TLS based on destination domains or system wide. The solution should support outbound SMTP authentication		
32	The proposed system shall be able to raise an alert when the number of messages in the email queues exceeds certain thresholds.		
33	The solution should support restricted access to the appliance for management through SSH or Web GUI. Administrator should be able to specify a list of authorized		

#	Description	Compliance (Y/N)	Remarks
	IP addresses, subnets or networks to administer the appliances.		
34	The proposed solution should include Anti-APT / Next Generation detection ability to quarantine emails suspected to been infected with malware both for inbound as well as outbound email		
35	The proposed solution should have an option to restore the configuration from a previous backup.		
36	The solution should have customizable Role-Based Administration views.		
37	Should generate reports showing the details of viruses found along with the username, time of access, URL access.		
38	The solution should alert management through email. It should send email alerts for: a. Anti-virus b. SPAM c. Phishing events d. Compliance e. System Events		
39	The solution should be able to automatically apply the latest security and software updates. Vendor should provide updates and security enhancements to the operating system, MTA, and supporting software updates including Antivirus and anti-spam engine updates when they become available.		
40	Should be able to configure, manage, and monitor multiple appliances from a central management console and should provide the real time health status of all the appliance modules on the dashboard for CPU and memory utilization, total no of concurrent connections etc.		

#	Description	Compliance (Y/N)	Remarks
41	The solution should have an option to restore an appliance to its original image configuration.		
42	Should be able to restrict mails based on attachment file types, file size.		
43	Should have a feature of domain blacklisting in order to restrict sending of mails to such domains.		
44	Solution should be capable of generating user access logs as well as activity logs.		
45	The solution should be able to integrate with the proposed Syslog and SIEM solutions.		
46	The solution should support backup of Email gateway rules and settings.		
47	The solution should have capability to consume external threat information in STIX/TAXII and custom feeds		
48	The solution should provide the URL defence service to: Re-write the original suspicious URL in the mail body to another URL and On clicking the re-written URL, the browser session should pass through a Web security scanning infrastructure of the same OEM		
49	The solution should provide capability of the appliance to perform recipient validation by querying an external SMTP server prior to accepting incoming mail for the recipient		
50	Solution should provide forged email detection protection against business executive compromise and provide detail logs on all attempts and actions.		
51	The solution should support outbound SMTP over TLS based on destination domains or system wide and support outbound SMTP authentication		

#	Description	Compliance (Y/N)	Remarks
52	The solution should support to selectively apply digital signatures on outbound emails including capability to apply digital signatures based on policy using mail or other attributes.		
53	The solution should support for SPF, DKIM, and DMARC email authentication including ability to apply email authentication requirements based on domain (specific or wildcard), ability to quarantine emails failing authentication, Include ability to selectively confirm email authentication success (SPF, DKIM, DMARC) for inbound messages on other filtering policies that may include whitelisting of those addresses.		
54	The solution should have DLP feature with full template based DLP, so that organization can deploy DLP as per their compliance and require database. "		
55	"The appliance should support the use of IPv6 for: o Appliance interfaces o Gateways (default routes) o Static routes o SMTP Routes o Querying external SMTP server with IPv6 address (for Recipient validation) o IPv6 Sending hosts o Content Filters o Sending to IPv6 destinations o Report searches"		
56	The Solution should be able to integrate with Domain Reputation Service that provides a reputation verdict for email messages based on a sender's domain and other attributes.		
57	The solution should support LDAP referrals i.e. When using LDAP referral's, the original query gets referred to another LDAP server.		
58	The solution Should offer Outlook Plug-in support for reporting missing spam, false positives, virus emails, encryption etc.		

#	Description	Compliance (Y/N)	Remarks
59	The solution should support trusted relay so that original senders' IP address can be identified from "Received" headers or other email headers (when appliance is not first layer mail gateway)		
60	The solution should provide protection against zero-day and targeted attacks. It should be able to dynamically analyze message attachments for malware without sending files to cloud. The Email Security Appliance must be able to provide a safe-printed PDF version of a message attachment detected as malicious or suspicious. The safe view of the message attachment is delivered to the end-user and the original attachment is stripped from the message.		

3.4.3.14 Database Activity Monitoring with High Availability

#	Description	Compliance (Y/N)	Remarks
1	All network based Data Base activities should be monitored in real time basis using the Appliance. Should not use any agents to monitor network based Data Base activities.		
2	Proposed DAM solution should keep all the audit trail tamperproof.		
3	DAM Solution component should be managed centrally.		
4	DAM Solution Should have the ability to aggregate, normalize and correlate activity from multiple heterogeneous Data Base Management Systems (DBMSs) viz. Oracle, MS-SQL (Microsoft SQL Server) DB2, MySQL, Teradata, HBase etc.		
5	Product should provide automated discovery of both new and existing Database tables.		
6	DAM Solution support identification of rogue or test databases.		

#	Description	Compliance (Y/N)	Remarks
7	Proposed solution should be capable of detecting sensitive data types, such as personal identifiable information in database objects.		
8	The solution verifies that default database accounts do not have a “default” password.		
9	The Solution should have pre-defined reports covering compliance, non-technical, incident and general technical reports.		
10	The product should support custom report generation.		
11	Should have an option to distribute reports on demand and automatically (on schedule).		
12	The solution should capture Select activity by user/role.		
13	The solution should capture update, insert and delete (DML) activity by user/role.		
14	The solution should capture schema/object changes (DDL) activity by user/role.		
15	The solution should capture manipulation of accounts, roles and privileges (DCL) by user/role.		
16	DAM solution be able to monitor activities at new DB interface/ connector created by any user/ system without any manual intervention.		
17	The solution should monitor privileged users and administrator activities.		
18	The solution should have an option to upgrade to block privileged users activity if required.		
19	The solution should monitor 100% of the DB traffic for all DB violation and attacks despite the traffic is not being audited.		

#	Description	Compliance (Y/N)	Remarks
20	The Solution should monitor for all DB attacks like SQL injection and alert despite the traffic is not audited.		
21	Solution should be capable of generating user access logs as well as activity logs.		
22	The solution should be able to integrate with the proposed Syslog and SIEM solutions.		
23	The solution should support Per User or User Group Policy and Multilevel Administration Privilege.		
24	The solution should support secured (encrypted) backup of DAM rules and settings.		

3.4.3.15 SSL VPN / IPsec VPN with High Availability

#	Description	Compliance (Y/N)	Remarks
1	Must be able to support minimum 200 concurrent IPsec and/or SSL clients scalable to 500 as a dedicated hardware/virtual appliance		
2	Provide support for client (IPsec VPN) and Clientless web access (SSL VPN) for desktop and laptop		
3	The IPsec VPN and SSL VPN solution should integrate natively (not via radius server) with Active directory for user authentication and authorization. It must support Active Directory group policy based granular resource and application control without third party application servers.		
4	Offer seamless application support for clientless access via SSL VPN using browser. Provide an easy configuration wizard for application integration with minimal manual configuration.		

#	Description	Compliance (Y/N)	Remarks
5	Support Windows 10, 11 and latest, Mac OS X and latest, Linux platforms, Android and Apple iOS etc.		
6	Provide easy web based management for IPsec VPN and SSL VPN appliance, role based administration, detailed audit and logs for incident isolation and troubleshooting, and extensive filters and statistics per day, week and month.		
7	The solution must be scalable, and easy to maintain and operate.		
8	Ability to present applications to user through a web VPN portal interface and apply access controls based on per-user, per-group and per-resource.		
9	Ability to provide SSL tunnel VPN service and apply access controls based on per-user, per-group and per-resource.		
10	Support high availability active/active or active/passive mode to minimize user interruption in case one VPN component fails. If one VPN component fails, the high availability feature should service all connections transparent to the users. For Active/Active solutions under normal conditions, redundant components should actively service VPN connections simultaneously.		
11	Include at least four 1 Gbps multi-mode fiber Ethernet ports and a minimum eight 10/100/1000 Mbps copper ports. All ports will be compatible and work with the existing network equipment.		
12	Support hot swappable (1+1) field replaceable redundant power supply and fan module		
13	Provide support for multiple security zones for different constituents and applications.		
14	By seamlessly integrating with Active directory, provide visibility and control by any combination of user, group, and IP address.		

#	Description	Compliance (Y/N)	Remarks
15	Supply QoS support for high priority application and control real- time traffic. Traffic classification is based on differentiated services code point (DSCP).		
16	Be a modular, scalable, industry standards-based platform and must interoperate with multi-vendor devices and management tools.		
17	Support 802.1q VLAN tagging.		
18	Support and accommodate terminal services and secure remote access to selected resources inside and outside of SL-UDI network.		
19	Provide a centralized web management console and out of band Ethernet interface for management that supports SSHv2 . Provide delegated management so that SSL VPN device can managed by different groups and individuals		
20	Offer the capability to track and log all remote access policy violations, exceptions, incidents and response activities and integrate with SIEM solution for security monitoring.		
21	All proposed equipment and software must be IPv6 compliant andIPv6 enabled in the delivered solution. Support for IPv4 to IPv6 transition technologies include IPv4 and IPv6 dual stack, automatic IPv4-compatible IPv6 tunnelling, IPv6- to-IPv4 tunnelling, All proposed equipment and software must IPv6 compliant and enabled.		
22	Provide extensive web based reporting capabilities and dashboards to show connected users and historical reporting usage in a graphical format.		
23	Support for integrity checking for end user systems		
24	Integrated Application identification, IPS, antimalware/spyware, antivirus, anti-phishing functionality, provided through a scalable and resilient platform. Vendor		

#	Description	Compliance (Y/N)	Remarks
	needs to state performance throughput if IPS, antivirus features are enabled.		
25	Dynamic policy-based network bandwidth control by application, user, source, destination, interface, IPsec VPN tunnel, URL categories, threats and data.		
26	Support for VRRP, QoS and full OSPF routing protocol.		
27	Support for link aggregation and load balancing.		
28	Support of device virtualization.		
29	Enforce granular, policy based controls for incoming and outgoing Internet traffic based on user identity and/or AD group membership.		
30	Provide Active Directory group membership based authentication for accessing web resources. At the same time, it should also support the SL-UDI permitted, limited web services for anonymous users.		
31	Supply a graphical feature-rich enterprise console with fast interactive customizable user interface for rapid real-time monitoring, threat investigation, comprehensive incident management and response.		
32	GUI management interface should include context sensitive help.		
33	Present real-time visibility into security and compliance posture.		

3.4.3.16 External Firewall (Next-Gen) with High Availability

#	Description	Compliance (Y/N)	Remarks
1	The External Firewall should be of different make than internal firewall		
2	The Firewall shall be configured in Active — Active configuration to provide control, power supply and software redundancy. Any components required for operating the firewall in active-active load shared mode, should be provided in a "no single point of failure" configuration.		
3	Firewall should be appliance based with hardened Operating System and support “Stateless” policy inspection technology. It should also include application intelligence for commonly used TCP/IP protocols like Telnet, FTP, SMTP, http, DNS, ICMP, DHCP, ARP, RPC, SNMP, Lotus Notes, and Exchange etc. It should also support encrypted protocols like SFTP, HTTPS etc.		
4	The platform should support Ether Channel, Ethernet protocol or equivalent.		
5	Minimum Throughput Requirement with NGFW, IPS and Application Control enabled: 30 Gbps (if as per bidder architecture they require more capacity they should plan for it)		
6	Minimum Concurrent Sessions with Layer 7 NGFW and Application control enabled: 5Million (if as per bidder architecture they require more capacity they should plan for it)		
7	Minimum New Connections per Second with Layer 7 NGFW and Application control enabled: 200K (if as per bidder architecture they require more capacity they should plan for it)		
8	VLAN: Minimum 1024 VLAN		
9	The platform must be supplied with at least 8*1Gbps copper interfaces ports and 8 Nos of 10 Gbps fiber ports and		

#	Description	Compliance (Y/N)	Remarks
	4*40/100Gbps ports. All fiber interfaces should be populated with multi-mode transceiver ports		
10	Appliance should be rack mountable and support side rails if required.		
11	Solution must have hot swappable field replaceable dual power supply and fan module		
12	The platform should support VLAN tagging (IEEE 802.1q).		
13	Firewall should support Link Aggregation functionality to group multiple ports as single port.		
14	Firewall should support Ethernet Bonding functionality for Full Mesh deployment architecture.		
15	It should support the IPSec VPN for both Site-Site and Remote Access VPN.		
16	Firewall system should support virtual tunnel interfaces to provision Route-Based IPSec VPN.		
17	It should support the system authentication with recognized authentication, authorization and accounting methodologies such as Radius, Tacacs+ etc.		
18	Firewall Appliance should have a feature of holding multiple OS images to support resilience and easy rollbacks during the version upgrades.		
19	Firewall should support PKI Authentication.		
20	Firewall should support dual stack (IPv4 and IPv6).		
21	Firewall should be capable of dynamic routing on VPN.		
22	Firewall should support client-based SSL/TLS as well as IPSec VPN Tunnels.		

#	Description	Compliance (Y/N)	Remarks
23	Firewall should support web based (http/https) configuration.		
24	Firewall should be integrated with SIEM solution		
25	Firewall should be of the next generation and support both Stateful and Stateless policy inspection technology. It should have an integrated IPS engine.		
26	The proposed firewall shall perform content based signature matching beyond the traditional hash base signatures		
27	The solution should support threat prevention and sandbox services to block exploits, prevent malware, and stop both known and unknown advanced threats		
28	All the proposed threat functions like IPS/vulnerability protection, Antivirus, C&C protection etc. should work in isolated environment without any need to connect with the Internet.		
29	The NGFW must be able to provide Machine Learning algorithm's for advanced protections		
30	Should support the report generation on a manual or schedule (Daily, Weekly, Monthly, etc.) basis		
31	The solution shall provide option to scan all ports at wire speed, detecting and blocking all malicious traffic trying to bypass existing security controls.		
32	Should have built in report templates base on Applications, Users, Threats, Traffic and URLs		

3.4.3.17 Internal Firewall (Next-Gen) with High Availability

#	Description	Compliance (Y/N)	Remarks
1	Firewall should support Syslog server logging.		
2	Should have support for SNMP V1 to V3.		

#	Description	Compliance (Y/N)	Remarks
3	Support for voice protocols: H.323, SIP, and NAT/ ALG for H.323/ SIP.		
4	Firewall should have Automated certificate enrolment (SCEP). PKI Support.		
5	Firewall should support multilevel administration privilege.		
6	Firewall should support software upgrades using secure web Interface.		
7	Firewall should support Command Line Interface using console SSH.		
8	Firewall should support secured backup of firewall rules and settings in the case of a replacement or an upgrade.		
9	The firewall should have extensive debugging capabilities to assist in hardware problem resolution.		
10	The Internal Firewall should be of different make than external firewall		
11	The Firewall shall be configured in Active — Active configuration to provide control, power supply and software redundancy. Any components required for operating the firewall in active-active load shared mode, should be provided in a "no single point of failure" configuration.		
12	Firewall should be appliance based with hardened Operating System and support “Stateless” policy inspection technology. It should also include application intelligence for commonly used TCP/IP protocols like Telnet, FTP, SMTP, http, DNS, ICMP, DHCP, ARP, RPC, SNMP, Lotus Notes, Exchange etc.		
13	Minimum Throughput Requirement with NGFW, IPS and Application Control enabled: 50 Gbps (if as per bidder architecture they require more capacity they should plan for it)		
14	Minimum Concurrent Sessions with Layer 7 NGFW and Application contron enabled: 15Million (if as per bidder architecture they require more capacity they should plan for it)		

#	Description	Compliance (Y/N)	Remarks
15	Minimum new Connections per Second with Layer 7 NGFW and Application control enabled: 300K (if as per bidder architecture they require more capacity they should plan for it)		
16	VLAN: Minimum 1024 VLAN		
17	Firewall should have 8*10Gbps SFP integrated data ports, 8 x 100Gbps ports. Fiber interfaces should be populated with multi-mode transceiver modules.		
18	The appliance should be capable of providing Firewall		
19	Should support translating between IPv4 and IPv6 for the following inspections: DNS, FTP, HTTP, and ICMP.		
20	Network address translation (NAT) shall be supported so that the private IP addresses of hosts and the structure of an internal network can be concealed by the firewall. Should support NAT 66, NAT46, NAT 66 and NAT44		
21	The firewall should have extensive debugging capabilities to assist in hardware problem resolution.		
22	The firewall should have support for IPSEC VPNs with DES/ 3DES and AES support.		
23	The firewall shall support a number of routing options and configurations. Routing protocol support shall include static routes, Open Shortest Path First (OSPF), RIPv1/v2.		
24	Virtual LAN (VLAN) support, high port density, WAN support and expandability of interfaces over time are some important network integration features shall be supported.		
25	It should support the system authentication with recognized authentication, authorization and accounting methodologies such as Radius/ Tacacs+ etc.		
26	It shall provide network segmentation features with powerful capabilities that facilitate deploying security for various internal, external and DMZ (Demilitarized Zone) sub-groups on the network, to prevent unauthorized access.		
27	Firewall should support dual stack (IPv4 and IPv6) for all features		

#	Description	Compliance (Y/N)	Remarks
28	Firewall should support web based (http/https) configuration with dual or multi-factor authentication.		
29	Firewall should support Syslog server logging and integration with SIEM		
30	Firewall should be of the next generation and support both Stateful and Stateless policy inspection technology. It should have an integrated IPS engine, AntiAPT		
31	The proposed firewall shall perform content based signature matching beyond the traditional hash base signatures		
32	The solution should support threat prevention and sandbox services to block exploits, prevent malware, and stop both known and unknown advanced threats		
33	All the proposed threat functions like IPS/vulnerability protection, Antivirus, C&C protection etc. should work in isolated environment without any need to connect with the Internet.		
34	The NGFW must be able to provide Machine Learning algorithm's for advanced protections		
35	Should support the report generation on a manual or schedule (Daily, Weekly, Monthly, etc.) basis		
36	Should have built in report templates base on Applications, Users, Threats, Traffic and URLs		
37	The firewall appliance should not include any wireless, Bluetooth, or infrared interfaces or tunnelling mechanisms that allow unauthorized access. Each appliance must be equipped with redundant and hot-swappable power supplies, fan modules/trays, SSDs, and interface slots.		
38	The solution should support multi-tenancy functionality, including dedicated RAM, CPU cores, independent reboot and upgrades and most important, predictable performance.		
39	The solution should support SSL/TLS termination with protocols TLS 1.2, TLS 1.3 or latest, and QUIC, capable of detecting and decrypting all TCP ports utilizing SSL/TLS (TCPS) and QUIC communication without downgrading the SSL/TLS standard. The solution should be IPv6 certified.		

#	Description	Compliance (Y/N)	Remarks
40	The solution must establish a bidirectional integration with the proposed NAC/AAA, Anti-APT, NDR solution to receive updates and transmit threat feeds, enabling NAC/AAA to quarantine or isolate users and devices.		

3.4.3.18 Web Application Firewall (WAF) with High Availability

#	Description	Compliance (Y/N)	Remarks
1	The solution must be appliance based.		
2	Supported application optimization modules such as compression, caching, connection multiplexing, SSL offloading, TCP optimization.		
3	The appliance should support virtualization and scalability without changing hardware		
4	WAF should support device fingerprint technology by involving various tools and methodology to gather IP agnostic information about the source.		
5	The solution should support integration with PAM/PIN/IAM solutions		
6	Must address web application layer attacks from at least OWASP Top 10 and SANS Top 25 or latest		
7	Should support graphical analysis and reporting		
8	Should have auto policy configuration, self-learning and tuning capability to prevent false positives		
9	Should have a minimum set of rules defined to prevent OWASP Top 10 and SANS Top 25 attacks in default configuration		
10	Throughput minimum 30 Gbps from day 1 with scalability to upto 100Gbps without changing the hardware appliance		
11	RAM 64 GB		

#	Description	Compliance (Y/N)	Remarks
12	SSL transaction 10,000 CPS/TPS		
13	Capacity 1 TB for internal storage		
14	Network interface ports – 24, 4*40Gbps and		
15	SSL throughput 2 GBPs		
16	Link failover detection time 6 seconds		
17	Concurrent session support – 5 million		
18	Internet link connections supported by load balancer – 8191		
19	Supported load balancing layer from layer 2 to layer 7		
20	Interface for device configuration and management GUI, HTTP/HTTPS, SSH/Telnet/CLI		
21	Supported Load balancing algorithms – Minimum misses, Hash, Persistent Hash, Tunable Hash, Weighted Hash, Least connections, Least connections per service, Round Robin, Response time, Bandwidth		
22	Compliance Certificates – RoHS, Compliant EU directive 2011/65/EU CE LVD EN 60950-1, CB-IEC60950-1, CCC, CTUVus CE EMC EU directive 2004/108/EC, FCCart 15B class A, ICES-003, VCCI, C-tick		
23	Type of load balancer – Server load balancer		
24	I/P and O/P port – USB, RS-232		
25	Support dynamic and static routing protocols		
26	Support PAT		
27	Support SNMP		
28	Support static NAT		
29	Support virtual grouping		
30	Integrate WAF with SIEM solution to provide a single dashboard to view events generated		

#	Description	Compliance (Y/N)	Remarks
31	Proposed WAF Solution should Identify and limit / block suspicious clients, headless browsers and also mitigate client- side malware.		
32	Proposed WAF Solution should protect API based communication between client & servers using all the relevant WAF signatures		
33	Should provide encryption for user input fields to protect from browser-based malwares stealing users credentials		
34	On detecting an attack or any other unauthorized activity, the Web application firewall must be able to take the appropriate action. Supported actions should include the ability to drop requests and responses, block the TCP session, block the application user, or block the IP address. For particularly destructive attacks, the Web application firewall should be able to block the user or the IP address for a configurable period of time.		
35	Proposed Solution should be able to track application changes over time and adjust config elements and rules based on that data		
36	Should provide extensive visibility into the health and performance of applications with dashboards to highlight applications with longest response time, top HTTP transactions, Top connections etc.		

3.4.3.19 Intrusion Detection System/ Intrusion Prevention System (IDS/IPS) with High Availability

#	Description	Compliance (Y/N)	Remarks
1	IPS shall be dedicated appliance based solution to detect and actively prevent attacks in real-time.		
2	The appliance should support Active-Active and Active-Passive configuration		

#	Description	Compliance (Y/N)	Remarks
3	The solution should deliver a sustained throughput of at least as follows: • Minimum 30 Gbps with 8x1Gbps and 8X10Gbps and 4 x 100G interfaces at the Public Zone • Minimum 50 Gbps with 8x10G and 8X100G interfaces at MZ and DMZ Zone		
4	Should be IPV6 ready to integrate with IPV6 infrastructure.		
5	IPS system should have High availability mechanism of pass-thru to allow traffic to flow uninterrupted even during the failure, malfunction, OS corruption or Hardware issues. Pass-thru mechanism should be achievable using internal bypass or external bypass switches.		
6	IPS system should support 802.1 Q tagged VLAN environment. IPS system should be capable to scan VLAN tagged frames bi- directionally for malicious content.		
7	IPS device should have redundant hot swappable and field replaceable power supply and fan module		
8	IPS should have inbuilt protection against DOS/DDOS attack. The IPS should use exploit based as well as volume based technique to prevent against DOS/DDOS attack.		
9	The IPS solution should support Connection Limiting Policies to restrict the number of connection from one single host / rate based attack system		
10	The IPS solution should support Connection Limiting Policies to restrict the number of connection from one single host / rate based attack prevention techniques		
11	IPS should have Protection against TCP, UDP and ICMP Flood, DHCP Flooding, DNS Flooding, Multi-layered Sync Flood Mechanism, SSL based attack etc.		

#	Description	Compliance (Y/N)	Remarks
12	Management: a. Should support SNMP V1 to V3 b. Should support HTTPS c. Should support SSH/TELNET d. Should support Console		
13	Security Maintenance and Reporting: a. IPS should support 24/7 Security Update Service b. IPS should support Real Time signature update c. IPS should support Automatic signature synchronization from database server on web		
14	IPS solution shall provide source reputation based analysis		
15	The solution should be able to integrate with the proposed Syslog and SIEM solutions		
16	IPS should maintain blacklisting or whitelisting for efficient traffic management		
17	The solution should support Per User or User Group Policy and Multilevel Administration Privilege.		
18	The solution should support secured (encrypted) backup of IDS/IPS rules and settings.		
19	The firmware of the proposed solution must be digitally signed by the manufacturer in order to ensure that it is not changed in any way, avoiding possible compromises or security problems. The initial sequence of the proposed device should validate these signatures and verify the integrity of the firmware used.		
20	The solution's detection engine must employ multiple methods for detecting threats, including exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioural anomaly detection techniques. Each type of detection mechanism supported should be identified and explained.		

#	Description	Compliance (Y/N)	Remarks
22	The solution should provide advanced host and event correlation to identify compromised hosts. This should be achieved by correlating events from multiple sources (IPS events, vulnerability information, CNC connections, network malware events) and leveraging reputation intelligence and big data analytics. Indicator of Compromise (IOC) tags must be associated with hosts to simplify analysis and understand the possible compromise "state" of the machine and network.		
23	The solution should include the following capabilities at a minimum: • -the ability to analyse network traffic to detect intrusions, store data on attacks, block and modify malicious traffic; • -the ability to create custom intrusion policies; the ability to detect sensitive data such as identity number or credit card or personal information in ASCII text; • -traffic anomaly detection and event impact analysis to prevent zero-day attacks; • -capture traffic for evidence analysis in TCPDUMP-supported format for attack reproduction; • -signature categorization based on MITRE ATT&CK TTPs with incidents viewable on the dashboard based on MITRE ATT&CK mapping to comprehend attack stages; • -dynamic, real-time analysis to create a monitored network map, including parameters such as Host, Application, Protocols, IOCs, OS, and Vulnerabilities.		
24	The solution should enable the allocation of intrusion events to different administrators for review and status updates regarding incidents. For instance, assigning a suspected intrusion event to an admin for review and updating the summary, next actions, and marking the status as resolved/escalated/closed, etc.		
25	The solution should seamlessly integrate with various security components, including Vulnerability Scanner, Custom Threat Feed sources, CMDB database, SIEM, NAC/AAA, NDR, SDN-Fabric, EDR/EPP, and third party etc. .		

#	Description	Compliance (Y/N)	Remarks
26	The solution should allow administrators to be able to customize and activate new protections based on attack parameters (such as source IP/port, destination IP/port, etc.). NIPS must offer an automated mechanism to update and download new signatures.		
27	The should have ability to categorize signatures based on MITRE ATT&CK TTPs with incidents viewable on the dashboard based on MITRE ATT&CK mapping to comprehend attack stages;		

3.4.3.20 Host Intrusion Prevention System (HIPS)/ Server Security Solution with High Availability

#	Description	Compliance (Y/N)	Remarks
1	The servers in DMZ, MZ, Management and Public zones should be enabled with Host Based Intrusion Detection and Prevention/Server Security Solution mechanisms.		
2	The solution should protect against common classes of attacks, such as port scans, buffer overflows, ransomware, remote access tools, malicious HTML requests, and worms, etc.		
3	The solution must capture and analyse flow and process telemetry from all workloads across all DCs, in real time and store in a time-series for long data retention		
4	The solution should be able to provide visibility into workload package vulnerabilities natively along with their CVE and CVSS Score data and create policies using CVE and CVSS Score to restrict access or quarantine workloads having these vulnerability attributes.		

#	Description	Compliance (Y/N)	Remarks
5	The solution should use the HTTPS and TLS protocols for the management interface and for communication between the HIPS and management centre.		
6	When an application attempts an operation, the HIPS should check the operation against the application's security policy, making a real-time allow or deny decision on its continuation and determine if logging the request is appropriate.		
7	By combining security policies implementing distributed firewall, operating system lockdown and integrity assurance, and audit event collection capabilities, the HIPS should provide comprehensive protection for exposed systems.		
8	It should support Signature as well as behavioural based detection.		
9	The solution must automatically generate per application whitelist policy and enforce the auto generated whitelist policy allowing only the required traffic, blocking everything else.		
10	The solution must automatically group endpoints with similar behaviour and security posture into policy groups and should be able to correlate network traffic to actual application process that generated it.		
11	The solution must provide application dependency map. As part of the application dependency map it must provide detailed and accurate application to application and service relations and inter-dependencies. Solution should have capability to do application whitelisting/blacklisting		
12	The offered product series or its operating system series may have achieved EAL (Evaluation Assurance Level) Certification of EAL2 or higher in the Common Criteria.		

#	Description	Compliance (Y/N)	Remarks
13	The proposed solution may be capable of filtering HTTP requests to prevent directory traversal and denial-of-service (DoS) attacks.		
15	The proposed solution should provide Executable matching for applications based on path, hash, digital signature and file description for signatures and exception and not just on path basis.		
16	The proposed solution should be capable of blocking and detecting of IPv6 attacks. The solution must provide details about each process that is launched on a server including the process start time, command line process ID and user.		
17	The solution must detect user logon activities, execution of malicious activity, privilege escalations, shell code execution and side channel attacks and alerting based on failures.		
18	The solution must integrate with orchestration tools to ingest workload tags and annotations & enrich application context of the workloads dynamically. The solution must track the process tree lineage for each server and maintain a historical record of the process tree over time.		
19	The solution must detect process hash consistency for similar processes across the application environment		
20	The solution must have threat intelligence to detect bad/anomalous process hash across workloads and capability to ingest anomalous/bad hash from 3rd party sources.		
21	The solution should provide capability to create customer Forensic rules to identify process behaviour deviations and provide alerts and notifications.		
22	The solution should provide capability to identify stale ports without active communications across applications and workloads to provide visibility into potential attack surface.		
23	The solution must Track application whitelist policy in near real-time for compliance deviations and generate alerts (including full detail of all flows in or out of policy compliance)		

#	Description	Compliance (Y/N)	Remarks
25	The solution must maintain policy modification and changes in policy versions and show the delta between different policy versions and provide ability to rollback between different versions.		
26	The solution must provide the ability to simulate and test the policies using real time and historical data, without having to enforce or configuring any rules on the workload .		
28	The solution must support hierarchical policy enforcements on workloads to apply overriding InfoSec and Network security controls to be inherited by workloads		
29	The solution should be able to share threat intelligence with Firewalls, ACS and DC Fabric to provide micro segmentation for east-west traffic flows wherever there is no agent installed		

3.4.3.21 Security Orchestration Automation and Response (SOAR) with High Availability

#	Description	Compliance (Y/N)	Remarks
1	The solution must be a fully on premise solution deployed in-house. The OEM should recommend the sizing for the hardware/VM for the proposed solution.		
2	The solution should support Role Based Access (RBAC)		
3	Solution should support multitenancy and provide a clear Architecture for function in multitenant environment.		
4	Solution should support deployment for access networks which are behind the firewall or isolated from Internet		
5	Solution should provide for dissolvable agents for machines that are under investigation to unobtrusively perform forensic tasks on those machines for Windows, Linux, and Mac platforms.		

#	Description	Compliance (Y/N)	Remarks
6	Solution should maintain SLA for incident		
7	Solution should support sending notifications to other users on per incident basis		
8	Solution should specify the mode of receiving an incident for example (REST API, mails, Syslog etc.)		
9	Solution should support grouping of multiple incidents of similar type into one incident		
10	The proposed solution must have a orchestrator ability to direct and oversee all activities from beginning to end.		
11	The propo1sed solution orchestrator must be able to ingest security data from any source and in any format.		
12	The proposed solution orchestrator must be able to poll data sources and pull data into the platform.		
13	The proposed solution orchestrator must be able to interpret the data and make it usable by the platform. Such indicators could be emails, IP address, Domains, File Hashes		
14	The ability to extract indicators from various files attachments such as PDFs, ODF, emails, or raw text. Example:.txt, .eml Email applications, Messages, PDF, Docx, CSV, HTML		
15	The proposed solution orchestrator must be able to initate automation upon creation of new events with artifacts or existing events with new artifacts without human intervention.		
16	The proposed solution orchestrator must be able to dispatch automation tasks from it's queue at the appropriate and optimal time, passing them to the automation engine for execution.		
17	The proposed solution orchestrator must be able to introduce human supervision if necessary, pausing the automation engine for an approval by asset owner is needed to execute a security action on a target.		

#	Description	Compliance (Y/N)	Remarks
18	The proposed solution orchestrator must ensure output data from one action is properly parsed, so that future actions can make use of it.		
19	Consistent, Standardized naming conventions for actions. Normalized action names in a Virtualization / Abstraction layer allows easy transition across API action calls and/or products		
20	The proposed solution must provide a built-in visual automation editor.		
21	The proposed solution built-in visual automation editor must enable users to construct comprehensive playbooks to fully validate, investigate and resolve incident using drag and drop capabilities visually without needing the expert ability to code.		
22	The proposed solution built-in visual automation editor must be able to represent code using blocks and blocks can be connected in a one-to-one, one-to-many and many-to-one fashion to dictate an order of execution.		
23	The proposed solution built-in visual automation editor must be able to provide an interface where testing and debug can take place allowing transition from edit mode to test mode seamless.		
24	The proposed solution must provide an open and extensible interface for new integrations to connect the platform to any of the thousands of point products available in the security market today.		
25	The proposed solution must provide easy transition in and out of other security technologies without negatively impacting automated playbooks.		
26	The proposed solution must provide users with the framework and open control of integrating with other technologies without relying on the solution provider for development work.		
27	The proposed solution must standardize on one language such as Python, java, C#, etc… for developing integrations with other technologies for custom actions and custom handling of SOAR		

#	Description	Compliance (Y/N)	Remarks
	playbooks confined in a block while retaining the original visual playbook editor functionality for the entire playbook.		
28	The ability to run multiple SOAR playbooks and actions while retaining the data in the containers/events/cases.		
29	Retaining the data of all multiple runs of SOAR playbooks ensure the retention of key artifacts especially with dynamic information such as threat reputation information.		
30	The proposed solution must have documented REST API access that allows full control over the platform.		
32	The proposed solution must have ability to label the nature of the event.		
33	The proposed solution must have ability to store attachment as part of the user manual workflow or as part of the automated playbook.		
34	The proposed solution must have the ability to mark artifacts as evidence.		
35	The proposed solution must be able to provide an indicator view to quickly pivot investigation of an indicator to past incident occurrences.		
36	The proposed solution must allow case or task assignment in relation to a ticket or an incident to other team members or group.		
37	The proposed solution must provide fine grained role-based access into actions and assets, so users can be granted with investigative actions and not containment actions.		
38	The proposed solution should have an out of the box guidance by offering suggestions to help investigate, contain, eradicate, and recover from a security event, allowing newer analyst to take and validate choices of more experienced analysts.		

#	Description	Compliance (Y/N)	Remarks
39	The proposed solution must have an activity log of actions taken (automated and manual), results returned by actions, chat and comment history in each event.		
40	The proposed solution must provide central management of incidents and administrative functions from a single web-based user interface.		
41	The proposed solution must have an activity log of actions taken (automated and manual), results returned by actions, chat and comment history in each event.		
42	The proposed solution must provide multi-tenancy support allowing multiple departments or business units to use the same solution with appropriate segregations/separations.		

3.4.3.22 Access Control and Directory Services with High Availability

#	Description	Compliance (Y/N)	Remarks
1	Directory services should support configuration of domain services		
2	It should authenticate and authorize all users and computers in SL-UDI network		
3	It should enable assigning and enforcing security policy for all system under control of Directory services		
4	It should enable storage and management of information, provide authentication and authorization framework, support other related services like certificate services, LDAP, rights management, SAML, federated authentication system and certificate management		
5	Solution should integration with industry leading two factor authentication solution.		

#	Description	Compliance (Y/N)	Remarks
6	Apart from end user systems, Operating system (Linux, Windows etc.) should be supported by directory services		
7	Solution should support user base of minimum 300+.		
8	Solution should be configured as per the security policy of SL- UDI		
9	Solution should support configuration of multiple forests and organizational units		
10	Solution should be configured in HA mode with minimal or zero down time		
11	Solution should be compliant with latest LDAP standards		
12	Solution should leverage native replication technology to ensure real time reflection of changes		
13	Solution should be deployed along with OEM recommended database and data replication solution		
14	Solution should support integration with PAM/PIM and IDAM solutions		
15	Solution should support integration with SIEM solutions		
16	Solution should support SSL/TLS-encrypted communication		

3.4.3.23 Endpoint Detection and Response (EDR)

#	Description	Compliance (Y/N)	Remarks
1	The Solution should provide Next Gen antivirus capabilities and should be a replacement for AV solutions		
2	Application whitelisting, IT Hygiene tools, Vulnerability assessment all in dashboards and with single lightweight agent		

#	Description	Compliance (Y/N)	Remarks
3	The solution must block fileless attacks, exploitation behaviour, ransomware using indicators of attacks (IOA)/indicator of compromise (IOC)		
4	The solution must identify malicious files and prevent them from execution, including viruses, Trojans, ransomware, spyware, crypto miners and any other malware type.		
5	The solution must identify malicious behaviour of executed files\running processes\registry modifications\ memory access and terminate them at runtime, or raise an alert (exploits, fileless, Macros, etc.).		
6	The solution must support the creation of rules to exclude files based on hash, filename and folders.		
7	The proposed solution shall work on a signature-less mechanism to stop threats without relying on a database to be present at the endpoint		
8	The proposed solution should have capability to track and report movement of all known and unknown malware and malicious activity across the endpoints.		
9	The solution must identify and block/alert on lateral movement		
10	The solution must identify user account malicious behaviour, indicative of prior compromise		
11	The solution must identify, and block memory based attacks, exploit prevention, script protection etc.		
12	The solution must identify malicious interaction with data files.		
13	The solution must identify and block usage of common attack tools such as Metasploit, Empire, Cobalt, Powershell scripts etc.		
14	The solution must have an internal protection mechanism against access and manipulation of unauthorized users.		

#	Description	Compliance (Y/N)	Remarks
15	The endpoint software should support malware tracking and provide visualization at the network level: systems and users affected, patient zero, and method/point of entry.		
16	The solution must generate an intelligence driven detection in the UI.		
17	The solution must continuously collect data on all the entities and their activities within the environment.		
18	The solution must support the display of entity and activity data.		
19	The solution must support and establish real time response connection to endpoints.		
20	The solution must have a user role for real time response attributes.		
21	The solution must blacklist hashes through UI.		
22	The solution must support queries like: Search for the occurrence of process/file/network/user activities across all endpoints in the environment.		
23	The solution must support the means to execute a forensic investigation.		
24	The solution must support isolation and mitigation of malicious presence and activity, locally on the endpoint.		
25	The solution must support isolation and mitigation of malicious presence and activity across the entire environment.		
26	The solution must support and show endpoints in network contained state.		
27	The solution must have built-in vulnerability assessment.		
28	The solution must provide the means to conduct Inventory Management.		

#	Description	Compliance (Y/N)	Remarks
29	The solution must generate inventory report of managed and un- managed assets on a network.		
30	The solution system must support continuous and persistent monitoring of files to detect polymorphic and time bound malware whenever they start turning bad and shall not be only an on-demand scan mechanism		
31	The solution must monitor user accounts including domain and local accounts, standard and administrative accounts.		
32	The solution must support log collection and retention.		
33	The solution must include threat hunting.		
34	Threat hunting alerts should come on same management console as endpoint solution.		
35	The solution must support the discovery of unattended attack surfaces.		
36	The solution must support rapid and seamless installation across all endpoints/servers in the environment.		
37	The solution must support automated distribution on endpoints/servers that were joined to the environment following the initial installation.		
38	The solution must support all commonly used Operating Systems including Windows, MAC, Linux and must be deployed on-premises with no requirement or connectivity to cloud environment		
39	The solution must provide full protection for endpoints and servers that are offline from the organization's network.		
40	The solution must have the ability to rate the severity of security alerts.		
41	The solution must have the ability to specify a list of alert exclusion rules for the selected objects.		

#	Description	Compliance (Y/N)	Remarks
42	The solution must assign a risk score to all objects within the protected environment.		
43	The solution must support the logging of events, alerts and updates.		
44	The proposed solution should have build in API's to support integration with 3rd party systems like SIEM, Firewalls, IPS, Proxy etc.		
45	The solution must collect endpoint, file, process, user activity and network traffic in a fully self-sustained manner.		
46	The solution must support integration with common SIEM solutions.		
47	Endpoint shall be capable of identifying fileless malware and memory based attacks.		
48	The solution must support standardized and customizable reports.		
49	The solution must co-exist with all commodity and proprietary software on the endpoints or servers.		
50	The Solution must have the capability of removable storage protection (block storage devices based on Device ID/ Product Category) and log files written to removable storage devices.		
51	The solution should have Custom Detections capability to serve the goal of delivering robust control to the security administrator by allowing to define custom signatures and enforce blacklists		
52	The solution should have block Malicious Activity Protection provides real-time detection and blocking of abnormal behaviour of a running program on the endpoint, for example, behaviours associated with ransomware		

3.4.3.24 Application Vulnerability Scanner (Web applications, mobile applications and APIs)

#	Description	Compliance (Y/N)	Remarks
1	The proposed solution should detect web application, Host and Network vulnerabilities via crawl/application analysis, stack finger printing, universal translator, normalization, pre-attack analysis, attack, and generating reports after the scan runs. Describe explicitly in details on how vulnerabilities are detected by the solution.		
2	The proposed solution provide coverage for the following technologies but not limited to: a. REST b. WSDL c. JSON d. GWT e. JavaScript f. Mobile g. AJAX h. HTML4 i. HTML5 j. Single Page Applications (SPAs) k. SOAP l. .NET m. Flash Remoting (AMF) n. Silverlight o. Living in the DOM p. Complex Sequences q. CSRF / XSRF Token Tracking r. HTTP/S, FTP, SMTP, and POP3		
3	The proposed solution should support minimally the below mentioned classes of security vulnerabilities: a. Apache Struts 2 Framework Checks b. Apache Struts Detection c. Arbitrary File Upload,		

#	Description	Compliance (Y/N)	Remarks
	d. Autocomplete attribute e. Blind SQL (improved) f. Brute Force (Form Auth) g. Brute Force (HTTP Auth) h. Business logic abuse attacks i. Cookie attributes j. Credentials stored in clear text in a cookie. k. Cross-Site Request Forgery (CSRF) l. Cross-site scripting (XSS), DOM based m. Cross-site scripting (XSS), reflected n. Cross-site tracing (XST) o. Directory Indexing p. Email Disclosure q. Forced Browsing r. Form Session Strength s. HTTP Response Splitting t. HTTP Strict Transport Security u. HTTPS Downgrade v. Information Disclosure w. Information Leakage x. Java Grinder y. OS Commanding z. Parameter Fuzzing aa. Predictable Resource Location bb. Privacy Disclosure cc. Profanity dd. Reflection ee. Remote File Include (RFI) ff. Reverse Proxy gg. Secure and non-secure content mix hh. Server Configuration		

#	Description	Compliance (Y/N)	Remarks
	ii. Session Fixation jj. Session Strength kk. Source Code Disclosure ll. SQL Injection mm. SQL injection Auth Bypass nn. SSL Strength oo. Unvalidated Redirect pp. URL rewriting qq. Web Beacon rr. Web Service Parameter Fuzzing ss. X-Frame-Options missing HTTP header tt. X-XSS-Protection missing HTTP header uu. Z-Customer created attacks vv. Accounts ww. CGI scripts xx. Common Hacker Attack Methods yy. Database zz. DNS services aaa. FTP servers bbb. IP Services ccc. Mail Servers ddd. DOS (Denial of service)		
4	The proposed solution should support scanning of well-known (e.g., those with known CWE entry) and/or unknown vulnerabilities in COTS / OSS and custom developed applications.		
5	The proposed solution should support testing web application for data injection and manipulation, such as SQL injection, buffer overflow, cross-scripting or command injection.		

#	Description	Compliance (Y/N)	Remarks
6	The proposed solution should support testing flow control vulnerabilities, such as forceful browsing and cross site request forgery.		
7	The proposed solution should support testing data disclosure vulnerabilities, such as leakage of PII.		
8	The proposed solution should support testing authentication, such as insufficient authentication and insufficient session expiration.		
9	The proposed solution should support testing general vulnerabilities, such as directory indexing and enumeration, file enumeration, and directory and path traversal.		
10	The proposed solution should support testing other vulnerabilities and flaws, such as session strength analysis and remote active content analysis.		
11	The proposed solution should support reducing the overall testing time of big applications by reducing duplicate attacks. Describe how this works in the solution in detail.		
12	The proposed solution should support the below all mentioned authentication login methods/techniques: a. Simple Form Authentication b. Macro Authentication c. Traffic d. Bootstrap e. Selenium f. Session Hijacking g. HTTP Authentication h. Oauth i. SSL Certificate j. ADAL k. User Accounts and Authorizations i. Account Information ii. Account Integrity		

#	Description	Compliance (Y/N)	Remarks
	iii. Login Parameters l. Password Strength		
13	The proposed solution should support email notifications for: • A scan has failed • A scan is awaiting bootstrap authentication • An on-premises engine has gone offline		
14	The proposed solution should support testing an application with multiple user / role perspectives.		
15	The proposed solution should have capabilities for human- assisted crawling of the application so the scanner can better understand authentication flow.		
16	The proposed solution should have capabilities to teach the crawler how to test and navigate a complex web application. Describe how it works in the solution.		
17	The proposed solution should support Selenium or other web scripting/automation tools. Describe how the solution support as such in details.		
18	The proposed solution should support testing applications that extensively use client-side JavaScript (such as Ajax) and the ability to understand what the JavaScript code is doing - for example, navigating, clicking buttons and providing user input. Describe how testing of client-side code is performed.		
19	The proposed solution should support attacks on JavaScript code that are launched/simulated by the solution. Describe how such attacks are performed.		
20	The proposed solution should support detection of hostile client-side JavaScript code. Describe how such code can be detected.		
21	The proposed solution should support detection of client-side JavaScript vulnerability. Describe how such code can be detected.		

#	Description	Compliance (Y/N)	Remarks
22	The proposed solution should support detection of XSS issue in client-side JavaScript. Describe how such issue can be detected.		
23	The proposed solution should support testing Rich Internet application (RIA) based on Adobe Flash and Flex. Describe how such testing works in the solution.		
24	The proposed solution should support automatically or programmatically generate URLs to crawl auto generated web pages (e.g., sequentially numbered pages, etc.).		
25	The proposed solution should prevent the scanner from entering an infinite loop scanning auto-generated web pages. Describe what mechanism are in place for such.		
26	The proposed solution should have capabilities for human- assisted crawling of the application so the scanner can better understand business logic flow and data types. Describe the mechanisms in place for such.		
27	The proposed solution should be able to test HTML5 applications. Describe how the solution achieves that and which standards the solution could explicitly support and test.		
28	The proposed solution should have the ability to create custom attacks. Please describe how this can be done.		
29	The proposed solution should have the ability to control the max number of findings to cap during the scan to have more predictable scan completion. Please describe how this can be done.		
30	The proposed solution should support testing web-service- enabled applications using Simple Object Access Protocol (SOAP), Web Services Description Language (WSDL), REST and Universal Description, Discovery and Integration (UDDI). Describe how the solution support those mentioned web services testing.		
31	The proposed solution should support parsing of WSDL and REST APIs (Swagger) files. Please describe how the solution achieves that.		

#	Description	Compliance (Y/N)	Remarks
32	The proposed solution should support WS-Security and/or WS-Addressing explicitly.		
33	The proposed solution should explicitly support the use of username tokens when testing web services enabled applications.		
34	The proposed solution should support Autodiscover and test these web services interfaces. Describe how the solution achieves that.		
35	The proposed solution should support testing RESTful-enabled applications using XML-based protocol fuzzing. Describe how the solution achieves that.		
36	The proposed solution should provide generic XML-based protocol fuzzing and/or testing? Describe how the solution does that.		
37	The proposed solution should provide JSON testing. Describe how the solution does that.		
38	The proposed solution should have the ability to be programmed to test custom in-house web protocol. Describe how can the solution achieve that.		
39	The proposed solution should not control number of project/apps to be configured as long it falls within the solution licensing limit, i.e., FQDNs		
40	The proposed solution should have options to reduce the risk that minimum disruptions to service are caused when testing/performed against production applications. Describe how can the solution achieve that.		
41	The proposed solution should have the ability for determining code coverage completeness of your testing solution - to understand and highlight areas of the application that were not covered with the testing. Describe how can the solution achieve that.		
42	The proposed solution should have options for a "quick scan" to get started, determine correct functioning, and so		

#	Description	Compliance (Y/N)	Remarks
	on, versus a deep full scan? Describe how can the solution achieve that.		
43	The proposed solution should have the ability to allow a mix of attack modules to be configure in a single attack template and allowing it to be reusable in different scan configuration with minimum changes. Describe how can the solution achieve that.		
44	The proposed solution security testing should satisfy regulations and provides the below types of reports. Describe how can the solution achieve that. a. Payment Card Industry (PCI) b. OWASP 2017 ~~c. Sarbanes-Oxley (SOX)~~ ~~d. Health Insurance Portability and Accountability Act (HIPAA)~~ ~~e. GDPR~~ PDPA 2022		
45	The proposed solution security testing should provide high- level executive reporting summarizes the overall health through the analysis of vulnerability severity, type, status and a variety of other metrics. Below is the required health overview (but not-limited to): a. Scan Statistics b. Top 10 Vulnerability Types c. Most Common Vulnerability Severity d. Most Common Vulnerability Status		
46	The proposed solution security testing should provide a high- level overview of your apps and vulnerabilities, without using external tools. Below is the required overview (but not-limited to): a. Number of Apps, Scans and Vulnerabilities b. Vulnerabilities By Status c. Vulnerabilities By Severity d. Apps With Most Vulnerabilities e. Top Vulnerability Types		

#	Description	Compliance (Y/N)	Remarks
	f. Running Scans g. Failed Scans h. Completed Scans i. Scheduled Scans j. Interrupted Scans k. Scan Usage by Month l. Apps Scanned This Month		
47	The proposed solution should provide the ability to execute retests of single vulnerabilities against previously discovered items once they are believed to have been remediated.		
48	The proposed solution should allow developers to quickly replicate discovered vulnerability without retesting the entire application. Describe how can the solution achieve that.		
49	The proposed solution should allow developers to quickly compare attacks performed and highlight differences between them. Describe how can the solution achieve that.		
50	The proposed solution should allow developers to edit parameters to request URL on the headers visually on editor before launching retest again. Describe how can the solution achieve that.		
51	The proposed solution should provide a record or replay capability of vulnerabilities discovered so that the exploitation of a vulnerability can be replayed by the developer investigating the issue or later by information security to ensure the vulnerability has been addressed when retesting.		
52	The proposed solution should support sequence auto detection and CSRF token detection. Describe how can the solution detect such.		
53	The proposed solution should have ability to handle Single Page Application's (SPA's).		

#	Description	Compliance (Y/N)	Remarks
54	The proposed solution should support testing Flash remoting sites (AMF).		
55	The proposed solution should provide the ability to attack workflow processes within an application. Please describe how it can be done.		
56	The proposed solution should produce logic-flow and data- flow analysis that could help find design flaws that cause security vulnerabilities. Describe the logic flaws analysis the solution detect.		
57	The proposed solution should support data-flow analysis capability span applications that run on different platforms written in different languages. Describe how the solution achieves that.		
58	The proposed solution shall provide Network based vulnerability assessment to perform automated, distributed or event driven probes of geographically dispersed network services, operating systems, routers/switches, mail servers, web servers, firewalls and applications and display scan results and remediation information.		
59	Perform policy compliance and report security vulnerabilities, based on standard security practices across the enterprise.		
60	Network and Server Settings: a. Network Vulnerabilities b. OS Patches c. System Auditing d. Services e. File System and Directories f. File Attributes g. File Access h. Registry Permissions		

#	Description	Compliance (Y/N)	Remarks
61	The proposed solution should have the ability to test mobile applications designed for use on mobile devices (android/ IOS). Describe how the solution does that.		
62	The proposed solution should have ability to analyze traffic between the mobile app and web server and/or ability to analyze web application/service that communicates with mobile app. Describe how the solution does that.		
63	The proposed solution should have the ability to traffic analysis mobile application. Describe the solution support that.		
64	The proposed solution should demonstrate evidence that your vulnerability detection is accurate. How does the solution achieve that		
65	The proposed solution should ensure the testing accuracy to reduce false positives. Describe any specific techniques/tuning are applies.		
66	The proposed solution should ensure the testing accuracy to reduce false negatives. Describe any specific techniques/tuning are applies.		
67	The proposed solution should be safe to scan Production environments. Please describe what had been done in the solution to achieve that.		
68	The proposed solution should support floating licenses between users (not locked to an individual user or MAC address).		
69	The proposed solution should support licenses with FQDNs with no limits to the number of scans to it.		
70	The proposed solution should minimally provide the following centralized control of scanning programs: a. User access control and permission levels b. Scheduling Blackout periods		

#	Description	Compliance (Y/N)	Remarks
71	The proposed solution should provide a rating scale and rating mechanism for detected vulnerabilities. Is it a proprietary rating or a standard/universally adopted one?		
72	The proposed solution provides the ability to manually assign/reassign the priority/severity rating that the application scanner has assigned a given vulnerability.		
73	The proposed solution should provide report can help a developer quickly focus on the highest severity, highest confidence issues.		
74	The proposed solution should identify the relevant Web page and URL where the vulnerability was detected. Please describe how this can be achieved.		
75	The proposed solution should support scanning of REST and SOAP APIs.		
76	The proposed solution should provide an API interface for integration and expansion. a. App Operations b. Attack Templates Operations c. Blackout Operations d. Engine Groups Operations e. Engines Operations f. Files Operations g. Scan Config Operations h. Scans Management i. Schedules Management j. Perform Search Operations k. Targets Operations l. Vulnerabilities Operations m. Vulnerabilities Comments Operations		
77	The proposed solution should help developers mitigate vulnerabilities earlier in the SDLC process. Please describe how can this be possible.		

#	Description	Compliance (Y/N)	Remarks
78	The proposed solution should have the ability to integrate with security information and event management (SIEM) systems. Describe how can the solution achieve that.		
79	The proposed solution should provide (or link to) remediation advice. Describe remediation advice comes in what format.		
80	The proposed solution should follow specific sources of advisory to determine web vulnerabilities. List those sources (i.e., OWASP, etc.).		
81	The proposed solution should have ability to perform testing different web applications within the same engine/installation.		
82	The proposed solution should have ability to scan even without on-premises scan engines installed by default.		
83	The proposed solution should have ability to scale horizontally in term of scan engine and yet able to consolidate results back.		
84.	Perform Dynamic Application Security Assessment or behavioral testing of the application.		
85	Perform authenticated and unauthenticated assessment including complex authentication such as use of OTP and CAPTCHA		
86	Assess underlying IT infrastructure for vulnerabilities		
87	Integrates with web browsers or other applications to support applications' browser compatibility.		
88	Provide controlled testing environment such as limiting attack parameters, non-invasive testing, limit packet injection in network etc.		
89	Facilitate regeneration of the vulnerability and provide feature to validate the results and identify false positives.		
90	Generate logs for scanner access and testing.		

#	Description	Compliance (Y/N)	Remarks
91	Provide detailed report as spreadsheet, PDF and HTML format, customizable as per the requirement and comparable to previous assessment.		
92	Should support periodic vendor updates for patches and attack signatures.		
93	The solution should provide reports from previous assessments.		

3.4.3.25 Network Vulnerability Scanner

#	Description	Compliance (Y/N)	Remarks
1	Ability to perform vulnerability assessment of all IPs internal / external.		
2	Ability to schedule periodic vulnerability scans as well as manual scans when necessary.		
3	Perform vulnerability scans on complex IT infrastructure even with overlapping IP addresses.		
4	Send an alert when a scan is scheduled, started, completed or interrupted.		
5	Can provide domain wise (server type, device type, network, VLAN etc.) comparable reports with respect to the previous scans.		
6	Identify vulnerabilities in range of devices such as routers, firewalls, Linux servers, windows servers, Linux workstations, windows workstations, Apple workstations etc.		
7	Should support plugin updates, maintenance, etc. for the specified period.		
8	Provide detailed description, risk ratings, recommendations and workarounds for the identified vulnerability.		
9	Review security configurations of the infrastructure with respect to Industry Best Practices and benchmarks		

10	Solution should have functionality to integrate with SIEM		
11	Identify and suggest missing patches.		
12	Provide detailed report as spreadsheet, PDF and HTML format, customizable as per the requirement		
13	Support for exploit capabilities and threat intelligence.		

3.4.3.26 Network Detection and Response (NDR)

#	Description	Compliance (Y/N)	Remarks
1	Analyse raw network packet traffic in real time or near real time.		
2	Monitor and analyse north/south traffic (as it crosses the perimeter), as well as east/west traffic (as it moves laterally throughout the network)		
3	Identify normal network traffic and highlight suspicious traffic that falls outside the normal range		
4	Offer behavioural techniques (non-signature-based detection), such as machine learning or advanced analytics in addition to signature based techniques that detect network anomalies.		
5	Provide automatic or manual response capabilities to react to the detection of suspicious network traffic		
6	Uses real-time analytics, AI and machine learning on wire data to detect known and unknown security incidents		
7	Automatically discovers and classifies device and set up device groups based (critical assets, workstation, etc.)		
8	The solution must be agentless		
9	The solution must automatically identify and classify threats, including attack phase and risk, without requiring any intervention.		
10	Solution must be able to Differentiate key assets from other hosts for risk prioritization		
11	Automatically score and prioritize each individual attacker behavior detected		
12	Automatically score and prioritize each host/account based on its behaviors over time.		

#	Description	Compliance (Y/N)	Remarks
13	The solution must have the notification capabilities for the detections.		
14	The solution should leverage both packet capture and flow based technologies		
15	Ability to detect threats within encrypted traffic (NO decryption capabilities are required).		
16	Solution should secure the data center within the virtual environment as well as the underlying infrastructure.		
17	Ability to perform matching on IOCs.		
18	The Solution should have the capabilities to be integrated with proposed SIEM solution		
19	The solution should integrate with proposed EDR, also have an API capable of integrating with others when needed.		
20	Detect the following type of threats (not limited to): a. Remote access tunnels used by attackers to control compromised systems b. Hidden tunnels over HTTP, HTTPS, or DNS to communicate with C&C or to exfiltrate data c. Web-based Command and Control (not relying on IP reputation or threat lists) d. Relay hosts. e. Malware replicating a payload to / exploiting vulnerabilities against other hosts f. TOR Anonymization g. Peer -to -peer traffic h. Botnet monetization behaviours: Click Fraud, Bitcoin Mining, outbound DoS, outbound SPAM i. Ransomware activity: encrypting file shares j. Network reconnaissance scans: port scans, port sweeps, scanning unused IPs. k. Privilege anomaly: to find use case such as realter Privilege escalation, accounts take over, brute force, credentials theft and misuse etc. - Use of a credential from a host it has not previously been used on l. Use of a credential from its normal system, but asking for unusual services or in excessive volume		

#	Description	Compliance (Y/N)	Remarks
	m. A host trying many credentials to attempt to gain access to a server n. Kerberos service scans o. Fake Kerberos servers p. Brute force attacks. q. Use of administrative protocols, such as RDP, SSH, IDRAC, and IPMI, where the target host is not typically administered by the source host on that protocol r. A host exfiltrating data to an unusual destination s. A host gathering unusual volumes of data and then sending exfiltrating to an external IP t. A host being used as a relay to exfiltration data to an external system" u. Ability to detect enumeration of file shares v. Ability to detect AD/LDAP reconnaissance using techniques similar to Bloodhound w. Ability to detect use of PowerShell/WMI and RPC to move laterally via remote code execution x. Ability to detect reconnaissance of RDP servers. y. Ability to detect the use of remote administration tools to move laterally via SMB. z. Ability to detect anomalies for protocols		
21	Even if the license exceeded, the NDR platform must work normally from technical perspective		
22	Solution must be able to forward the Network security Metadata to an existing Data Lake or SIEM. Or can Use Its own HW for on-prem storage.		
23	The solution should provide ability to establish “normal” traffic baselines through flow analysis techniques and the ability to detect deviations from normal baselines.		
24	Unsupervised and supervised machine learning along with probabilistic mathematics without predefined rules and signatures should be employed by the solution to detect significant anomalies and drifts in user, device or network activities and traffic that signal an attack.		
25	The solution should be able to get threat intelligence from research team to make detections of malware activity with higher accuracy and efficacy including Botnets, C&C servers, Bogons, Tor Entry/Exit Nodes, Connections to bad reputation Nations and Dark IPs..		

#	Description	Compliance (Y/N)	Remarks
26	The solution should be able to combine/stitch the flow records coming from different network devices like routers/switches/firewall/endpoints/NAT gateway that are associated with a single conversation and present them as a single bi-directional flow record including traffic traversing NAT devices.		
27	The solution components must be separated for raw traffic sensor, telemetry processing, telemetry storage, traffic replication and management functions and not all-in-one appliance for ideal performance.		
28	The solution must store processed telemetry in a redundant fashion on a clustered N+1 database scalable such that data is accessible for querying and reporting even in the case of a failure of the telemetry processing component.		
29	The solution must be able to consume flow information from the network in the form such as Netflow V5, Netflow V9, IPFIX, sFlow, Jflow, cFlowd, NSEL as well as port-mirrored traffic to perform behavioural analysis.		
30	The solution should detect common anomalous events like Scanning, Worms, Unexpected application services (e.g., tunneled protocols, backdoors, use of forbidden application Protocols), Policy violations, etc.		
31	The solution should utilize anomaly detection methods to identify attacks such as zero-day exploits, self-modifying malware, attacks in the ciphered traffic or resource misuse or misconfiguration.		
32	The solution should support the capability to identify network traffic from high risk applications such as file sharing, peer-to-peer, etc.		
33	The solution should be capable of detecting fake applications, traffic using incorrect ports/protocols, the use of forbidden application protocols etc.		
34	The solutions should provide the capability of behavioural analysis on a dynamic custom user-defined relationship between groups of network assets based on certain parameters like services, protocols and events etc.		
35	The solution should have the ability to state fully reassemble unidirectional flows into bi-directional conversations; handling deduplication of data and asymmetry and eliminate redudant telemetry to improve system performance.		

#	Description	Compliance (Y/N)	Remarks
36	The solution should provide compliance use cases to identify usage of insecure, legacy and deprecated encryption algorithms being used by servers on the network.		
37	The solution should be capable of providing visibility of east-west traffic in an encapsulated network of ACI / SDA fabric by decapsulating the overlying VxLAN headers to track endpoints.		
38	The solution should Integrate with Identity management or other equivalent solutions to provide user Identity information in addition to IP address information throughout the system. It should allow creation of user groups based on Identity & provide mapping of User Name to IP address on a device.		
39	The behaviour analytics solution should be a dedicated solution supporting out of box machine learning algorithms and not a subset capability of SIEM or Forensic analysis.		
40	The solution should have capability to assign risk and credibility rating to alerts and hosts and present critical high fidelity alerts prioritized based on threat severity with contextual information on the dashboard.		

*3.4.3.27 DNS, DHCP, IPAM**

S.No	Description	Compliance (Yes/No)	Remarks
1	The solution shall be integrated system incorporating DNS, DHCP, IP Address Management and Security capabilities in a single platform.		
2	The solution shall have a clear separation between Management and Service layers.		
3	The solution shall be a scalable platform capable of managing an unlimited number of DNS/DHCP servers and IP addresses from a single management core.		
4	The solution shall permit adding DNS/DHCP servers without the need to change the architecture or deploy additional management cores.		
5	The deployment of additional managed servers shall not require supplementary licenses on the management layer.		
6	The solution shall not generate excessive control messages/synchronization traffic between components.		

7	The solution shall provide a web-based user interface presenting a unified view of all DNS, DHCP and IPAM data regardless of where it resides on the network.		
8	The solution shall provide a granular access rights model with five levels of access: Hide, View, Change, Add, and Full Access.		
9	The solution shall provide built-in change request workflows allowing delegating administration tasks to various users/user groups while enforcing a formal approval process.		
10	The solution shall provide a pre-deployment data validation mechanism to prevent syntactical and logical configuration errors from being pushed to the managed DNS/DHCP servers.		
11	The solution shall support a referential data integrity model that will ensure that no configuration change will result in orphaned objects or incompatible data leading to outages.		
12	The solution shall provide extensive auditing capabilities on all database objects including user login sessions.		
13	The solution's management system must support performing database backups on demand or scheduled with the ability to write backup files to the local server or to a remote server using FTP or SFTP.		
14	The solution's shall provide LDAP integration enabling importing Active Directory groups and using AD credentials for sign-on.		
15	The solution shall allow pass-through authentication using 3rd party authenticators such as LDAP, Kerberos, RADIUS, RSA SecurID, Oauth API authorization, SAML-based Web Single Sign-On and TACACS+.		
16	The solution shall provide monitoring the status of essential services running on the management and services such as CPU utilization, memory utilization, network card interface utilization, disk space utilization and DNS/DHCP performance metrics per service.		
17	The solution shall include containers that provide access to management features such as favourites, tasks, workflow requests, server statistics and quick actions.		
18	The solution should support multiple configurations to maintain different networks with the ability to create isolated environment supporting multi-tenancy capabilities.		
19	The solution shall have the ability to generate scheduled reports and with the following supported formats: PDF, HTML, CSV, XLS or RTF.		
20	The solution shall have the ability to add custom logo to the reports with support for JPEG or GIF format.		
21	The solution shall provide high availability scheme that includes application layer clustering, database replication and failover to a secondary or tertiary server.		

22	The solutions IP Address Management system shall natively integrate with the DNS/DHCP service layer and enable full configuration and control of managed servers.		
23	The solution should be able to concurrently manage disparate versions of DNS/DHCP servers.		
24	The solution shall have the ability to manage both IPv4 and IPv6 blocks, networks and IP addresses.		
25	The solution should provide the ability to create discrete IP infrastructure models with overlapping IP spaces that can co-exist in the system in separate configuration spaces.		
26	The solution should provide network templates that include pre-configured settings such as default gateways, DHCP ranges, host records, and DNS/DHCP deployment options.		
27	The solution should provide multi-layer IP Block hierarchy allowing grouping IP address space into logical containers to make the data more manageable.		
28	The solution should provide a built-in IP discovery engine capable of using both proprietary and non-proprietary discovery protocols in order to collect network information for both on premises and cloud based networks.		
29	The solution should support the addition of user-defined fields to IPAM objects.		
30	The solution should support adding user-defined fields to each of the management object types to capture and track information associated with each unique object.		
31	The solution should user-defined fields such as: Text, Date, Boolean, Integer, Long, Email Address, URL and Workflow etc.		
32	The solution should be capable of performing the following roles: DNS Authoritative, DNS Recursive, and DHCP server.		
33	The solution DNS Services should support the following roles: master, slave, caching, forwarding, and stealth.		
34	The solution DNS Services should support both IPv4 and IPv6 with tracking of dual-stacked addresses.		
35	The solution DNS Services should support DNS64 for integration with NAT64.		
36	The solution DNS Services should provide secure zone transfers using TSIG or equivalent encryption standards.		
37	The solution DNS Services should support Response Policy Zone definition and accept threat updates via security feeds.		
38	The solution DNS Services should support DNSSEC security extensions with several signature digest and key signing algorithms.		
39	The solution DNS Services should provide a DNSSEC key management mechanism supporting different rollover policies for each type of key.		

40	The DNS service shall support DNS traffic steering to facilitate DNS resolution from different sets of DNS resolvers in an agentless fashion. For example, Internet breakout for SaaS solutions such as Office 365.		
41	The solution DHCP service should support IPv4 and IPv6 addresses.		
42	The solution DHCP service should support standard, advanced, vendor-specific, and custom options for both DHCPv4 and DHCPv6.		
43	The solution DHCP service should provide Dynamic DNS updates secured using TSIG and GSS-TSIG or its equivalent .		
44	The solution DHCP service should be able to filter DHCP requests by specific identifiers, custom and complex match statements.		
45	The solution DHCP service should be streamlined to reduce deployment times and near-zero downtime DHCP without service interruptions or DHCP service restart.		
46	The solution DHCP service should be capable of generating alerts when dynamic address usage within a DHCP range or shared network is unusually low or exceptionally high.		
47	The system has the capability to collect the protocol level DHCPv4 DORA and DHCPv6 SARR broadcast operations.		
48	The solution shall support the creation of multiple policies, policy types, and policy hierarchies to support a wide range of control objectives related to DNS traffic.		
49	The solution shall be capable of integrating with multiple threat intelligence (TI) sources to be used for policy enforcement.		
50	The solution shall allow for the automatic ingest of custom TI from internal sources as well as public sources.		
51	The solution shall provide various policy outcomes including Allow, Block, Monitor, and Redirect for DNS queries.		
52	The solution shall support automatic action (Block, Monitor, Redirect) on threats detected via threat analysis and analytic processing.		
53	The solution shall support the whitelisting of DNS domains for extended IoT devices the estate.		
54	The solution shall perform threat analysis on all DNS queries in real-time to detect:		
55	DNS Tunneling (a common form of data exfiltration and/or malware Command & Control communications)		
56	Domain Generation Algorithm (DGA) abuse, which is a common approach to masking the location and activity of Command & Control servers		
57	Significant changes in DNS activity, thus detecting events such as distributed denial of service (DDoS) attacks		
58	Divergence from learned historical patterns of a client by analyzing geographic patterns of usage		

E	DNS query activity that diverges from standard practices (e.g. clients querying MX records which should only be done by mail servers, or high number of TXT records being queried which may indicate DNS Tunneling)		
55	The solution shall have the ability to provide a security event feed to be used by ticketing or alerting systems, such as Security Information and Event Management (SIEM) systems.		

3.4.3.28 SOC/NOC -Desktop

#	Criteria	Description	Compliance (Y/N)	Remarks
1	Brand	Bidder to specify. All relevant brochures must be submitted		
2	Model	Bidder to specify		
3	Country of Origin & Country of Manufacture / Assembly	Bidder to specify		
4	Processor	Option 1: Intel® Core i5-10400 10th Generation Processor or Later		
		Option 2: AMD Ryzen™ 5 4600G Processor or Later		
5	Base Frequency	Intel: 2.9GHz or Higher AMD: 3.7GHz or Higher		
6	Cache	Intel: 12MB or Higher AMD: 11MB L2/L3 Cache or Higher		
7	Video Controller	Intel UHD Graphics 630 / Radeon™ Vega 11 Graphics or Better		
8	Form Factor	Business Desktop		
9	Chassis	Mini ITX or Micro ATX Tower Casing		
10	Chipset	Intel: Intel Express B / H Business 400 Series Chipset or Higher AMD: AMD B Chipset or Higher Note: Bidder should clearly specify the chipset		

#	Criteria	Description	Compliance (Y/N)	Remarks
11	Motherboard	Should be the same quoted brand (Serial number of the CPU should show in BIOS)		
12	Memory	32 GB DDR 4 2666MHz or Higher		
13	Maximum Memory	Upgradeable to Maximum of 64 GB RAM		
14	Memory DIMM's	2 DIMM's		
15	Hard Disk Drive	1TB Serial ATA Minimum		
16	Keyboard	128 Key Standard Keyboard to be as same brand in English		
17	Mouse	Two buttons with scroll wheel optical Mouse with Mouse Pad		
18	Optical Drive	SATA DVD Drive (+/-RW)		
19	Expansion Slots	Minimum 2 Expansion Slots including 1 Nos PCI x 16, (Specify)		
20	Network Interface	Gigabit Ethernet Network Interface Card (10/100/1000) Internal Wi-Fi Card - USB Dongle is not accepted		
21	I/O Ports	Minimum 8 USB Ports; from that at least 2 USB Ports should USB 3.2 – Minimum 1 HDMI Port and 1 VGA Port		
22	Power Supply	250W PFC, auto-sensing, 80 PLUS# Platinum, or higher Power Supply		
23	Operating system	Windows 10 Pro (Required license should be included)		
24	Product certifications of the quoted Model	Product certifications of the quoted Model Energy Star or any other equal certificate to Energy Star issued by authorized body who has the authority to do so (Documentary evidence must be provided)		

#	Criteria	Description	Compliance (Y/N)	Remarks
		Valid ISO 9001: 2015 and ISO 14001:2015 Offered Model must possess FCC or CE or Equal		
25	Display	19.5" Widescreen Color LED Monitor supporting resolutions WXGA or better. Should be as the same brand of the Desktop		
26	Manufacture Experience	The manufacturer should have a minimum of 3 years' experience in manufacturing the same brand. (Proof document should be attached)		
27	Manufacturer Authorization Certificate	Manufacturer Authorization Certificate should be provided. (Originals should be provided on request)		
28	support and maintenance	Comprehensive on-site manufacturer authorized support and maintenance for 36 months (Labour & Parts) Excluding Consumes a. Bidder or its parent company or its subsidiary should have Island-Wide owned branch network b. Documentary evidence to be provided of the following under bidders' name, Address, Contact Details & Date of Commencement of each branch/regional office (Should have completed minimum of 5 years from the Date of Commencement of each branch/regional office)		
29	Brochure	Supplier should provide original brochure of make/model quoted as per above specification		

3.4.3.29 SOC / NOC - Laptop

#	Criteria	Description	Compliance (Y/N)	Remarks
1	Make & Model	Bidder to specify. All relevant brochures must be submitted		
2	Country of manufacture	Bidder to specify		
3	Country of origin	Bidder to specify		
4	Form Factor	Business Laptop Computer (Manufacture Confirmation must be attached)		
5	Chipset	Intel: Q370 Chipset or higher or equivalent AMD chipset		
6	Processor	Option 1: Intel® Core i7-1165G7 11th Generation Processor with IPU or Later Option 2: AMD Ryzen™ 7 5800U Processor or Later		
7	Processor Frequency	Intel: 4.70GHz Max Turbo Frequency or Higher AMD: 1.9GHz Base Frequency or Higher		
8	Cache	Intel: 12MB or Higher AMD: 20MB L2+L3 Cache or Higher		
9	RAM	16 GB of DDR4 System Memory, Upgradable to 32 GB or Higher Capacity		
10	RAM Speed	2666 MHz, DDR4 or Higher		
11	Hard Disk	1TB SSD or Above		
12	Graphics	Intel UHD Graphics / AMD Radeon™ Graphics or Better		
13	Keyboard	Keyboard with Touch Pad		
14	Touch Pad	Multi-Gesture Touchpad, Supporting Two-Finger Scroll		

#	Criteria	Description	Compliance (Y/N)	Remarks
15	Audio, Audio Integrated Speakers, Microphone	Integrated High-Definition Audio, Integrated Internal Speakers, Built-In Microphone		
16	Communications, Modern Ethernet, Wireless Bluetooth	WLAN: 802.11ac, WPAN: Bluetooth 4.0		
17	Inbuilt Camera	720p HD Camera		
18	Expansion Options, PC Card I/O Ports	SDTM Card reader, Microphone / Earphone - In jack, USB 2.0 Port, 2 x USB 3.0 Ports, HDMI® Port, DC-In Jack for AC adapter, Fingerprint Reader		
19	Display Type	Option 1: 14 Inch TFT LCD HD Resolution Option 2: 15.6 Inch TFT LCD HD Resolution		
20	Quality Stability and Reliability Tests of the Product Quoted	The quoted product should possess test reports of the following, Spill-resistant keyboard to Provides protection against water spillage. (Should provide lab test as proof)		
21	Operating System	Windows 10 Pro (required licence should be included)		
22	Battery	Minimum 8 Hours Battery Life (Specify Type / mAh / Hours)		
23	Security	Kensington Lock Slot		
24	Accessories - The Carrying Bag	Should be Same Brand		
25	Product certifications of the quoted Model	Energy Star or any other equal certificate to Energy Star, issued by authorized body who has the authority to do so, Documentary evidence must be		

#	Criteria	Description	Compliance (Y/N)	Remarks
		provided. Valid ISO 9001: 2015, and ISO 14001:2015		
26	Manufacture Experience	The manufacturer should have a minimum of 3 years' experience in manufacturing the same brand. (Proof document should be attached)		
27	Manufacturer Authorization Certificate	Manufacturer Authorization Certificate should be provided (Originals should be provided on request)		
28	Support and Maintenance	Comprehensive on-site manufacturer authorized support and maintenance for 36 months (Labor and Parts) Excluding Consumes. Bidder or its parent company or its subsidiary should have Island wide owned branch network Documentary evidence to be provided of the following under bidders' name. (a) Address, Contact Details and Date of Commencement of each branch/regional office (Should have completed minimum of 5 years from the Date of Commencement of each branch/regional)		
29	Additional Conditions	1-year support and maintenance for Battery and Power Adapter		
30	Support and Maintenance Information	A sticker with		
		a. Supplier name		
		b. Contact Numbers		
		c. Date of Commissioning of Hardware		
		d. Support and Maintenance period		
		On all Laptops		
31	Brochure	Supplier should provide original brochure of make/model quoted as per above specification		

3.4.3.30 SOC / NOC – Monitor

#	Criteria	Minimum Requirement	Compliance (Yes/No)	Remarks
1	Technology	LED or better		
2	Brand	(Specify)		
3	Model	(Specify)		
4	Country of Origin	(Specify)		
5	Year of Manufacture	(Specify)		
6	Screen Size	22 inch		
7	Panel type	(Specify)		
8	Resolution	1920 x 1080 (Full HD)		
9	Aspect Ratio	16:9		
10	Colour support	16.7 million colors		
11	Refresh rate	50Hz		
12	I/O	01 HDMI 01 VGA		
13	Accessories	01 HDMI cable should provide 01 VGA Cable should provide Monitor Stand		
14	Power Supply	AC 100~240V 50-60Hz		
15	Weight	(please mention)		
16	Size	(please mention) W*D*H		
17	Manufacturer	The manufacturer should have a minimum of 3 years' experience in manufacturing the same brand. (Proof document should be attached)		

#	Criteria	Minimum Requirement	Compliance (Yes/No)	Remarks
18	Manufacturer Authorization Certificate	The Manufacturer Authorization Certificate should be provided. (Originals should be provided on request)		
19	Support and Maintenance	Comprehensive on-site manufacturer authorized support and maintenance for 36 months (Labour & Parts) Excluding Consumes.		
20	Brochure	Supplier should provide brochure of Make / model quoted as per above specification		

3.4.3.31 SOC / NOC – UPS

All the electronic devices in SOC will share the proposed UPS. Similarly, all the electronic devices in NOC will share the proposed UPS

#	Criteria	Minimum Requirement	Compliance (Yes/No)	Remarks
1	Brand	(Specify)		
2	Model	(Specify)		
3	Country of Origin & Country of Manufacture / assembly	(Specify)		
4	Manufactured Year	(Specify)		
5	Capacity	650VA		
6	Input Voltage	140 - 300V 5VAC		
7	Frequency	50Hz		
8	Phase	Single + GND		
9	Output Voltage	230VAC +10% -10%		

#	Criteria	Minimum Requirement	Compliance (Yes/No)	Remarks
10	Battery Mode	230VAC 10%		
11	Frequency	50Hz 1Hz (Battery Mode)		
12	Waveform	-Simulated Sine Wave (Battery Mode) -Sine Wave (AC Mode)		
13	Transfer Time	2ms 2-6ms		
14	Battery Type	12V/7 AH — 1pc		
15	Backup Time	7 ~ 20 minutes depending on load		
16	Recharge Time	90% capacity after 8 hours		
17	Surge Protection	Yes		
18	Overload	Line Mode 100 ~ 120% 5mins change to fault mode, 120% change to fault mode immediately		
19	Battery Management	-Battery Mode 100 ~ 102% 5 secs shutdown, 120% -Prevent overcharging		
20	Alarm	Yes		
21	General Noise Level	40dB		
22	Temperature	0°C ~ 40°		
23	Humidity	0 ~ 95% relative humidity		
24	Power Factor	Up to 0.7		

3.4.3.32 PABX

#	Item	Minimum Specification	Compliance (Y/N)	Remarks
1	Make	Specify		
2	Model	Specify		
3	Country Origin	Specify		
4	Country of Manufacture	Specify		
5	Year of Manufacture	Specify		
6	Concurrent Calls	Up to 5		
8	IP phone Registers / Extensions	Up to 10		
9	Recording & Voicemail	Up to 5 recording and 10 voice mail		
10	System should be able handle 15 SIP sessions with expandability to 50 on concurrent. Also, system should have at two interfaces to terminate SIP trunks from SIP service Provider			
11	System Should have High Availability, Auto backup and archive mechanism			
10	Communications, Modern	LAN, WAN		

#	Item	Minimum Specification	Compliance (Y/N)	Remarks
	Ethernet, Wireless			
12	Storage Option	Internal		
13	Audio In/Out	Optional		
14	Power Requirements	Input 220 ~ 240V AC		
15	Standard	SIP 2.0,		
16	Support Protocols	SIP 2.0, TCP/IP, UDP/RTP/RTC, HTTP, , ARP, DNS, DHCP, NTP/SNTP, ,		
17	Support Audio Codec	G.711-Ulaw, G.711-Alaw, G.722, G.726, G.729/G.728,		
18	Voice Processing	DTMF detection & generation, RFC 4733, SIP info, In-band & auto		
19	Network Features	DDNS client, DHCP server/ SNMP (latest)		
		IEEE 802.1Q of VLAN, IP assignment (DHCP/Static)		
		IPv4, IPv6, The solution should be compatible to connect agents over internet.		
20	Security Features	The system should support SRTP, AES256/higher, SSH and TLS(latest). . Remote agents should get connected via firewall and the traffic should be encrypted. The firewalls in HA required for this setup needs to be factored.		
		SIP Register with UDP/TCP/TLS(Latest)		
		Phone Auto-Provision		
		Agent initiated One Touch Recording		
21	PABX Features	Mobility Extension		
		Black List		

#	Item	Minimum Specification	Compliance (Y/N)	Remarks
		BLF (Busy Lamp Field)		
		CDR (Call Detailed Record)		
		DID (Direct Inward Dialing)		
		DOD (Direct Outward Dialing)		
		DISA (Direct Inward System Access)		
		DNIS (Dialed Number Identification Service)		
		SRTP (Secure Real-time Transport Protocol)		
		Call Back, Call Forward, Call Group, Call Hold		
		Call Paging and Intercom		
		Call Park, Call Pickup, Call Queue, Call Record, Call Route		
		Blind Transfer, Attend Transfer		
22	Call Features	Call Waiting, Caller ID, Dial by Name, Customized IVR,		
		On-hold Music, Call Transfer		
		Three-way Conferencing,		
23	Proposed Help desk solution should integrate with proposed Call center System and CRM etc.			
24	Should support SMS and email integration			

#	Item	Minimum Specification	Compliance (Y/N)	Remarks
25	System Should support user level and supervisor level privileged access levels			
26	Should have Automatic Call Distribution or Uniformity Call Distribution with Skilled based routing			
27	Dashboard / Wall board			
28	Should have Interface for IT Help desk Call Centre statistics like Total calls per day, Live calls, Calls in IVR, Calls in queue, Calls ringing at agents, Agents on calls, Total incoming calls, answered & dropped per day, Free agents, Agents in breaks - summary and details with health checker			
29	Should have minimum 3 language selection (Sinhala, Tamil and English)			

#	Item	Minimum Specification	Compliance (Y/N)	Remarks
30	Should have Auto day / night mode selection			
31	Should have Holiday calendar to mark full or half day holidays			
32	Should have black list table and authorized agents or supervisors be able add/ edit or delete as necessary			
33	Should have user configurable IVR menus, and to defined automatic call diversion to specific IVR options			
34	Reports	3 Years Comprehensive support and maintenance		
35	Should provide Answered / missed / Abandoned calls in detailed and summaries			
36	Should provide date/ticket number wise detailed and summaries			
37	Should provide IVR breakdown and related user			

#	Item	Minimum Specification	Compliance (Y/N)	Remarks
	required customized reports			
38	Should provide Agent / group performance			
39	Should provide Agent login / logout / breaks			
40	Should provide Hourly call count, Call Gap reports			
41	Product certifications of the quoted Model			
42	Manufacturer Authorization Certificate			
43	Support and Maintenance			

3.4.3.33 IP Phones

#	Description	Specification Sheet	Compliance (Y/N)	Remarks
1	Make			
2	Model			
3	Brand			
4	Sip accounts			
5	Display Type	Colour		
6	Screen size (or should mention specify)	800 x 400 pixel or better WVGA Colour dis- play with 5" or higher diagonal screen		

#	Description	Specification Sheet	Compliance (Y/N)	Remarks
7	Call indicators	Sound & Notification Light		
8	Call features	Call Forward Call Transfer Call Waiting Hotline Call Hold Call time Auto Answer Redial Mute DND 03-Way Conferencing Speed Dial Local Phonebook On hook dialing		
9	Hands free	Full duplex speaker phone		
10	Programmable (Soft) keys	4		
11	Feature keys	Transfer Conference Hold Redial Options Directory Mute Volume controls		
12	Handset	Wired & Bluetooth headset (must provide)		
13	Connectivity	For the wired connectivity, Should have a minimum of 2 x 100/1000 BASE-Tx Ethernet ports, one for the LAN connection and the other for connecting to PC/laptop & Wi-Fi (IEEE 802.11b/g/n)		
14	Interfaces	2 * RJ 45 (Input & out- put for PC) 1 * headphone jack		
15	Power interfaces	PoE & AC power Adapter		

#	Description	Specification Sheet	Compliance (Y/N)	Remarks
16	IP addressing	DHCP, Static		
17	Protocol	SIP, RTP, RTCP, SRTP,		
18	Quality of service	VLAN, DiffServ / ToS		
19	Audio codes	Should support Audio Codecs G.711, G.722, G.729a/b		
20	POE Class 1 or better			
21	Should support text-based XML based applications for productivity enhancement			
22	Should have Adjust- able Desk Stand:			

3.5 Minimum Technical Specifications for Biometric Registration Kits (including Biometric Capture Devices)

3.5.1 Biometric Registration Kit

3.5.1.1 Laptop

#	Criteria	Minimum Specifications	Compliance (Y/N)	Remarks
1	Make	Must be specified		
2	Model	Must be specified. All relevant brochures must be submitted.		
3	Processor	Latest Generation x86 multi-core processor with base clock frequency at 3.2 GHz (or higher) with 6 MB cache (or higher) Note: The processor must be first launched in the processor manufacturer not earlier than 2020.		

#	Criteria	Minimum Specifications	Compliance (Y/N)	Remarks
4	System Responsiveness & Performance	Intel Core i7 7700, or AMD A10- 8750 or better processor. Where the processor is other than Intel Core i7 7700, or AMD A10-8750, the details of the processor are to be specified along with the documentary evidence from an acceptable accrediting benchmarking agency (like SPECfp_rate2006 or latest Sysmark score) to confirm that the proposed processor is rated either equal or higher than Intel Core i7 7700 or AMD A10-8750		
5	Motherboard & Chipset	OEM Motherboard with chipset corresponding to the processor quoted.		
6	Memory	16 GB DDR4 RAM, One Slot must be free for future upgrade		
7	Ports	Two x USB 3.2 Port One x USB 2.0 One x Gigabit LAN (RJ 45), One x HDMI Port (v1.4b), One x VGA Port, One x Headphone / Microphone		
8	Display	Maximum 14" Diagonal TFT Widescreen with minimum 1920 x 1080 resolution (16:9 ratio)		
9	Audio	Built-in Speakers		
10	Web Camera	Built in webcam		
11	Hard Disk Drive	Minimum 512 GB SSD		
12	Ethernet	Integrated (10/ 100/ 1000) Gigabit LAN		
13	Wireless / Bluetooth	Inbuilt Wi-Fi with Bluetooth - 802.11 b/g/n/ac, Bluetooth (v5)		
14	Battery	Minimum 4 Cell lithium-ion or lithium polymer battery with minimum 10 hours as battery backup		

#	Criteria	Minimum Specifications	Compliance (Y/N)	Remarks
15	Power Supply	Standard AC Adaptor for Sri Lanka		
16	Keyboard	Standard Keyboard		
17	Touchpad	Multi-touch support		
18	Mouse	Wired - USB 3.2 button optical Scroll Mouse with mouse pad		
19	Weight	Laptop with battery (without mouse) should not weigh more than 2 Kg		
20	Operating System	Windows® 11-Pro 64bit (Down gradable to Windows 10) It should be pre-loaded, licensed copy with certificate of authenticity (or equivalent authenticity information) and all necessary and latest patches and updates.		
21	Other pre-loaded software (open source/ free)	Adobe Acrobat Reader, Drivers (as applicable) All software should be pre-installed & shipped at various locations mentioned in the RFP		
22	Certification	Energy Star 5.0 or above / BEE star certified		
23	Antivirus with Internet Security Solution	This must be Factory Installed		
24	Accessories	Laptop carrying Back-pack. It must be from same OEM as laptop		

3.5.1.2 Dual Display Monitor (Touch Sensitive)

#	Criteria	Minimum Specification	Compliance (Y/N)	Remarks
1	Make	Same as Laptop		
2	Colour	Same as laptop		
3	Plug and Play	Yes		

#	Criteria	Minimum Specification	Compliance (Y/N)	Remarks
4	Screen Form Factor	Flat		
5	Size	15-16 inch or higher		
6	Type	LCD		
7	Resolution	HD, or Full HD		
8	Response Time	8 ms (or less)		
9	Touch	Touch Sensitive		
10	Ports	1 x HDMI Port (v1.4b), 1 x VGA Port		
11	Panel	IPS / VA		
12	Accessories	Stand to mount the monitor on top of the table		
13	Accessories	Cable to connect this monitor with the laptop		

3.5.1.3 USB Hub

#	Criteria	Minimum Specification	Compliance (Y/N)	Remarks
1	Ports	USB 2.0 and USB 3.0 ports compatible with laptop, desktop and other accessories quoted by the ISI		
2	Power	USB powered through laptop		

3.5.1.4 Background Screen (Photograph Capture)

#	Criteria	Minimum Specification	Compliance (Y/N)	Remarks
1	Size	4 X 5 ft		
2	Accessories	Stand		
3	Non-Reflecting	Yes		

#	Criteria	Minimum Specification	Compliance (Y/N)	Remarks
4	Opaque	Yes		
5	Miscellaneous	Stand mountable and Wall mountable		

3.5.1.5 Power Extension Board

#	Criteria	Minimum Specification	Compliance (Y/N)	Remarks
1	General	Minimum 6 number of power sockets (compatible with Sri Lanka electrical supply)		
2	Features	Fuse, On/Off Switch		
3	Certification	SIS		

3.5.1.6 Flash Drive

#	Criteria	Minimum Specification	Compliance (Y/N)	Remarks
1	Connectivity	USB 3.0 (Plug and Play)		
2	Capacity	64 GB		
3	Safety	Water resistant		
4	Storage	Images, Documents, etc.		
5	Design	Compact and Portable		
6	Compatibility	Latest Windows OS and Operating System for Laptops being supplied by ISI		

3.5.1.7 Enrolment Kit container with wheels

#	Criteria	Minimum Specification	Compliance (Y/N)	Remarks
1	Material	High-Quality Fibre		
2	Life / Durability	Minimum 6 years		
3	Size	Should be able to accommodate items in the enrolment kit		
4	Cushion	Should have sufficient cushions for all the equipment from Top, Bottom and all sides		
5	Space	Separate enclosures should be built for the items of enrolment kit		
6.	Lock and Keys	One lock and three keys		
7	Wheels	Should have high quality 4 number of wheels		

3.5.1.8 Flash Light

#	Criteria	Minimum Specification	Compliance (Y/N)	Remarks
1	Capacity	60W (with bulb)		
2	Accessories	Stand, 2Mrts Wire and on/off Switch near the operator		
3	Light	White		

3.5.1.9 Internet Dongle

#	Criteria	Minimum Specification	Compliance (Y/N)	Remarks
1	Connectivity	Wired or Wireless		
2	Accessories	Connection wire (with extension cord) to connect Internet Dongle with USB Hub and Laptop		

#	Criteria	Minimum Specification	Compliance (Y/N)	Remarks
3	Compatibility	Latest Windows OS and Operating System for Laptops being supplied by ISI		
4	Network Type	4G, 3G and 2G		
5	Network Firm	One of the most widely available and consistent networks in Sri Lanka		
6	Safety	Water resistant		
7	Design	Compact and Portable		
8	Port	USB 2.0 or USB 3.0 compatible with USB Hub and Laptop		

3.5.1.10 Signature Pad

#	Criteria	Minimum Specification	Compliance (Y/N)	Remarks
1	Connectivity	Wired connectivity		
2	Port	USB 2.0 or USB 3.0 compatible with USB Hub and Laptop		
3	Accessories	Connection wire (with extension cord) to connect signature pad with USB Hub and Laptop		
4	Accessories	1 x High Quality Stylus 1 x Pen-Clipper 10 x Pen Nibs; 1 x Nib Extractor 1 x Cleaning Cloth		
5	Compatibility	Latest Windows OS and Operating System for Laptops being supplied by ISI		
6	Dimension	Screen Size of more than 4 inch (measured diagonally)		
7	Power	Through USB		

#	Criteria	Minimum Specification	Compliance (Y/N)	Remarks
8	Usage	Plug and Play		
9	Accuracy	Coordinate Accuracy of +/-0.5 mm (center)		
10	Resolution	Sensor Resolution of at least 2500 lpi		
11	Sensitivity	Pressure sensitivity of at least 7500 levels		
12	Reading	Electromagnetic resonance (EMR)		

3.5.1.11 QR Code Reader

#	Criteria	Minimum Specification	Compliance (Y/N)	Remarks
1	Connectivity	Wired connectivity		
2	Port	USB 2.0 or USB 3.0 compatible with USB Hub and Laptop		
3	Accessories	Connection wire (with extension cord) to connect reader with USB Hub and Laptop		
4	Compatibility	Latest Windows OS and Operating System for Laptops being supplied by ISI		
5	Power	Through USB		
6	Usage	Plug and Play		
7	Shock Proof	Withstands a drop of maximum of 1.5 meters on concrete surface		
8	Operation	Handheld		
9	Mode	Manual and Automatic		
10	Time	Scanning within 5 milliseconds		

#	Criteria	Minimum Specification	Compliance (Y/N)	Remarks
11.	Angle	Scanning at a maximum of elevation 65°, rotation angle 30°, and deflection angle 55°		
12	Accuracy	Higher decoding accuracy, easy to interpret all kinds of incomplete and fuzzy barcodes, reverse barcodes		
13	Reading	1-D and 2-D Bar Codes (2D: QR code, data matrix, PDF417, Aztec, Maxi code, and 1D: UPC / EAN / JAN, UPC-A and UPC-E, EAN-8 and EAN-13, JAN-8 and JAN-13, ISBN / ISSN, code 39 (with full ASCII), Codabar (NW7), code 128 & EAN 128, Code 93, Interleaved 2 of 5 (ITF), Appendix 2 of 5, IATA Code, ISI / Plessy, Code 32 (Italian Pharmacode), RSS 14, RSS Limited, RSS Extension) Note: Should also read the barcode for standards specified in the Volume-2.		
14	Miscellaneous	Buzzer and LED light		

3.5.1.12 Multi-function Printer

#	Criteria	Specifications	Compliance (Y/N)	Remarks
General				
1.	Compatible operating systems	Latest Windows OS and Operating System for Laptops being supplied by ISI		
2.	Certification	Energy Star		

#	Criteria	Specifications	Compliance (Y/N)	Remarks
3.	Port	USB 2.0 or USB 3.0 compatible with USB Hub and Laptop		
4.	Accessories	Connection wire (with extension cord) to connect device with USB Hub and Laptop		
5.	Power	Power adaptor (Sri Lanka) and power cable		
6.	Function	Scan, Print, Copy		
7.	Media	Plain Paper, Photo Paper, Brochure Paper		
Printer				
8.	Functions	Mono Print		
9.	Printer Type	Monochrome		
10.	Technology	Inkjet or Laser (Black & White)		
11.	First Print	Maximum of 20 seconds		
12.	Print Speed (A4)	Minimum 10 pages-per- minute (mono) in A4 format		
13.	Print Resolution (Hardware)	Minimum 300 x 300 dpi		
14.	Duty cycle	Minimum 8,000 Pages per month		
15.	Memory	64 MB RAM or better		
16.	Paper Capacity	Min. 100-sheet Input Standard tray and Min. 20-sheet Output Standard tray		
17.	Duplex	Manual		

#	Criteria	Specifications	Compliance (Y/N)	Remarks
18.	Printer Cartridges / Toner	Only Genuine and Original Compatible cartridges from the OEM of the Printer. Minimum one brand new, unused cartridge to be supplied with Printer		
Scanner				
19.	Function	Scanner		
20.	Scan Type	Flatbed		
21.	Scan Resolution	Minimum 600 x 600 DPI		
22.	Scan Size	A4, Letter, Legal		
23.	Scan file format	JPEG and PDF		
24.	Scan Speed	Less than 15 seconds for a coloured page		
25.	Bit Depth Colour	16-bit / 8-bit		
Copier				
26.	Function	Copier		
27.	First Copy Out Time	Maximum of First Print specification		
28.	Speed	Maximum of Print Speed specification		

3.5.1.13 Speaker

#	Criteria	Minimum Specification	Compliance (Y/N)	Remarks
1	Type	Portable		
2	Connection	Bluetooth (range of minimum 5 meter)		

#	Criteria	Minimum Specification	Compliance (Y/N)	Remarks
3	Power	AC adaptor (Sri Lanka Compatible) through Micro- USB port		
4	Battery Life	Minimum of 8 hours (at 50% volume)		
5	Charge Time	Maximum of 4 hours		
6	Output	Minimum 16 Watt		
7	Usage	Plug and Play		
8	Design	Compact and Portable		
9	Accessories	Charging Cable, Adaptor		
10	Configuration	Stereo		
11	Memory Card	Supported up to 32 GB		
12	Shock Proof	Withstands a drop of maximum of 1.5 meters on concrete surface		
13	Safety	Water resistant		

3.5.2 Biometric Capture Devices (Enrolment and Authentication)

3.5.2.1 Fingerprint Specifications (Enrolment)

Capture Time across modalities should be less than 4 Seconds (time taken for providing a final capture response to the calling application, when the biometrics are well placed on the sensors). The devices should be ergonomic, easily accessible, ease to use and common available. Please Refer ISO 19794- 4:2011 Specifications.

#	Factor	Registration Devices	Compliance (Y/N)	Remarks
1	MOSIP Compliance	Latest SBI specification compliance With MDS and device management server With SDK for biometric capture & quality check.		

#	Factor	Registration Devices	Compliance (Y/N)	Remarks
2	Image Specification	ISO 19794-4:2011 Annex B1		
3	Minimum Resolution	>= 500 native DPI. Higher densities are preferred.		
4	Minimum Active Platen Area or Capture area*	>=1.6 x 1.5 inches for 1 to 2 fingers >=3.2 x 2.0 inches for 4 fingers		
5	Greyscale Density	8 bits (256 grey levels)		
6	Image Format	JPEG 2000 Lossless		
7	Compression Ratio	Lossless		
8	Quality Score	NFIQ v2.0		
9	Capture Mode	Auto Capture		
10	Preview	> 3 FPS M-JPEG frames with NFIQ 2.0 score superimposed		
11	ESD	>= 8kv		
12	EMC Compliance	FCC class A or equivalent		
13	Operating Temperature*	0 to 50 °C		
14	FTM**	SBI 1.0 - Use host-based security (and above)		
15	Host operating	Latest Windows, Actively- supported Android		

#	Factor	Registration Devices	Compliance (Y/N)	Remarks
	system supported			
16	Maximum Capture Time	4 seconds (this is the time for capturing, processing and giving a final response out to the calling application, after the biometrics are well placed on the sensors)		

* MOSIP adopters can change this if needed, please refer to MOSIP website[1] for latest values

** Please refer SBI specification documentation[2]

[1] MOSIP Device Specifications (https://docs.mosip.io/platform/biometrics/biometric-specification)

[2] SBI Specification Document (https://docs.mosip.io/platform/biometrics/secure-biometric-interface-specification)

3.5.2.2 Fingerprint Specifications (Authentication)

Capture Time across modalities should be less than 4 Seconds (time taken for providing a final capture response to the calling application, when the biometrics are well placed on the sensors). The devices should be ergonomic, easily accessible, ease to use and common available. Please Refer ISO 19794-4:2011 Specifications.

#	Factor	Registration Devices	Compliance (Y/N)	Remarks
1	MOSIP Compliance	Latest SBI specification compliance With MDS and device management server Support for Windows and Android based authentication		
2	Image Specification	ISO 19794-4:2011 Annex B2		
3	Minimum Resolution	>= 500 native DPI		
4	Minimum Active Platen Area or Capture area*	>=0.5 x 0.65 inches*		

#	Factor	Registration Devices	Compliance (Y/N)	Remarks
5	Greyscale Density	8 bits (256 grey levels)		
6	Image Format	JPEG 2000 Lossy or WSQ		
7	Compression Ratio	Up to 15:1		
8	Quality Score	NFIQ v1.0		
9	Capture Mode	Auto Capture		
10	Preview	Not Applicable		
11	ESD	>= 8kv		
12	EMC Compliance	FCC class A or equivalent		
13	Operating Temperature*	0 to 50 °C		
14	FTM**	SBI 2.0 - FTM supported security		
15	Host operating system supported	Latest Windows, Actively- supported Android		
16	Maximum Capture Time	4 seconds (this is the time for capturing, processing and giving a final response out to the calling application, after the biometrics are well placed on the sensors)		

* MOSIP adopters can change this if needed, please refer to MOSIP website[3] for latest values

** Please refer SBI specification documentation[4]

[3] MOSIP Device Specifications (https://docs.mosip.io/platform/biometrics/biometric-specification)

[4] SBI Specification Document (https://docs.mosip.io/platform/biometrics/secure-biometric-interface-specification)

3.5.2.3 Iris Specifications (Enrolment)

Capture Time across modalities should be less than 4 Seconds (time taken for providing a final capture response to the calling application, when the biometrics are well placed on the sensors). The devices should be ergonomic, easily accessible, ease to use and common available. Please Refer to ISO 19794- 6:2011 Specifications.

#	Factor	Registration Devices	Compliance (Y/N)	Remarks
1	MOSIP Compliance	Latest SBI specification compliance With MDS and device management server. With SDK for biometric capture & quality check.		
2	Image Specification	ISO 19794-6:2011 Annex B		
3	Minimum Iris Diameter	>=210 pixels		
4	Greyscale Density	8 bits (256 grey levels)		
5	Spatial Resolution	>=60% @ 2Lp/mm		
6	Pixel Resolution	>10 pixels/mm		
7	Capture Distance	>=10 CM		
8	Imaging Wavelength	Approximately 700-900 nm		
9	Illumination	The eye should be illuminated using infrared or any other source that could produce high-quality gray scale image		
10	Image Format	IMAGE_TYPE_VGA (K2) OR IMAGE_TYPE_CROPPED (K3)		
11	Compression	JPEG 2000 Lossless		

#	Factor	Registration Devices	Compliance (Y/N)	Remarks
12	Compression Ratio	Lossless		
13	Aspect Ratio	1:1		
14	Capture Mode	Auto Capture		
15	Scan Type	Progressive		
16	Preview	>= 3 FPS M-JPEG frames with quality score superimposed		
17	EMC compliance	FCC Class A or equivalent		
18	Operating Temperature *	0 to °50 C		
19	FTM**	SBI 1.0 - Use host-based security (and above)		
20	Host operating system supported	Latest Windows, Actively-supported Android		
21	Maximum Capture Time	4 seconds (this is the time for capturing, processing and giving a final response out to the calling application, after the biometrics are well placed on the sensors)		

* MOSIP adopters can change this if needed, please refer to MOSIP website[5] for latest values

** Please refer SBI specification documentation[6]

[5] MOSIP Device Specifications (https://docs.mosip.io/platform/biometrics/biometric-specification)

[6] SBI Specification Document (https://docs.mosip.io/platform/biometrics/secure-biometric-interface-specification)

3.5.2.4 Iris Specifications (Authentication)

Capture Time across modalities should be less than 4 Seconds (time taken for providing a final capture response to the calling application, when the biometrics are well placed on the sensors). The devices should be ergonomic, easily accessible, ease to use and common available. Please Refer to ISO 19794- 6:2011 Specifications.

#	Factor	Registration Devices	Compliance (Y/N)	Remarks
1	MOSIP Compliance	Latest SBI specification compliance With MDS and device management server. Support for Windows and Android based authentication		
2	Image Specification	ISO 19794-6:2011 Annex B		
3	Minimum Iris Diameter	>=150 pixels		
4	Greyscale Density	8 bits (256 grey levels)		
5	Spatial Resolution	>=50% @ 1Lp/mm		
6	Pixel Resolution	>10 pixels/mm		
7	Capture Distance	>=10 CM		
8	Imaging Wavelength	Approximately 700-900 nm		
9	Illumination	The eye should be illuminated using infrared or any other source that could produce high-quality gray scale image		
10	Image Format	IMAGE_TYPE_CROPPED_AND_MASKED (K7)		
11	Compression	JPEG 2000 Lossy		

#	Factor	Registration Devices	Compliance (Y/N)	Remarks
12	Compression Ratio	Up to 15:1 (>= 3.5 KB)		
13	Aspect Ratio	1:1		
14	Capture Mode	Auto Capture		
15	Scan Type	Progressive		
16	Preview	Not Applicable		
17	EMC compliance	FCC Class A or equivalent		
18	Operating Temperature*	0 to °50 C		
19	FTM**	SBI 2.0 – FTM supported security		
20	Host operating system supported	Latest Windows, Actively-supported Android		
21	Maximum Capture Time	4 seconds (this is the time for capturing, processing and giving a final response out to the calling application, after the biometrics are well placed on the sensors)		

* MOSIP adopters can change this if needed, please refer to MOSIP website[7] for latest values

** Please refer SBI specification documentation[8]

[7] MOSIP Device Specifications (https://docs.mosip.io/platform/biometrics/biometric-specification)

[8] SBI Specification Document (https://docs.mosip.io/platform/biometrics/secure-biometric-interface-specification)

3.5.2.5 Face Specifications (Enrolment)

Capture Time across modalities should be less than 4 Seconds (time taken for providing a final capture response to the calling application, when the biometrics are well placed on the sensors).

The devices should be ergonomic, easily accessible, ease to use and common available. Please Refer ISO 19794- 5:2011 Specifications.

#	Factor	Registration Devices	Compliance (Y/N)	Remarks
1	MOSIP Compliance	Latest SBI specification compliance With MDS and device management server. With SDK for biometric capture & quality check.		
2	Image Specification	ISO 19794-5:2011		
3	Camera Specification	1080p with 90-degree FoV or above		
4	Skin Tone	All		
5	Exception Image Specification	Full Frontal with FACE features, two palms next to the face, waist up photo. 60mm (width) X 40mm (height)		
6	Image quality	ICAO - Full frontal image, +/- 5 degrees rotation, 24-bit RGB, white background 35 mm (width) X 45mm (height)		
7	Image Format	JPEG 2000 Lossless		
8	Compression Ratio	Lossless		
9	EMC compliance	FCC Class A or equivalent		
10	Operating Temperature*	0 to °50 C		

#	Factor	Registration Devices	Compliance (Y/N)	Remarks
11	FTM**	SBI 1.0 – Use host-based security (and above)		
12	Host operating system supported	Latest Windows, Actively-supported Android		
13	Maximum Capture Time	4 seconds (this is the time for capturing, processing and giving a final response out to the calling application, after the biometrics are well placed on the sensors)		

* MOSIP adopters can change this if needed, please refer to MOSIP website[9] for latest values

** Please refer SBI specification documentation[10]

[9] MOSIP Device Specifications (https://docs.mosip.io/platform/biometrics/biometric-specification)

[10] SBI Specification Document (https://docs.mosip.io/platform/biometrics/secure-biometric-interface-specification)

3.5.2.6 Face Specifications (Authentication)

Capture Time across modalities should be less than 4 Seconds (time taken for providing a final capture response to the calling application, when the biometrics are well placed on the sensors). The devices should be ergonomic, easily accessible, ease to use and common available. Please Refer ISO 19794-5:2011 Specifications

#	Factor	Registration Devices	Compliance (Y/N)	Remarks
1	MOSIP Compliance	Latest SBI specification compliance With MDS and device management server. Support for Windows and Android based authentication.		
2	Image Specification	ISO/IEC 19794-5:2011		

#	Factor	Registration Devices	Compliance (Y/N)	Remarks
3	Camera Specification	720p or above		
4	Skin Tone	All		
5	Image Specification	Not Applicable		
6	Image quality	ICAO is not mandated		
7	Image Format	JPEG 2000 Lossless		
8	Compression Ratio	Up to 15:1 (>= 3.5 KB)		
9	EMC compliance	FCC Class A or equivalent		
10	Operating Temperature*	0 to °50 C		
11	FTM**	SBI 2.0 – FTM supported security		
12	Host operating system supported	Latest Windows, Actively-supported Android		
13	Maximum Capture Time	4 seconds (this is the time for capturing, processing and giving a final response out to the calling application, after the biometrics are well placed on the sensors)		

* MOSIP adopters can change this if needed, please refer to MOSIP website[11] for latest values

** Please refer SBI specification documentation[12]

[11] MOSIP Device Specifications (https://docs.mosip.io/platform/biometrics/biometric-specification)

[12] SBI Specification Document (https://docs.mosip.io/platform/biometrics/secure-biometric-interface-specification)

3.5.2.7 Mobile Registration KIT

The mobile registration KIT consists of the following (not limited to): -

a. Laptop/Desktop
b. HD webcam including photo booth peripherals
c. Fingerprint slap capture device
d. Iris capturing device
e. Extended portable coloured monitor
f. Printer
g. Document scanner
h. Light

#	Factor	Registration Devices	Compliance (Y/N)	Remarks
1	MOSIP Compliance	Latest SBI specification compliance With MDS and device management server. With SDK for biometric capture & quality check.		
2	Laptop	• Processor – Latest Generation Processor with the following minimum specifications: 2 GHz Base Frequency, 8MB cache with turbo boost technology • 4 cores • 16 GB RAM or more • OS - Windows 10 Pro 64-bit must be installed in the SSD storage. • Storage - Hybrid Technology: 512 GB SSD (M.2 PCIe) and 1 TB HDD		

#	Factor	Registration Devices	Compliance (Y/N)	Remarks
		• Screen - Full HD, 14-14.1 inches • External Power Supply - AC power adapter can operate on 220V supply voltage and 60Hz • Battery - 6 hours of continuous usage during registration • Network Connectivity - Ethernet RJ45; and Wi-Fi (IEEE 802.11 b/g/n) • Ports - 2x USB 3.0, 1x USB 2.0, 1 x USB Type C, • HDMI port to attach a second monitor • Mouse - one (1) wired • Touch pad - Touch pad below keyboard (no minimum size) • Accessory - Charging Cable/ adapter • Anti-Virus - Third-party anti-virus Pre-installed with the latest updates and availability to update virus definitions. • The enterprise antivirus license must cover three (3) years from acceptance of the registration kits. • Chip - TPM 2.0 or higher		

#	Factor	Registration Devices	Compliance (Y/N)	Remarks
3	Type C USB Hub	• Components - 1 x Power adapter (5V / 2A), 1 x USB 3.0 Charging Cable • Number of Ports - Minimum of four (4) USB 3.0 and two (2) USB 2.0 ports • Connection - USB Type C connection • Power Supply - USB-powered or AC/DC power adapter		
4	Face Specifications (Enrolment)	Should be in compliance with the requirements mentioned in the 3.5.2.5		
5	Iris Specifications (Enrolment)	Should be in compliance with the requirements mentioned in the 3.5.2.3		
6	Fingerprint Specifications (Enrolment)	Should be in compliance with the requirements mentioned in the 3.5.2.1		
7	Extended Portable Coloured Monitor	• Type - Coloured • Size - 14 inches LED screen • Stand - Detachable, adjustable, can be customized and can hold/grip extended monitor • Resolution - 16:9 aspect ratio, 1080p, full HD • Input - HDMI (compatible with the laptop without the use of adapters)		

#	Factor	Registration Devices	Compliance (Y/N)	Remarks
		• Cable - HDMI Cable • External Power Supply – USB-powered or AC/DC power adapter		
8	Printer	• Resolution - 600 x 600 dpi • Paper Size - A4 • PPM - Black (A4) - >8 ppm • Duty Cycle - 5000 pages • Media Used - Ink tank for low cost running with additional 2 in tank refills of 150 ml • Monochrome – Yes (Black) • Connectivity - USB • Compatibility – Operating system of the laptop		
9	Portable HD Document Camera Scanner	• Image Sensor – Minimum CMOS of 5 megapixels. • Scan Resolution - Minimum 300 dpi with TWAIN driver • Scan Size - Can support documents with sizes smaller than A4, A4, and legal size • Focus Mode – Can operate both Manual and Auto Focus • Crop - Automatic • Light - LED supplement light • Connectivity - USB 2.0 or higher • Scan Speed - 1 second or better		

#	Factor	Registration Devices	Compliance (Y/N)	Remarks
		• Scanner Type - Camera-based document scanner with adjustable height connected via USB • Pad Size - Can accommodate A4 and legal- size paper • Compatibility - Operating system of the laptop		
10	Type	Rugged, Portable		
11	Customizations	Adaptation to country requirements		
12	Registration client	Should be able to run/integrate MOSIP registration client and enroll citizens as per the requirement in Annex-1		
13	Compatibility	Compliant with the operating system and SLUDI device manager specifications to handle device discovery, streaming, capture and other device lifecycle management requirements as specified in the MOSIP specification document.		
14	Light	• LED Ring Light • 14"Outer diameter 55W • Adjustable Light Stand • Dimmable • Can be rotated • With on/off switch near the operator • Can operate 220V supply voltage and 60Hz		

#	Factor	Registration Devices	Compliance (Y/N)	Remarks
15	Other	Weather-Resistant, Water repellent, Waterproof and shockproof Should accommodate in a single case (with high quality 4 or 8 wheels) with enclosures and cushion from all sides: • Laptop • Wired mouse • Fingerprint Slap Scanner • Iris scanner • Web Camera • Printer • Extended monitor • Portable Document Scanner • All cables (Power, USB, others)		
16	Technical Support	Support and Maintenance - Standard support and maintenance is 3 years of onsite support and maintenance. Scope - All parts including the devices, wires, casing, software, anti-virus engine, drivers and mountings that constitute the registration kit.		

3.5.2.8 Device Management

#	Factor	Registration Devices	Compliance (Y/N)	Remarks
1	MOSIP Compliance	Latest SBI specification compliance With MDS and device management server.		

#	Factor	Registration Devices	Compliance (Y/N)	Remarks
		Compliance: https://docs.mosip.io/1.1.5/apis/device- management-apis Compliance: https://docs.mosip.io/1.1.5/biometrics/mosip- device-service-specification		
2	Functions	Biometric devices are expected to get connected with the management server and get a certificate issued by the device provider for its usage Mouse - one (1) wired		
3	Management Server	• The management server has the following objectives • Validate the devices to ensure it is a genuine device from the respective device provider. This can be achieved using the device info and the certificates of the Foundational Trust Module • Manage/Sync time between the end device and the server. The time to be synced should be the only trusted time accepted by the device • Ability to issue commands to the end device for • Clean up of the device keys • Collect device information to maintain, manage, support, and upgrade a device remotely • A central repository of all the approved devices from the device provider		

#	Factor	Registration Devices	Compliance (Y/N)	Remarks
		• Safe storage of keys using HSM FIPS 140-2 Level 3. These keys are used to issue the device certificate upon registration of the device with the Management Server. The Management Server is created and hosted by the device provider outside of SLUDI. The communication protocols between the MDS and the Management Server can be decided by the respective device provider. Such communication should be restricted to the above specified interactions only. No transactional information should be sent to this server • Should have the ability to push updates from the server to the client devices		
4	Management Client	• The Management Client is the interface that connects the device with the respective management server. • Features of the management client include: • For better and efficient handling of devices at large volume, we expect the devices to auto register to the Management server • All communication to the server and from the server should follow that below properties		

#	Factor	Registration Devices	Compliance (Y/N)	Remarks
		• All communications are digitally signed with the approved algorithms • All communications to the server are encrypted using one of the approved public key cryptographies (HTTPS – TLS1.2/1.3 is required with one of the approved algorithms • All requests have timestamps attached in ISO format to the milliseconds inside the signature • All communication back and forth should have the signed digital id as one of the attributes • It is expected that auto registration has an absolute way to identify and validate the devices • The management client should be able to detect the devices in a plug and play model • All key rotation should be triggered from the server • Should have the ability to detect if it is speaking to the right management server • All upgrades should be verifiable, and the client should have ability to verify software upgrades • Should not allow any downgrade of software • Should not expose any API to capture biometric. The management server should		

#	Factor	Registration Devices	Compliance (Y/N)	Remarks
		have no ability to trigger a capture request • No logging of biometric data is allowed. (Both in the encrypted and unencrypted format) • Should securely store data		
5	Certifications and documentation related to the management server environment and FTM provisioning environment	• ISO 27001 certification • FIPS 140-2 Level 3 HSM certification • VAPT conduct and report • Disaster recovery plan • Architecture diagram • Demonstration of compliance to requirements		

3.6 Minimum Technical Specification for Biometric Software and Hardware

3.6.1 Functional and Technical Requirements of Biometric Software

3.6.1.1 ABIS

#	Requirement	Functional and Non-Functional Requirement Description	Compliance (Y/N)	Remarks
Enrolment Related				
1	MOSIP Compliance	Compliance to MOSIP specification https://docs.mosip.io/1.1.5/biometrics/automated-biometric-identification-system-abis		
2	Insert	Use to insert biometric data (templates) into the reference database without performing		

#	Requirement	Functional and Non-Functional Requirement Description	Compliance (Y/N)	Remarks
		biometric matching. Obtain the biometric and demographic data for the supplied ID, process the biometric samples as required by the biometric solution and store [templates] in a reference database. The function will internally invoke segmentation, feature extraction and template generation.		
3	Identify	Use to perform de-duplication and identification (in case of lost UDI of an enrolled person) across entire or sub-set of the database. It compares the query data for the supplied index against the entire reference database, sub-set of the database, a set of supplied indices or a single supplied index. Incoming query data samples shall at all times consist of images, possibly cropped and compressed without any loss. The function returns a candidate list of transaction numbers of potential duplicates above a threshold and associated comparison scores scaled on the interval [0,100] with 0 being the measure of least similarity.		
4	Delete	Use to remove an ID from the reference database. The removal need could arise for a variety of reasons. All such incidents should be automatically brought to the notice of DRP on an immediate		

#	Requirement	Functional and Non-Functional Requirement Description	Compliance (Y/N)	Remarks
		basis. The DELETE functionality of the ABIS should be disabled by the BSP.		
5	Update	Updating biometric data in the reference database will be accomplished by inserting a new record. On rare occasion, the ABIS will be subsequently directed by the SL-UDI application to delete an existing record in connection with the update operation.		
6	Deduplication	ABIS is expected to use fingerprints and iris for de-duplication. The BSP may choose to use face photo13 for de-duplication within the ABIS as well. The deduplication mechanism will be finalized at the time of implementation.		
Management Functions				
7	General	Management related functions will be at two levels of security and allow the ABIS component to be managed using a programming interface. On the higher security level, the key required functions include shutdown, clear and configure functions. On lower security level, pining function is required.		
8	Shutdown[14]	The ABIS component is required to shut itself down.		

#	Requirement	Functional and Non-Functional Requirement Description	Compliance (Y/N)	Remarks
9	Clear[15]	The ABIS component is required to delete all the data from its reference database and clear all queues.		
10	Configure	At the time of initialization, ABIS Component is provided with vendor specific information to configure itself. The information will include operating characteristic.		
11	Pinging	Pinging the system is at the lower security level. Additional functions required for system management, configuration, logging and reporting should be provided under the appropriate requirements.		
Verification Related				
12	Verify	Verification is a special case required to identify the above mentioned where only 1:1 comparisons are performed. ABIS is sent a query consisting of the fingerprint, iris or photograph image or minutiae. A scaled comparison score and a "match/non- match" decision is always returned. Fingerprint, Iris and Photograph verification utilizing biometric standard compliant templates will be done without use of proprietary extended data.		

#	Requirement	Functional and Non-Functional Requirement Description	Compliance (Y/N)	Remarks
Data Storage Requirement				
13	General	Persistent data including the reference database may be stored in industry standard RDBMS or in file system. In both cases, the vendor should provide export tools to allow access to the data in situations including but not limited to change of BSP, database synchronization, backup, upgrade or maintenance. The exported data should be in industry standard format readable using open-source tools and compliant to defined biometric standards.		
14	Backup and Restore	ABIS should have necessary backup and restore functions for routine system administration.		
15	Standard DB	A copy of the reference database will be stored in an industry standard database or file system existing at a separate location. Therefore, BSP shall provide all necessary assistance for the same.		
Logging and Monitoring				
16	General	Capability to log transactions at the component interface level, should be implemented such that it allows dynamic starting and stopping of this transaction logging service. The level of		

#	Requirement	Functional and Non-Functional Requirement Description	Compliance (Y/N)	Remarks
		logging should be controllable using a configuration parameter.		
17	General	The audit system should be centrally managed and should be secured against tampering. The system should be able to capture before and after values from transaction logs, privileged user audits, and raise alerts on suspicious activity. It should provide security facilities for role segregation within audit organization in terms of administrator, auditor etc. These audit logs should be kept per the retention policy of the SL-UDI application. Until SL- UDI's retention policy is published, BSP will retain all logs as specified in indicative list below.		
18	Audit	Audit and logging systems should be scalable and should have the space to grow. The system should be flexible to accommodate new audit requirements in the future.		
19	ABIS Log	a. Template generation time b. Total time taken for multi modal matching process (in seconds) c. Matching algorithm throughput d. Matching scores of each matcher including Fusion and the decision		

#	Requirement	Functional and Non-Functional Requirement Description	Compliance (Y/N)	Remarks
		e. Percentage of automated identification vs. manual intervention rate Above parameters should be recorded along with Registrar information, Geographical information, time of access, and the vendor name performing the matching g. System availability reports h. System usage reports (CPU usage, memory usage, IO usage)		
20	Verification Log	a. Verification Transaction Time b. System availability reports c. System usage reports (CPU usage, memory usage, IO usage)		
21	Management Function Log	a. Information on user (operator/manager/supervisor/ auditor) roles and/or privileges, including creation/deletion of users and changes to roles b. Changes to database records, including deletion of records c. Periodic (such as hourly) statistics on various databases including size d. Access log (including physical access of biometric servers) e. Activity log f. Change log g. Error log h. Denial of access		

#	Requirement	Functional and Non-Functional Requirement Description	Compliance (Y/N)	Remarks
		i. Audit log		
Security Requirement				
22	Persistent Data	All persistent personal information data will be encrypted.		
23	Data Access	Encryption password or user name / password should be required for data access.		
24	Access to Network	ABIS will not have access and should not try to access any network resources except the resources referenced by the URLs provided through the API.		
25	Backup Encryption	All backup data shall be stored in encrypted format using a key(s) available to the DRP.		
Other requirements				
26	Operator Interface	All administration and configuration features should be available through graphical UI (in addition to command level access).		
27	Platform Requirement	ABIS should be compatible with Windows as well as Linux OS with both 32- and 64-bit support on X86 COTS H/W.		
28	Standards	ABIS will comply with most recent applicable ISO standards and Biometric Standards for SL-UDI Applications		

#	Requirement	Functional and Non-Functional Requirement Description	Compliance (Y/N)	Remarks
29	Re-template	The ABIS should support re-template creation i.e. re-creation of biometric gallery from raw images based on latest algorithm with zero or minimal downtime during this re-template exercise.		
30	Quality	For verification (1:1) as well as Deduplication (1: N) Receiver operation characteristic, and Equal Error Rate (EER) <= 2%		
31	Miscellaneous	a. Should be able to work where segmentation is difficult due to missing Iris b. Should be able to work where there is spurious Iris c. Should be able to work where segmentation is difficult due to missing Iris d. Should be able to work where segmentation is difficult due to poor quality Fingerprint, Face and Iris e. Should be able to reject records without biometrics f. Should be able to detect duplication using one or more duplicate modalities g. Should be able to work for Iris where segmentation is difficult due to overlapping Iris with or without manual segmentation specification h. Should be able to deduplicate even with exceptionally low quality of images		

#	Requirement	Functional and Non-Functional Requirement Description	Compliance (Y/N)	Remarks
		i. Should be able to work with range: ±5 degrees for Face, ±10 degrees and flips for Iris j. Should be able to deduplicate with Iris with one iris matching, while the others do not: with the gallery pair		
32	Export	Should be able to export data in required format		
33	GetPendingJobs API	Should give the number of pending jobs		
34	GetReferenceCount, GetReferences APIs	Should provide required results in response to API calls		

3.6.1.2 Multimodal SDK

The SDK should come with latest industry practices such as liveness detection and should be tested on a wide variety of scenarios before being delivered for this project. The SDK is a set of libraries that provide the following functions.

#	Requirement	Functional and Non-Functional Requirement Description	Compliance (Y/N)	Remarks
1	MOSIP	MOSIP compliance and integration compatibility (Latest Biometric SDK APIs)		
2	Country customization	Allow customizations as per the country requirements.		
3	Optimization	Biometric SDK for Client Side should be optimized for client-side infrastructure requirement		
4	Quality	For verification (1:1) as well as Deduplication 1: N), Receiver operation		

#	Requirement	Functional and Non-Functional Requirement Description	Compliance (Y/N)	Remarks
		characteristic, and Equal Error Rate (EER) <= 2%		
5	Quality	The SDK should be able to work with varying quality of biometric images		
Fingerprint				
1	Segmentation	Slap sequence check / segmentation will be used to check if the claimed sequence: right or left slap is correct and also to visualize the segmentation result and use it for the feature extraction. It segments slap image of 2 to 4 fingers into respective digits with associated confidence level of segmentation accuracy. It will allow specification of missing or extra digits		
2	Quality Check	The capture quality check will be used to determine if the enrolment software needs to re-capture and provide corrective action; for example, finger is misplaced on the scanner. Quality check must be able to provide actionable feedback (e.g., “move finger to the left”).		
3	Compression / de-compression and format conversion	For verification applications, transmission of single fingerprints compression will be required, with decompression upon receipt by the verification function. During enrolment, the SDK is required to convert the image format, such as from RAW to PNG. The SDK will supply compression and de-compression algorithms with compression ratio which can be tuned.		

#	Requirement	Functional and Non-Functional Requirement Description	Compliance (Y/N)	Remarks
		This should be compatible to defined biometric standards.		
4	Template generation	The SDK should be able to generate defined biometric standards compliant templates that have been tested to be interoperable with other third-party matchers in an independent test.		
5	Identification or Deduplication (1: Nfew)	The SDK will be able to compare features extracted from a FP image against a set of reference templates and return a scaled comparison score between [0,100], with 0 indicating least similarity.		
6	Verification (1:1)	The SDK will be able to compare features extracted from a FP image against a specified reference templates and return a scaled comparison score between [0,100], with 0 indicating least similarity.		
Iris				
1	Quality Check	The capture quality check will be used to determine if the enrolment software needs to re-capture and provide corrective action, for example image is out of focus or has motion blur. Quality check should be able to provide actionable feedback.		
2	Segmentation	The SDK will be able to extract KIND_VGA, KIND_CROPPED, and KIND_CROPPED_AND_MASKED from ocular image. Should be able to work with 5 to 8% rotation of Iris		

#	Requirement	Functional and Non-Functional Requirement Description	Compliance (Y/N)	Remarks
		Should be able to work with varying quality - blurred, occlusion, poor iris ratio, noise, not suitable for capture Should be able to work with Iris Images with flipped and inverted irises (due to camera flip)		
3	Compression/ decompression and format conversion	The SDK will be able to convert image from one format to another (for example, BMP to KIND_VGA)		
4	Feature / Template generation	The SDK will be able to extract and store proprietary template from the segmented Iris image		
5	Identification or Deduplication (1:Nfew)	The SDK will be able to compare features extracted from a query iris image against a set of reference templates and return a scaled comparison score between [0,100], with 0 indicating least similarity.		
6	Verification (1:1)	The SDK will be able to compare features extracted from a query iris image against a specified reference template and return a scaled comparison score between [0,100], with 0 indicating least similarity.		
Facial				
1	Segmentation	Should be able to work with varying data quality including extremely poor quality Face images (non-frontal view, with dark glasses, motion blur, noise, poor illumination) Should be able to work with Blurred Looking Away, Ink Marked/Creased,		

#	Requirement	Functional and Non-Functional Requirement Description	Compliance (Y/N)	Remarks
		Hair Across Eyes, Eyes Closed, Shadows Across Face & Frame Covering Eyes		
2	Automatic Capture	Automatic capture will analyse video frames from the camera, provide actionable feedback, and select the best frame.		
3	Quality check	The capture quality check will be used to determine if the enrolment software needs to re-capture and provide corrective action.		
4	Image enhancement	Enhancement such as face cropping will automatically find the face in the photograph and crop/resize the image to an ICAO compliant format. The SDK should not carry out any grey-level manipulations		
5	Feature / Template generation	The SDK will be able to extract and store a proprietary template from the segmented face image.		
6	Compression / de- compression and format conversion	The SDK will be able to convert image from one format to another (for example, BMP to JPEG 2000) and compress or decompress images.		
7	Identification or Deduplication (1:Nfew)	The SDK will be able to compare features extracted from a query iris image against a set of reference templates and return a scaled comparison score between [0,100], with 0 indicating least similarity.		
8	Verification (1:1)	The SDK will be able to compare features extracted from a query face		

#	Requirement	Functional and Non-Functional Requirement Description	Compliance (Y/N)	Remarks
		image against a specified reference template and return a scaled comparison score between [0,100], with 0 indicating least similarity.		
9	Compliance	• ISO/IEC 19794-5 Compliance • Eye Location Accuracy. • Face Location Accuracy (other points). • Eye Distance (min 90 pixels). • Relative Vertical Position (0.5B<=BB<=0.7B) • Relative Horizontal Position (no tolerances) • Head Image Width Ratio • (0.5A<=CC<=0.71A) • Head Image Height Ratio (0.7B<=DD<=0.8B) • Blurring • Looking Away • Ink Marked/Creased • Unnatural Skin Tone • Too Dark/Light • Washed Out • Pixilation • Hair Across Eyes • Eyes Closed • Varied Background • Roll/Pitch/Yaw Greater		

#	Requirement	Functional and Non-Functional Requirement Description	Compliance (Y/N)	Remarks
		• Flash Reflection on Skin • Red Eyes • Shadows Behind Head • Shadows Across Face • Dark Tinted Lenses • Flash Reflection on Lenses • Frames too Heavy • Frame Covering Eyes • Hat/Cap • Veil over Face • Mouth Open • Presence of Other Faces or Toys too Close to Face		
Standards requirements				
1	Uncompressed Image	All uncompressed images should be as per defined biometric standards (e.g., PNG)		
2	Compressed Image	All compressed images should be as per defined biometric standards (e.g. WSQ or JPEG 2000 lossless)		
Reliability Requirements				
1	Consistent	The SDK should perform consistent to the specifications, for all possible data in the specified formats.		
2	Reproducible	The results should be reproducible on a variety of platforms.		

#	Requirement	Functional and Non-Functional Requirement Description	Compliance (Y/N)	Remarks
3	Miscellaneous	The libraries should work without any segmentation violations, memory faults or memory leaks		
Other Requirements				
1	Security Requirements	SDKs should be purely computational libraries and should have minimum system dependencies and should not attempt to access any resources such as hardware, files or network.		
2	User Interface	SDKs should not have any user interface		
3	Platform requirements	SDK should support Windows (8 & above) and Linux OS with both 32 and 64 bit support.		

3.6.2 Technical Requirements of Infrastructure for Hardware and Software

3.6.2.1 Blade Chassis

#	Description	Compliance (Y/N)	Remarks
1	Blade enclosure Should occupy a max of 8RU rack height, supporting a minimum 8 half height/4 Full height modular server per blade chassis.		
2	Blade enclosure should support all x86 based Intel/AMD processor blade servers		
3	Chassis should have sufficient number of redundant converged modules with 25G/100G ports to provide a minimum FCoE uplink bandwidth of 50 Gbps per blade server for a fully populated chassis for converged Traffic		
4	The chassis should support redundant modules for connectivity. The overall solution should support aggregation of multiple chassis for connectivity.		

#	Description	Compliance (Y/N)	Remarks
5	The enclosure should be populated fully with power supplies of the highest capacity available with the vendor. Power supplies should support N+N /N+1 redundancy configuration, where N is greater than 1. Chassis should be configured with Titanium certified Power supply.		
6	Each blade enclosure should have a cooling subsystem consisting of redundant hot pluggable fans or blowers enabled with technologies for improved power consumption and acoustics. The chassis cooling should be modular so that future enhancements can potentially handle open- or closed-loop liquid cooling to support higher-power processors.		
7	3 years comprehensive support and maintenance		
8	Management/controlling software's having to be from the OEM.		
9	The management solution and the switches that provides the connectivity to LAN and SAN environment should be provided		
10	Blade chassis management solution may be provided internal / external (SaaS or appliance based), to the chassis and must provide single console for managing up to 10 chassis.		
11	The same management solution should also be capable to manage Rack Servers along with Blade Servers and it should provide the visibility to virtualization infra of the leading hypervisor as well as to the SAN environment of leading OEMs like NetApp, Hitachi, Pure storage, etc.		
12	The management appliance/solution should be deployed in High Availability and should provide the administration of rack & blade servers across chassis from the same console.		
13	The management solution should provide Role based Access Control and remote management capability. The management software can be used to create resource pools based on a hierarchal structure and have the blade resources assigned to the respective resource pools		

#	Description		Compliance (Y/N)	Remarks
14	Firmware upgrade/downgrade should be possible for all the components in the infrastructure including the server, chassis management modules , converged switch, other modules from the same console that is used to manage the individual blades The management solution should provide email notification/alerts. It should also provide API to integrate with 3rd party solution.			
15	Administrators have the flexibility to define power policies so that the power can be limited to a specific server and have the flexibility to define power policies so that the power can be limited to a specific server			
16	Server management system should provide an alert in case the system is not part of OEM Hardware Compatibility list			
17	The proposed management solution should provide security & advisory details via same unified dashboard and Supports multiple level of authentication methods including TACACs+/ LDAP/ RADIUS/AD			

3.6.2.2 Blade Server

#	Description	Compliance (Y/N)	Remarks
1	Blade server should be proposed with the latest generation x86 Intel/AMD processors Should be quoted with minimum 2 x 16 Core processors with minimum 2.8GHz of clock cycle		
2	OS support: 64 bit Microsoft® Windows Server Enterprise Edition / Red Hat® Enterprise Linux / SUSE® Linux Enterprise Server, Oracle Linux Hypervisor Support - Citrix® XenServer® /VMware vSphere® ESXi/,-KVM/, All servers will be based on x86 architecture Shall be certified for proposing virtualization / Operating systems		
3	Blade server should be quoted with minimum 512 GB memory, expandable up to 8TB, 4800/5600 MHz		

#	Description	Compliance (Y/N)	Remarks
	DDR4/DDR5 DIMMS and should support RAS features and memory mirroring		
4	The blade server should support min 6 no's of SAS/SSD/NVMe disk drive and should be quoted with minimum 2 x 480GB M.2 Boot drive in RAID 1 -All the hard disks and power supplies to be hot-swappable		
5	The Blade server should support Converged Network Adapters. The Converged Network Adapters should aggregate both the Ethernet and FC connectivity on a single fabric providing 100Gbs bandwidth per blade		
6	All servers to be connected to Ethernet with redundancy.		
7	3 years comprehensive support and maintenance 24x7		
8	manage the blade servers across multiple chassis , rack servers from the same unified console. It should provide the complete administration including operating system installation and firmware management from the single console with a unified view of all the blade servers, server identities, configuration details, monitoring and alerting system should support embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated phone home support.		
9	System remote management should support browser based Graphical Remote Console along with Virtual Power button, Remote boot using USB / CD/ DVD Drive. It should be capable of offering upgrade of software and patches from a remote client using Media / image/folder; It should support server power capping and historical reporting and should have support for multifactor authentication.		

3.6.2.3 Rack Server

#	Description	Compliance (Y/N)	Remarks
1	OS support: 64 bit Microsoft® Windows Server Enterprise Edition / Red Hat® Enterprise Linux / SUSE® Linux Enterprise Server, Oracle Linux Hypervisor Support - Citrix® XenServer® VMware vSphere® ESXi, KVM, All servers will be based on x86 architecture Shall be certified for proposing virtualization/Operating systems		
2	Server should be quoted with latest generation x86 Intel/AMD processor Server should be configured with minium of 2 x 16 Cores 2.8GHz latest generation Intel/AMD processors		
3	Memory (RAM): Min. 512 GB scalable up to 8TB of Memory with DDR5 memory DIMMS		
4	12Gbps SAS RAID controller with 4GB Cache supporting RAID 0,1, 5, 6,10, 50, 60 supporting capacity drives configured in system.		
5	HDD: Minimum 2 x 600GB 10K/15K RPM SAS		
6	Support for min 20 small form factor hot plug SAS / SCSI/SSD/NVMe hard drives in disk drive		
7	Atleast 4 x 10/25 G Ethernet ports or more		
8	Server should support 32/64G FC ports.		
9	Rear: One USB ports (Ver 2.0 or higher); RJ-45 Ethernet; ; two RJ-45 Ethernet; / Front: One USB (Ver 2.0)/KVM Connector		
10	Graphics controller: Should support video using the Matrox G200e video/graphics controller		

#	Description	Compliance (Y/N)	Remarks
	Supports display resolutions up to 1920 x 1200 16bpp @ 60H		
12	Security: Power-on password / admin password / Should have a cyber resilient architecture for a hardened server design for protection, detection & recovery from cyber attacks Should protect against firmware which executes before the OS boots * Hardware based Root of Trust * Signed firmware updates * Secure default passwords * Secure alerting		
13	Cooling fans: minimum Four fans / multispeed / hot-swap and redundant fan failure signals to management module / fan in each power supply / CPU / memory		
14	Power supplies: Hot plug redundant AC power supply		
15	Management feature to identify failed components even when server is switched off.		
16	Rack Mountable 2U		
17	It should provide Secure Sockets Layer (SSL) 256 bit encryption and Secure Shell (SSH) Version 3 and support VPN for secure access over internet.		
18	Should be able to manage systems through a web-browser		

3.6.2.4 Rack

#	Description	Compliance (Y/N)	Remarks
1	19” 42U racks shall be used in the Data Centre for hosting the department applications. All the racks should be mounted on the floor with castor wheels with brakes (set of 4 per rack)		
2	Floor Standing Server Rack - 42U with Heavy Duty Extruded Aluminum Frame for rigidity. Top cover with FHU provision. Top & Bottom cover with cable entry gland plates. Heavy Duty Top and Bottom frame of MS. Two pairs of 19" mounting angles with 'U' marking. Depth support channels - 3 pairs. with an overall weight carrying Capacity of 500Kgs.		
3	The racks should conform to EIA-310 Standard for Cabinets, Racks, Panels and Associated Equipment and accommodate industry standard 19” rack mount equipment.		
4	Front and Back doors should be perforated with atleast 63% or higher perforations.		
5	All racks should be OEM racks with Adjustable mounting depth, Multi-operator component compatibility, Numbered U positions, Powder coat paint finish and Protective grounding provisions.		
6	All racks should have mounting hardware 2 Packs, Blanking Panel (1) varying from 1U to 4 U size.		
7	Keyboard Tray with BB Slides (Rotary Type) (1 no. per Rack)		
8	Stationery Shelf 627mm Network (2 sets per Rack)		
9	All racks must be lockable on all sides with unique key for each rack		
10	Racks should be compatible with floor-throw as well as top-throw data center cooling systems.		

#	Description	Compliance (Y/N)	Remarks
11	Racks should have Rear Cable Management channels, Roof and base cable access		
12	Wire managers: Two vertical and four horizontal		
13	Power Distribution Unit - Vertically Mounted, 32AMPs with 25 Power Outputs. (20 Power outs of IEC 320 C13 Sockets & 5 Power outs of 5/13 Amp Sockets), Electronically controlled circuits for Surge & Spike protection, LED readout for the total current being drawn from the channel, 32AMPS MCB, 5 KVA isolated input to Ground & Output to Ground (1 No per Rack)		
14	The racks must have steel (solid / grill / mesh) front / rear doors and side panels. Racks should NOT have glass doors / panels.		
15	Both the front and rear doors should be designed with quick release hinges allowing for quick and easy detachment without the use of tools.		
16	Fan Housing Unit 4 Fan Position (Top Mounted) (1 no. per Rack) - Monitored - Thermostat based - The Fans should switch on based on the Temperature within the rack. The temperature setting should be factory settable. This unit should also include - humidity & temperature sensor		
17	Keyboard, Video Display Unit and Mouse Unit (KVM) and/or other Control Devices/PCs may be used for the IT Infrastructure Management for which the necessary consoles/devices shall be placed in the location earmarked. The KVM unit should provide the following functionalities: a. It should be rack-mountable. b. It should have a minimum of 8 ports scalable up to 24 ports. c. It should support local user port for rack access. d. It should support both USB and PS/2 connections.		

#	Description	Compliance (Y/N)	Remarks
	e. It should be capable of storing usernames and profiles. f. It should support high resolution 1600 x 1200 g. It should be capable to auto scan servers h. It should work on CAT 6 / CAT 7 cables. i. Rack Mountable LCD Monitor with In-built Keyboard & Mouse		
18	IP KVM Switch should have a minimum of 16 ports scalable & upgradeable.		
19	IP KVM Switch should support 2 remote users and 1 user at the rack		
20	IP KVM Switch should support Dual (redundant) Power supply, Dual Ethernet with Failover, PC selection – On screen Display menu hot key, 19 inch Rack mountable design, KVM access over IP		

3.6.2.5 SAN (in case separate hardware is required)

#	Description	Compliance (Y/N)	Remarks
1	Proposed storage should deliver min 150,000 IOPS at 8KB block size from day 1 with 80% Reads and 20% write		
2	The system shall be a scale-out, all-flash NVMe architecture with a modular controller design featuring Dual Active-Active symmetric controllers to ensure high availability and load balancing. Storage should support cluster scale out architecture		
3	Storage should have enterprise class dual ported high performance NVMe TLC SSD drives with the capacity 30TB or less capacity of each drive		

#	Description	Compliance (Y/N)	Remarks
4	Proposed storage should he All Flash that supports high performance NVME SSD Drives that supports high density and high endurance (>0.5+) with capacity 30 TB less		
5	The proposed array must be scalable to at least double of the disks to be required for meeting the solution requirements.		
6	All necessary licenses required to enable supported RAID levels, data/volume replication, DC/DR provisions, and array management features must be provided for the full supported storage capacity of the array. The solution must support RAID levels such as RAID 6 with dual parity support		
7	Must support multiple host interfaces including Fibre Channel (up to 64 Gbps), iSCSI (10/25 Gbps), and NVMe/TCP (up to 100 Gbps		
8	The proposed array shall have no single point of failure, with fully redundant and hot-swappable components. It must support non-disruptive hardware replacement, firmware upgrades, and guarantee 100% availability with built-in redundancy and dynamic drive protection.		
9	The storage system shall have a minimum of 256 GiB cache memory per system to ensure low latency performance. The proposed array must ensure cache data integrity during manual shutdowns or unexpected power outages by automatically destaging cached data to non-volatile media such as flash or disk.		
10	The proposed storage should support all the popular enterprise operating systems.		
11	Offered Storage array shall support heterogeneous storage virtualization (native/external) for vendors like, but not limited to, EMC, HP, IBM, Hitachi, Netapp etc. Storage should be supplied with Unlimited capacity of virtualization license for existing storage. In case of non-native/external		

#	Description	Compliance (Y/N)	Remarks
	component used, it should be supplied in redundant mode with no single point of failure.		
12	The proposed all-flash storage array shall deliver consistent high performance across its entire capacity without requiring auto-tiering between different storage media types.		
13	The proposed array must support storage provisioning based on service level. There should be an option to configure and allocate storage space based on service level i.e. response time required for an application.		
14	The proposed array must provide continuous monitoring and movement of sub-LUN data chunks to provide real-time performance improvements		
15	The storage should be configured with Software/ Hardware Controller based Encryption for data security.		
16	The proposed array should allow control and predictability over the application performance by limiting the performance of applications to a specific IOPS or MB/s quota so that the front-end resources can be accurately partitioned between the applications that share these resources		
17	The proposed storage must provide an audit service to record activities including host-initiated actions, physical component changes, attempts blocked by security control. Audit log should be secure and tamper-proof.		
18	The proposed array must have capability to create target less snapshot for space efficiency, easy administration and minimal performance impact on production volumes		
19	The proposed array must support full copy clones for backup and reporting purposes.		

#	Description	Compliance (Y/N)	Remarks
20	The proposed storage solution should support snapshot capabilities, ensuring efficient data protection and recovery. It must include the necessary software licenses		
21	The Proposed storage system should support Active-Active Storage configuration across two sites replicating to each other for same LUN/volume for zero RPO/zero RTO configuration.		
22	The storage should support both Synchronous and Asynchronous Data Replication to remote site		
23	The proposed storage array should support Three-Data-Center (3DC) replication, ensuring robust disaster recovery and high availability		
24	The proposed storage array should support Three-Data-Center (3DC) replication, ensuring robust disaster recovery and high availability		
25	The proposed array remote replication solution should support incremental failover and failback. There should not be requirement for full data synchronization in any failover and failback scenarios		
26	The proposed array remote replication solution should support consistency group feature to ensure consistency of the data distributed across multiple devices of an application within an array or across homogenous arrays.		
27	Storage management software should be able to Orchestrate and Automate storage configuration operations		
28	The proposed array replication solution should have the software / hardware compression or equivalent capabilities to optimize the replication data to reduce the link bandwidth requirement. Required hardware / software licenses should be part of the solution. This should not have any impact on the performance of the system		

#	Description	Compliance (Y/N)	Remarks
29	Storage management software should be intuitive, browser-based user interface that configures and manages array		
30	Storage management software should be able to manage access controls, user accounts and permission roles		
31	Storage management software should provide interface to allow end users to replace disk drives		
32	Storage management software should provide interface/wizards to perform configuration operations like create LUNs present LUNs to host, set LUN attributes etc.		
33	Storage management software should be able to perform and monitor local and remote replication operations		
34	Storage management software should be able to send notifications for alerts generated in the end to end infrastructure i.e. virtual machines, Host OS, hypervisors, SAN devices, Storage devices		
35	Storage management software should be able to monitor alerts		
36	Should support system management console. Solution should provide: 1. Performance Analytics (Minimum 01 year Historical data & Real-time), 2. Replication monitoring, 3. Management Utilities.Logging. All Licenses required for the features described shall be provided for unlimited capacity.		
37	Storage management software should provide real time monitoring and historical analysis of storage performance		
38	Proposed replication solution should support incremental failover and failback. There should not be requirement for full data synchronization in any failover and failback scenarios		

#	Description	Compliance (Y/N)	Remarks
39	Proposed replication solution should ensure data consistency on the remote storages		
40	The solution shall support inline data reduction with a minimum guaranteed effective ratio of 2:1.		
41	The proposed replication solution must support multi host and multi-array enterprise consistency in an open system environment. Should ensure data consistency for mission and business critical application data that spans across multiple LUNs and Raid groups		
42	The offered storage solution must be able to cater to file, block, and object workloads		
43	Proposed storage should be offered with Usable capacity of 1 PB scalable by minimum 25%. This is an indicative requirement and MSI shall assess the actual requirement		

3.6.2.6 SAN Switch (in case separate hardware is required)

#	Description	Compliance (Y/N)	Remarks
1	The proposed director or chassis-based solution must have complete redundancy in case of failure including hot swappable control plane module/supervisor, fabric modules, fan modules, power supplies, software modules on the OS.		
2	The switch(or director platform) must be able to provide up to 384 - 8/16/32/64-Gbps, 8/16/32/64-Gbps FC or 10-Gbps full line-rate autosensing Fibre Channel ports		
3	The switch(or director platform) should be able to support 64G FC speeds on all its ports at line rate from day1		
4	With the combination of 64-Gbps Fibre Channel switching module and supervisor switching modules it should be		

#	Description	Compliance (Y/N)	Remarks
	capable of enabling up to 3 terabits per second (Tbps) at the aggregate level		
5	The switch must have non-blocking architecture and be capable of dropping bad / corrupt frames at the ingress of the switch		
6	The switch must support the following modules types: • 8/16/32/64 Gbps FC Module • 10 Gbps and FCoE Module • 10G ports of FCIP		
7	All FC ports for device connectivity should be 8/16/32/64 Gbps auto-sensing Fibre Channel ports.		
8	The switch module must support switching across the entire 48-ports on a module as one switched domain. The latency between any two ports chosen within the module or across modules needs to be consistent.		
9	The switch must be able to support non-disruptive software upgrade.		
10	The switch must be able to support stateful process restart.		
11	The switch must support port aggregation of up to 16 physical Fibre Channel ports into a single aggregated link. The aggregated ports must NOT be consecutive ports on a line card and should support distributed model.		
12	Switch should provide comprehensive tool set for analysing, troubleshooting, and debugging storage networks. Power-on self-test (POST) and online diagnostics to proactively monitor system health. Identify the exact path and timing of flows with capabilities such as Fibre Channel traceroute. Capture network traffic using Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) without any limitation.		

#	Description	Compliance (Y/N)	Remarks
14	Proposed switch or via solution should have the capability to provide FC analytics natively on switch ports or via external monitoring agent. The analytics solution should help measure via GUI end2end traffic from host to storage along with Disk Access Latency, Exchange completion times, SCSI related errors etc.. All licenses need to be provided from day one		
15	When analytics is turned on parameters such as disk access latency, exchange time completion, rx/tx rates, etc need to be shown for end to end traffic from server to storage and back.		