Corrigendum – Tender Reference No.: DGRPG/PSDC_DCO/2023/1					
SN	**Tender / ATC Clause No.**	**Page No.**	**Tender / ATC Clause**	**Tender / ATC clause details / specification**	**Revised Clause**
1	5.10	17	Technical Qualification Criteria	**No. of Tier III Data Centers managed by the bidder (excluding bidder's in-house data centers)** 5 marks for each Tier III Data Center subject to a maximum of 20 marks.	**No. of TIA - 942 or ISO/IEC 22237 or (Uptime Tier III or higher) or equivalent certification (consideration of equivalent certification will be at the sole discretion of DGRPG) Data Centers managed by the bidder** 5 marks for each Tier III Data Center subject to a maximum of 20 marks.
2	7.3.2.5.2	37	Application Performance Monitoring & Network Behaviour Analyzer (APM & NBS)	Currently, PSDC is using the Network Behaviour Analyzer solution of Checkpoint which is required to be **upgraded** with APM & NBS	Currently, PSDC is using the Network Behaviour Analyzer solution of Checkpoint which is required to be **upgraded/replaced** with APM & NBS
3	7.3.2.5.4	38	Layer - 3 Switch (Core)	**PSDC is using HP core switch in HA mode which is required to be upgraded. The proposed switch should have at least 48 nos. 10G/25 SFP+ ports 4 x 40G/100G QSFP+ QSFP28 uplink ports and should support 1 RJ-45 serial console port,1 RJ-45 out-of-band management port and 1 USB port.**	Clause stands deleted.
4	Annexure - B	150	EMS/NMS Specifications for 05 Years warranty and AMC support	Proposed solution should have **Out-of-the-Box connectors/ probes** to integrate with multiple EMS solutions, including industry standard solutions from top 10 market leaders for EMS and should also provide mechanisms (XML, APIs etc.) to integrate with other EMS and NMS solutions, to provide an integrated topology and event views and reports to the operator.	Proposed solution should have **Out-of-the-Box connectors/ probes/Rest API's** to integrate with multiple EMS solutions, including industry standard solutions from top 10 market leaders for EMS and should also provide mechanisms (XML, APIs etc.) to integrate with other EMS and NMS solutions, to provide an integrated topology and event views and reports to the operator.

5	Annexure - B	150	EMS/NMS Specifications for 05 Years warranty and AMC support	Proposed EMS/NMS solution must be **ISO 27001:2013 certified** to ensure security compliances.	Proposed EMS/NMS solution must be **ISO 27001:2013 / ISO 27034** certified to ensure security compliances.
6	Annexure - B	150	EMS/NMS Specifications for 05 Years warranty and AMC support	The proposed EMS/NMS solution must be an industry standard, enterprise grade solution recognized by leading analysts (IDC/Gartner/ Forrester) in ITSM, **NPMD & AI Ops reports.**	Clause stands deleted.
7	Annexure - B	151	EMS/NMS Specifications for 05 Years warranty and AMC support	Proposed NMS solution must have at least 3 deployments in Central Government/ Public Sector/State Govt./**PSU`s and Large Enterprise**, out of which one should be in a DC environment, monitoring & managing 10,000+ **network nodes in each of such deployments.**	Proposed solution must have at least 3 deployments in Central Government/ Public Sector/State Govt./**PSU`s / Large Enterprise,** out of which one should be in a DC environment, monitoring & managing 10,000+ **nodes/servers/endpoints accross these three deployments.**
8	Annexure - B.D	155	Helpdesk and IT Service Management	The proposed Helpdesk tool must be ITIL certified on at least 6 processes.	The proposed Helpdesk tool must be ITIL 4 certified.
9	Annexure - B.D	156	Application Performance Management	End to end **Management of applications (J2EE/.NET based)**	End to end **monitoring of the network for the application and its performance.**
10	Annexure - B.D	156	Application Performance Management	Storage of historical data is for problem diagnosis, trend analysis etc.	Storage of historical data is for problem diagnosis, trend analysis etc. **Also the retention period for the same is at least 6 months.**
11	Annexure - B.D	156	Application Performance Management	Should drill down from slow, end-user transactions to the bottlenecked component, **method or SQL statement**, helping to solve memory, exception and other common problems.	Should drill down from slow, end-user transactions to the bottlenecked component, **front end, backend related issues over network** helping to solve memory, exception and other common problems.
12	Annexure - B.D	157	Application Performance Management	**Sniffer Solution** should support store and replay session information for the real user along with snapshots and text pattern events.	**Solution** should support store and replay session information for the real user along with snapshots and text pattern events.
13	Annexure - B.D	157	Application Performance Management	The proposed solution should expose performance of individual SQL statements within problem transactions	Clause stands deleted.

14	Annexure - B.D	157	Application Performance Management	The proposed solution should be JVM & JDK independent, thereby enabling to manage applications on any Java Virtual Machine.	Clause stands deleted.
15	Annexure - B.D	157	Application Performance Management	**Should support J2EE, .NET, SAP, SOA or Siebel Applications**	**The solution should monitor any application based on packet capture at network layer.**
16	Annexure - B.D	157	Application Performance Management	Solution should monitor application performance, availability and usage volume. It should provide breakdown **of user experience by location, username, browser, OS,**	Solution should monitor application performance, availability and usage volume. It should provide breakdown **based on location, username, browser, OS, mobile carrier / ISP, and installed application version etc.**
17	Annexure - B.D	157	Application Performance Management	Solution should support mobile native applications to collect various metrics for mobile networks, such as device type, operating system, mobile carrier, and installed application version. Supported platforms should include iPhone and Android device.	Clause stands deleted.
18	Annexure - B.E	158	Security Incident Management Solution (SIEM)	Solution should encompass log, packet and end point data with added context and threat Intelligence. Should provide complete network visibility through deep **packet inspection high speed packet capture and analysis.**	Solution should encompass log, packet and end point data with added context and threat Intelligence. Should provide complete network visibility through deep **inspection of logs.**
19	Annexure - B.E	159	Security Incident Management Solution (SIEM)	The SIEM & Log Monitoring solution should be from a different OEM than the Prevention Security solutions like F/W, IPS, HIPS, AV, DLP and Encryption, application security	Clause stands deleted.
20	Annexure - B.E	160	Security Incident Management Solution (SIEM)	Solution should support minimum 30,000 EPS scalable to **50,000 at correlation, management and collection layer and packet capture solution should support upto 1GBPS line rate for capturing from network.**	Solution should support minimum 30,000 EPS scalable to **40,000 at correlation, management.**

21	Annexure - B.E	160	Security Incident Management Solution (SIEM)	The solution should be storing both raw logs as well as normalized logs. **Should store RAW packet DATA for 7 days and normalized packet data for 120 days for forensics.**	The solution should be storing both raw logs as well as normalized logs. **Should store for 7 days and normalized data for 120 days for forensics.**
22	Annexure - B.F	160	Antivirus Specifications	Should support Firewall, Anti-Malware, Integrity Monitoring, Application Control and Recommended scan features in single module with agentless and agent based capabilities along with broader range of Operating Systems support **i.e. MS Windows, Red Hat Enterprise Linux, CentOS Linux, Oracle Linux, SUSE Linux, Ubuntu Linux, Debian Linux, Solaris and AIX.**	Should support Firewall, Anti-Malware, Integrity Monitoring, Application Control and Recommended scan features in single module with agentless and agent based capabilities along with broader range of Operating Systems support **i.e. MS Windows & Linux family.**
23	Annexure - B.F	161	Antivirus Specifications	Host IPS should be capable of recommending rules based on vulnerabilities with the help of **virtual patching** and should have capabilities to schedule recommendation scan and entire features of solution should be agentless.	Host IPS should be capable of recommending rules based on vulnerabilities with the help of **patching** and should have capabilities to schedule recommendation scan and entire features of solution should be agentless.
24	Annexure - B.F	161	Antivirus Specifications	Host based IPS should support **virtual patching** both known and unknown vulnerabilities until the next scheduled maintenance window.	Host based IPS should support **patching** both known and unknown vulnerabilities until the next scheduled maintenance window.
25	Annexure - B.F	161	Antivirus Specifications	Proposed solution should be Leader in Server Security Market as **per IDC latest report**.	Clause stands deleted.
26	Annexure B.G	162	Next Generation Firewall	The solution should have atleast **4 X 100/1000/10G Cu, 16 X 1G/10G SFP/ SFP+, 4 X 40G/100G QSFP28 from day 1 with all SFP included. All below requirements should be available from day 1 onwards.**	The solution should have atleast **4 X 1G/10G Cu, 16 X 10G/25G (SFP/ SFP+), 4 X 40G/100G (QSFP/ QSFP+) with all ports fully loaded from day 1.**
27	Annexure B.G	162	Next Generation Firewall	The appliance hardware should be a multicore CPU architecture with a hardened 64 bit operating system to support higher memory **and should support minimum of 64 GB of RAM or more.**	The appliance hardware should be a multicore CPU architecture with a hardened 64 bit operating system to support higher memory. **Also, must have minimum 128 GB of RAM or more.**

28	Annexure B.G	162	Next Generation Firewall	Firewall Solution should have at least 5 Lakh new sessions per second	Firewall Solution should have at least 5 Lakh new sessions per second **or minimum 3,80,000 new Layer 7 sessions per second**
29	Annexure B.G	162	Next Generation Firewall	Firewall Solution should have at least **32M Maximum sessions and concurrent sessions**	Firewall Solution should have at least **32M Concurrent sessions** **-OR- at least 7.2 million Layer-7 Concurrent Sessions.**
30	Annexure B.G	162	Next Generation Firewall	**Redundant power supply is available along with 1200 W AC or DC (1:1 fully redundant) , 100–240 VAC (50–60 Hz)**	**1:1 fully redundant AC power supply.**
31	Annexure B.G	162	Next Generation Firewall	Firewall solution based on **3U space** design form factor	Firewall solution based on **upto 3U space** design form factor.
32	Annexure B.G	162	Next Generation Firewall	The proposed solution must have atleast 240 GB SSD RAID1 at storage level	Clause stands deleted.
33	Annexure B.G	162	Next Generation Firewall	Firewall Solution should have at least 2TB log capability	Firewall Solution should have at least 2TB log capability **internally along with support for scalable external storage (eg: SAN/RAID) feature.**
34	Annexure B.G	163	Next Generation Firewall	Proposed Solution must support User identification and control such as **VPNs, WLAN controllers, captive portal, proxies, Active Directory, eDirectory, Exchange, Terminal Services, syslog parsing, XML API**	Proposed Solution must support User identification and control such as **VPNs, captive portal, proxies, Active Directory, eDirectory, Exchange, Terminal Services, XML API**
35	Annexure B.G	163	Next Generation Firewall	Proposed Solution **must support Virtual systems** such as logical, separately managed firewall instances within a single physical firewall, with each virtual system’s traffic kept **separate**	Proposed Solution **must at least 10 Virtual systems** such as logical, separately managed firewall instances within a single physical firewall, with each virtual system’s traffic kept **separate and scalable virtual systems.**
36	Annexure B.G	163	Next Generation Firewall	Solution must support Networking feature such as dynamic routing (RIP, OSPF, BGP, multiprotocol BGP), DHCP, DNS, NAT, route redistribution, ECMP, LLDP, **tunnel content inspection**	Solution must support Networking feature such as dynamic routing (RIP, OSPF, BGP, multiprotocol BGP), DHCP, DNS, NAT, route redistribution, ECMP, LLDP, **tunnel inspection & Deep packet inspection**

37	Annexure B.G	164	Next Generation Firewall	Solution must be scalable management of minimum up to 30,000 hardware and all VM-Series Firewalls; role-based access control; logical and hierarchical device groups; and templates	Clause stands deleted.
39	Annexure - B Non It Components	168	Supply, installation, testing and commissioning of BMS	RACK PDU (5 points per unit) - 34+8	Intelligent Rack PDU should have following specs:- a) 3 phase 16AMP b) Support 11KW load c) Minimum 30 no’s C13 and 6 no’s C19 socket for power distribution to IT equipment d) Should be mounted vertically in rear of rack occupying 0U space e) UL certified
40	Annexure - B Non It Components	196	Precision Air Conditioner/ Compressor	PAC should be equipped with Latest-generation **hermetic** scroll compressors	PAC should be equipped with Latest-generation **hermetic / variable** scroll compressors
41	Annexure - B Non It Components	196	Precision Air Conditioner/ Refrigerating circuits (air-cooled DX versions)	**Each circuit is composed of, as standard, a fluid intake complete with a Rota lock on-off cock and safety valve, a dehydrating filter and flow sensor. The former enables** the refrigerating circuit to be kept free of humidity (thus increasing the life of all the circuit's components), while the latter enables a rapid check on whether the system is charged with refrigerant correctly and whether it contains any humidity.	**Each circuit should be designed so as to enable** the refrigerating circuit to be kept free of humidity (thus increasing the life of all the circuit's components), and to keep a rapid check on whether the system is charged with refrigerant correctly and whether it contains any humidity.
42	Annexure - B Non It Components	212	Data Center Infrastructure Management Systems (DCIMS) / Cluase no. C	The system shall monitor SNMP/Modbus TCP devices and manage Inventory for at least **4 Racks**.	The system shall monitor SNMP/Modbus TCP devices and manage Inventory for at least **42 Racks**.

43	Annexure - B Non It Components	213	Data Center Infrastructure Management Systems (DCIMS) / Cluase no. D.9	Proposed system shall offer **web services (WSDL, REST, SOAP) to allow** integration of the DCIM system to third party Customization platforms. Vendor must submit a detailed Schema documentation for the same.	Proposed system shall offer **web services to allow** integration of the DCIM system to third party Customization platforms. Vendor must submit a detailed Schema documentation for the same.
44	Annexure - B Non It Components	213	Data Center Infrastructure Management Systems (DCIMS) / Cluase no. D.10	DCIM server/VM system should allow integration of client email server via SMTP channel as well as it should support integration to SMS Gateway servers by utilizing the **HTTP post method**.	DCIM server/VM system should allow integration of client email server via SMTP channel as well as it should support integration to SMS Gateway servers by utilizing the **HTTP/HTTPS post method**.

45	Annexure - B Non It Components	215	Data Center Infrastructure Management Systems (DCIMS) / Cluase no. F.9	To ensure data security for any vendor proposing **cloud based** solution following rules would apply: 1. Flow of information over IP will be allowed using **HTTPS TLS 1.2** encrypted outbound connections on port 443. 2. All connections from the **Cloud based** monitoring gateway to OEM DCIM Monitoring cloud should be validated using an industry standard 2048-bit RSA certificate and data is encrypted in transit using **128-bit AES encryption**. 3. To prevent unauthorized or even malicious access to OEM -**DCIM Cloud system**, all parts of the cloud engine should be protected by state-of-the-art firewalls. In addition, this cloud network should be configured to only allow access from specific sources (using Access Control Lists), and only a limited set of authorized personnel to have access – and only through multi-factor authentication. Preference will be given to systems **offering Mobile based OTP Two factor authentication.**	To ensure data security for any vendor proposing on **premises / cloud based** solution following rules would apply: 1. Flow of information over IP will be allowed using **HTTPS or TLS 1.3** encrypted outbound connections on port 443. 2. All connections from the **on premises / cloud based** monitoring gateway to OEM DCIM Monitoring cloud should be validated using an industry standard 2048-bit RSA certificate and data is encrypted in transit using **(128 / 256) bit AES encryption**. 3. To prevent unauthorized or even malicious access to OEM -**DCIM on premises / cloud based system**, all parts should be protected by state-of-the-art firewalls. In addition, this cloud network should be configured to only allow access from specific sources (using Access Control Lists), and only a limited set of authorized personnel to have access – and only through multi-factor authentication. Preference will be given to systems **offering multi factor authentication**.
46	Annexure - B Non It Components	215	OEM Qualifications	**ISO 9001, ISO 14001, ISO 50001**	**ISO 9001, ISO 14001, ISO 50001 or ISO/IEC 27001**

47	7.4.13	43	PSDC Website	The selected bidder shall develop a dedicated website for Punjab State Data Centre (PSDC) for providing digital e-services delivery platform **within 3 months** of signing of contract	The selected bidder shall develop a dedicated website for Punjab State Data Centre (PSDC) for providing digital e-services delivery platform **within 6 months** of signing of contract
48	10.7.a.1	79	SLA for O&M of PSDC	Description - Go-live of PSDC website / portal Timeline - **T + 3 months**	Description - Go-live of PSDC website / portal Timeline - **T + 6 months**
49	7.3.2	36	Upgradation of the PSDC	Additional point (clause no.: 7.3.2.8)	IT components mentioned in the scope are required to be upgraded or replaced as per the given specifications.
50	7.3.2	36	Upgradation of the PSDC	Additional point (clause no.: 7.3.2.9)	The specifications given in Annexure - B for the non-IT components are applicable only in case a new component is required to be installed or existing component is required to be replaced
51	7.3.2.1	36	Upgradation of the PSDC	**In case of any downtime during upgradation, any alternate arrangement to maintain data center operations shall be borne by the successful bidder.**	**Any downtime during upgradation shall be planned in consultaion with DGRPG. Service levels will be applicable for the downtime beyond the approved schedule.**
52	11.4	94	Fiancial Bid Form	-	Refer Updated Commercial Sheet.
53	3.1.17	8	Definitions	“Similar Work” means Setup / Operation & Management of ISO 27001 & ISO 20000 certified Data Centers **(excluding bidder’s in-house data centers) having a minimum capacity of 15 racks.**	“Similar Work” means Setup / Operation & Management of ISO/IEC 27001 & ISO/IEC 20000 certified Data Centers.
54	5.2	12	Earnest Money Deposit (EMD)	Earnest Money Deposit (EMD) through online mode - Rs. 5,00,000/- (Rs. Five Lakh Only)	Earnest Money Deposit (EMD) through online mode - Rs. 5,00,000/- (Rs. Five Lakh Only) **Earnest Money Deposit to be exempted for Public Sector Undertakings (PSUs)**

55	5.10	16	Technical Qualification Criteria TQ 2	Successfully completion of “similar work” (minimum 15 rack) in government (departments/ boards/ corporations/ PSUs/ Societies) or Large reputed Enterprise in the last 10 years as on 31.12.2022. 5 marks for each project subject to a maximum of 20 marks. **Note - Bidder’s in house Data Centre’s shall not be considered unless used for commercial use.**	Successfully completion of “similar work” (minimum 15 rack) in government (departments/ boards/ corporations/ PSUs/ Societies) or Large reputed Enterprise in the last 10 years as on 31.12.2022. 5 marks for each project subject to a maximum of 20 marks.
56	5.14.1	20	Performance security	As soon as possible, but not more than 20 days after the issue of Letter of Intent (LoI), the successful bidder shall furnish **performance security @10% of the contract value** to DGRPG as performance security.	As soon as possible, but not more than 20 days after the issue of Letter of Intent (LoI), the successful bidder shall furnish **performance security @7% of the contract value** to DGRPG as performance security.
57	6.11.2	28	Subcontracting by Data Centre Operator	**Under all circumstances, the value of the works sub-contracted by the service provider should not exceed 40% of the Facility Management Services prices.** It is clarified that the service provider shall be the principal employer for all claims arising from the liabilities statutory or otherwise, concerning the subcontractors, and shall, notwithstanding such sub-contract (or any approval thereof by the Authority) continue to be liable for any work or services provided by any subcontractors. The service provider undertakes to indemnify the Authority from any claims on the grounds stated hereinabove. The service provider shall not allow a sub-contractor to assign or enter into further secondary subcontract for any of the work to be carried out by the subcontractor. For avoidance of doubt, service provider shall not be allowed to sub-contract the entire Project/work/Services.	It is clarified that the service provider shall be the principal employer for all claims arising from the liabilities statutory or otherwise, concerning the subcontractors, and shall, notwithstanding such sub-contract (or any approval thereof by the Authority) continue to be liable for any work or services provided by any subcontractors. The service provider undertakes to indemnify the Authority from any claims on the grounds stated hereinabove. The service provider shall not allow a sub-contractor to assign or enter into further secondary subcontract for any of the work to be carried out by the subcontractor. For avoidance of doubt, service provider shall not be allowed to sub-contract the entire Project/work/Services.

58	5.1	10	Eligibility / pre-qualification criteria	The Bidder should hold valid certificates for ISO 9001, ISO- 20000 & ISO-27001	The Bidder should hold **at least 2 out of following 3** valid certificates i.e. ISO 9001 / ISO- 20000 / ISO-27001
59	7.4.42.1.5	65	AMC of IT infrastructure in PSDC	Additional Point	Service Provider shall provide OEM support till End of Support of equipment is declared from the OEM. Post that service provider can provide third party support and SLAs will be applicable in both cases.
60	Annexure - B	308	14. Technical specifications for IPDUs	Additional Point	Intelligent Rack PDU should be 3 phase 16AMP must support 11KW load have minimum 30 no's C13 and 6 no's C19 socket for power distribution to IT equipment and should be mounted vertically in rear of rack occupying 0U space,UL certified
	Annexure - B	308	15. Technical specifications of DG set	Additional Point	Annexure - A of this Corrigendum
61	6.12.1	29	Insurance	**All the PSDC equipment's and services provided by the service provider shall be fully insured against loss or damage incidental to manufacture or acquisition, transportation, storage, delivery and installation.**	**The bidder shall provide comprehensive insurance coverage for all scope assets against any and all types of incidents, including but not limited to fire, theft, riots, earthquake, accidental fire suppression system release, and cyber attacks, for the entire duration of the project. The insurance coverage shall be in compliance with all relevant Indian laws and regulations and shall include coverage for any damages or losses incurred by the client or any third parties due to the bidder's actions or inactions. The bidder shall provide proof of insurance coverage and maintain it throughout the project duration.**
62	7.3.2.5.7	39	IBMS	Integrated Building Management System (IBMS) - PSDC is using IBMS for monitoring of all non-IT equipment (energy meter, DG set parameter, UPS parameter, FAS, WLD, VESDA etc.) using Siemens software (DIGIGOCC) and same is required to be **upgraded.**	Integrated Building Management System (IBMS) - PSDC is using IBMS for monitoring of all non-IT equipment (energy meter, DG set parameter, UPS parameter, FAS, WLD, VESDA etc.) using Siemens software (DIGIGOCC) and same is required to be **upgraded / replaced.**

63	Annexure - B.G.30	162	Next Generation Firewall (NGFW)	Solution must have minimum operating temperature from **0° to 50° C.**	Solution must have minimum operating temperature from **0° to 40° C.**
64		197	Electronic Expansion Valve	**Electronic Expansion Valve (EEV)** controlled by the microprocessor with special software created and tested by the manufacturer shall be provided.	**Electronic Expansion Valve (EEV) /TXV** controlled by the microprocessor with special software created and tested by the manufacturer shall be provided.
65		197	Electrical Heating	Electric heating with aluminum-finned heating elements **(minimum 15 Kw rating in multistage arrangement)**,	Electric heating with aluminum-finned heating elements
66	7.3.2.5.8	39	Upgradation to Tier III	PSDC is currently a Tier II Data Centre. Service Provider shall undertake all the required upgradation activities, not included in the points above, so that PSDC is enhanced to Tier III standards. Service Provider shall also be responsible for getting **"Uptime" certification for Tier III**. Bidders shall provide separate rates for all the activities involved for Tier III upgradation in the financial bid including that of certification. Payment for the same will be made post PSDC Tier III certification.	PSDC is currently a Tier II **compliant** Data Centre. Service Provider shall undertake all the required upgradation activities, not included in the points above, so that PSDC is enhanced to Tier III standards. Service Provider shall also be responsible for getting **Tier III certification from Uptime for design and construction**. Bidders shall provide separate rates for all the activities involved for Tier III upgradation in the financial bid including that of certification. Payment for the same will be made post PSDC Tier III certification.
67	7.3.3.3	40	Final Acceptance Testing	During the FAT, the Service Provider shall be required to demonstrate the features / facilities / functionalities of all the components **installed / upgraded**.	During the FAT, the Service Provider shall be required to demonstrate the features / facilities / functionalities of all the components **installed / upgraded including that of upgradation to Tier - III standards**.

68	9.1.2	76	Project Implementation and Payment Schedule	Milestone - Operation and Maintenance of SDC before FAT. Description - Operations and Maintenance for **3 months** starting from the fourth month. Timeline (in months) - **T + 6** Payable - **100%** of the price quoted for O&M before FAT in the **Financial bid**. (In case of delay in FAT, the O&M cost will be paid on proportional basis for the delay period subject to SLA)	Milestone - Operation and Maintenance of SDC before FAT. Description - Operations and Maintenance for **6 months** starting from the fourth month. Timeline (in months) - **T + 9** Payable - **50%** of the price quoted for O&M before FAT in the **Financial bid per quarter**. (In case of delay in FAT, the O&M cost will be paid on proportional basis for the delay period subject to SLA)
69	9.1.3	76	Project Implementation and Payment Schedule	Milestone - Final Acceptance Test. Description - FAT of all the Installed and Commissioned Infrastructure. Timeline (in months) - **T + 6**	Milestone - Final Acceptance Test. Description - FAT of all the Installed and Commissioned Infrastructure. Timeline (in months) - **T + 9**
70	9.1.4	76	Project Implementation and Payment Schedule	Milestone - PSDC Tier III certification. Description - Successful completion of Tier III Uptime certification of PSDC. Timeline (in months) - **T + 6**	Milestone - PSDC Tier III certification. Description - Successful completion of Tier III Uptime certification of PSDC. Timeline (in months) - **T + 9**
71	9.1.5	76	Project Implementation and Payment Schedule	Milestone - Operation and Maintenance of SDC after FAT (i.e. of existing portion of SDC as well as upgraded portion). Description - Operations and Maintenance for 60 months (from the date of successful completion of FAT). Timeline (in months) - **T + 66**	Milestone - Operation and Maintenance of SDC after FAT (i.e. of existing portion of SDC as well as upgraded portion). Description - Operations and Maintenance for 60 months (from the date of successful completion of FAT). Timeline (in months) - **T + 69**
72	10.6.1	79	10.6 SLA for Upgradation of PSDC	Description - Completion of Final Acceptance Test (FAT) Activities / Deliverables - FAT report Timeline (in months) - **T + 6**	Description - Completion of Final Acceptance Test (FAT) Activities / Deliverables - FAT report Timeline (in months) - **T + 9**
73	11.4	95	Financial Bid Form	Opex cost (mentioned at sr. no. - 3, 4 & 5) cannot be less than capital cost (mentioned at sr. no. - 1 and 2).	Total capital expenditure (mentioned at sr. no. - 1 & 2 combined) cannot be more than 'Opex Cost for PSDC after FAT for 60 months' (mentioned at sr. no. 4).

74	5.10	17	Technical Bid Evaluation	Largest ‘Similar Work’ executed by the bidder in terms of racks. Above 36 Racks: 20 Marks 26 to 35 Racks: 14 Marks 16 to 25 Racks: 7 Marks	Largest ‘Similar Work’ executed by the bidder in terms of racks. Above 36 Racks: 15 Marks 26 to 35 Racks: 10 Marks 16 to 25 Racks: 5 Marks
75	5.10	17	Technical Bid Evaluation	Additional Point TQ 6	Technical Qualification Criteria - Valid certification for ISO 9001, ISO- 20000 and ISO-27001 - 5 Marks Max Marks : 5

TECHNICAL SPECIFICATIONS OF DCC DG SET **(Annexure – A)**

S. No	Description
1	Supply and install of 1010KVA/ 808KW, 415V minimum, 3 Phase, 4 wire, 50 Hz Continuous Power (Data Centre Continuous – DCC) rated Diesel Generator.
2	The diesel engine shall be of robust type with suitable BHP, cylinders, totally enclosed, continuous duty, direct fuel injection, turbo charged compression ignition, complete with its self-contained lubricating system. Engine and alternator shall be mounted on MS base frame structure. The base frame shall be fixed over anti-vibration mounts with proper spacing. Engine Makes: Cummins (Jakson)/ CAT (TIPL)/ MTU
3	The engine shall be water-cooled through radiator as specified in data sheet. The Blower fan and cooling water circulation pump shall be engine driven
4	A fuel day tank shall be provided on a suitably fabricated steel platform. The tank shall be fabricated out of 2mm thick MS Sheet, complete with level indicator.
5	415V, 0.8pf alternator shall be Self-ventilated, Screen protected & drip proof, Salient pole, Brushless & Revolving field type, Self-excited & Self-regulating type. The main and exciter winding shall be Class H insulated.
6	The Genset controller should be an integrated microprocessor-based generator set controller providing monitoring, metering, and control system. The control provides an operator interface to the Genset, digital voltage regulation, digital governing, and generator set protective functions.
7	Design Consideration: Ambient temperature: 40 deg C Altitude above mean sea level: ≤500 mtrs.
8	Exhaust piping should be with LRB rock wool of proper density along with aluminum sheet cladding to avoid heat dissipation. The thickness of lagging should not be less than 50mm. Exhaust piping shall be suitably supported and padded to avoid damage to thermal insulation. Aluminum cladding should be with Aluminum sheet or with minimum 24SWG thickness.
9	Starting battery sets of 24 V, heavy- duty high performance shall be provided to enable crank & start the engine even in cold/winter morning conditions. The battery shall be capable of performing at least (3) three normal starts without recharging and maintenance free. Battery Make: Cummins/ As per OEM recommendation

10	Performance requirement: The D.G. set shall operate up to 100% of load, without undue vibration and noise. Warranty against manufacturing failure of 5 Major components comprising of Crank Shaft, Cam Shaft, Cylinder Head, Cylinder Block and Connecting Rod for 5 Years.
11	Testing: The Bidder shall carryout successfully on load test run in all completely assembled DG Sets for one hour at 100% load at DG manufacturers works prior to dispatch. For routine tests, certificates to be submitted
12	Testing at Site: Contractor shall carry out the entire work of erection, testing and commissioning of equipment supplied under this package and performance and guarantee tests to be conducted at the site and included under the scope of this specification.
13	Major components of genset like engine, alternator, batteries, turbo charger preferably should be of single make.

Response to Queries (RTQ) – Tender Reference No.: DGRPG/PSDC_DCO/2023/1

SN	Firm's Name	Tender / ATC Clause No.	Page No.	Tender / ATC Clause	Tender / ATC clause details/specification	Amendment Sought / Suggestion	Justification	PSeGS response
1	CMS Computers Limited	3.1.17	8	Definitions	"Similar Work" means Setup / Operation & Management of ISO 27001 & ISO 20000 certified Data Centers (excluding bidder's in-house data centers) having a minimum capacity of 15 racks.	We request you to kindly amend this clause as below: "Similar Work" means Setup / Operation & Management of ISO 27001 certified Data Centers (excluding bidder's in-house data centers) having a minimum capacity of 15 racks.		Refer Corrigendum
2	Netcon,Mapl World	5.1	10	Eligibility / pre-qualification criteria	The bidder should have positive net worth and average annual turnover of more than Rs. 200 crores for any three of last five financial years reported i.e. till FY 2021-22.	**Netcon:** We request you to change the clause as follows for fair competition: The bidder should have positive net worth and average annual turnover of more than **Rs. 100 crores** for any three of last five financial years reported i.e. till FY 2021-22. **Mapl World:** The bidder should have positive net worth and average annual turnover of more than Rs. **180 crores** for any three of last five financial years reported i.e. till FY 2021-22	We request you to change the clause as follows for fair competition.	As per RFP
3	Sify	5.1	10	Eligibility / pre-qualification criteria	The Bidder should hold valid certificates for ISO 9001, ISO- 20000 & ISO-27001	We request to amend the clause as The Bidder should hold at least 3 out of following 4 valid certificates i.e. ISO 9001 / ISO- 20000 / ISO-27001 / CMMi Level 5		Refer Corrigendum

4	Mapl World, TechAgeis	5.1	10	Eligibility / pre-qualification criteria	**Mapl World**: Bidders should have successfully completed "similar work" in government (departments/ boards/ corporations/ PSUs/ Societies) / Large reputed Enterprise during the last five years ending 31.12.2022. ● One similar work costing not less than the amount equal to Rs. 30 crore. OR ● Two similar works each costing not less than the amount equal to Rs. 25 crore each. OR ● Three similar works each costing not less than the amount equal to Rs. 15 crore each.	**Mapl World**: Successfully completion of "similar work" of IT/ITES executed in government (departments/ boards/ **TechAgeis**: Need confirmation if Non govt PO will be considered here.	It allows wider participation	**Mapl World:** As per RFP **TechAgeis:** Yes
5	TechAgeis	5.1	11	Eligibility / pre-qualification criteria	Pre-Qualification checklist along with reference page and submitted documents.	Need clarity on what is mentioned in the checklist to check the eligibility		Checklist to be submitted as per clause - 5.1.2

6	Railtel	5.2	12	Earnest Money Deposit (EMD)	EARNEST MONEY DEPOSIT (EMD) OF RS. 5,00,000/- (RUPEES FIVE LACS ONLY):	Earnest Money Deposit to be exempted for Public Sector Undertakings (PSUs) participating in the bid as per Justification given	It is certified and declared that RailTel Corporation of India Ltd (A Mini Ratna Category-I enterprise) is a Central PSU under the Ministry of Railways, Government of India and was incorporated in Sept., 2000. 1) Exemption clause as per the policy of Government of India in vogue: Under GFR Rule 2017 (iii), Rule No. 170: Provision of Bid Security Declaration in place of EMD. General terms and conditions on GeM 3.0 (Version 1.13):	Refer Corrigendum
7	Mapl World	5.4.6	13	Preparation of Bid	The bids submitted by a consortium of companies/firms or any subcontractors will be rejected	Please allow consortium.	It will allow wider participation	As per RFP

8	HPE	5.6.1	14	Validity of bids	Bids shall remain valid till 180 (one hundred and eighty) days from the date of submission of bids. DGRPG reserves the right to reject a proposal valid for a shorter period as non-responsive	Bids shall remain valid till 60 (sixty) days from the date of submission of bids. DGRPG reserves the right to reject a proposal valid for a shorter period as non-responsive.	The prices quoted for the products and services are dynamic in nature which will keep changing in short periods of time. Due to this, 180 days' period is quite long and hence the request for reduction of the validity to 60 days.	As per RFP
9	Netcon, TechAgeis, CMS Computers Limited	5.10	16	Technical bids evaluation	Average annual turnover of bidder in India for any three of last five financial years reported i.e. till FY 2021-22 ▪ Above 400 Crores: 20 Marks ▪ >300 Crores & <=400 Crores: 15 Marks ▪ >=200 Crores & <=300 Crores: 10 Marks	**NetCon**: We request you to change the clause as follows for fair competition: Average annual turnover of bidder in India for any three of last five financial years reported i.e. till FY 2021-22 ▪ Above 100 Crores: 20 Marks ▪ >75 Crores & <=100 Crores: 15 Marks ▪ >=50 Crores & <=75 Crores: 10 Marks **Tech Ageis**: ▪ Above 240 Crores: 20 Marks >180 Crores & <=240 Crores : 15 Marks ▪ >=120 Crores & <=180 Crores: 10 Marks **CMS Computers Limited**: Average annual turnover of bidder in India for any three of last five financial years reported i.e. till FY 2021-22 ▪ Above 250 Crores: 20 Marks ▪ >=200 Crores & <=250 Crores: 15 Marks	**NetCon**: request you to change the clause as follows for fair competition. **CMS Computer Limited**: The project like O&M of such data centre, the requsite Turnover is on very higher side. Request you to kindly amend	As per RFP

10	Railtel, Mapl World, TechAgeis, CMS Computers Ltd	5.10	16	Technical Qualification Criteria	Successfully completion of “similar work” (minimum 15 rack) in government (departments/ boards/ corporations/ PSUs/ Societies) or Large reputed Enterprise in the last 10 years as on 31.12.2022. 5 marks for each project subject to a maximum of 20 marks. Note - Bidder’s in house Data Centre’s shall not be considered unless used for commercial use.	**Railtel**: Clarification is required: Whether Data Centre Racks Placed by Customer as Colocation in bidder's in-house Data Centre shall be considered or not under this criteria? **Mapl World**: Successfully completion of “similar work” of IT/ITES executed in government (departments/ boards/ corporations/ PSUs/ Societies) or Large reputed Enterprise in the last 10 years as on 31.12.2022 **Tech Ageis**: Remove the “rack” clause. We have PO for server, storage and network devices. **CMS Computers Ltd**:We request you to modify the criteria inline with PQ criteria Successfully completion of “similar work” (minimum 15 rack) in government (departments/ boards/ corporations/ PSUs/ Societies) or Large reputed Enterprise in the last 10 years as on 31.12.2022. One similar work costing not less than the amount equal to Rs. 30 crore. or Less than 50 Crore -- 10 Marks One similar work costing not less than the amount equal to Rs. 50 crore. or Less than 75 Crore -- 15 Marks	**Railtel**: The amendment is requested to be considered as Colocation of Data Centre Racks in a Data Centre is equivalent to Own Data Centre. May kindly confirm/clarify. **Mapl World**: This will allow wider particiaption	**Railtel** - Refer Corrigendum **Rest** - As per RFP

11	Railtel,Sify, Tech Ageis, CMS Computers Ltd	5.10	17	Technical Qualification Criteria	No. of Tier III Data Centers managed by the bidder (excluding bidder's in-house data centers) 5 marks for each Tier III Data Center subject to a maximum of 20 marks.	**Railtel**: No. of Tier III Data Centers managed by the bidder (excluding bidder's in-house data centers) 5 marks for each Tier III Data Center subject to a maximum of 20 marks. **Sify**: No. of Tier III Data Centers managed by the bidder (includes bidder's in-house data centers which is 100% for commercial use) **Tech Ageis**: Non Compliant Need to remove **CMS Computers Ltd**: We request you to amend this clause as below No. of Data Centers with ISO 27001 managed by the bidder (excluding bidder's in-house data centers) 10 marks for each ISO 27001 certified data centre Center subject to a maximum of 20 marks.	**Railtel**: This component carries Significant Weightage in the bid and since the Evaluation is on QCBS method (70% TS & 30% FS). This is requested to be amended by deleting the word Tier III from the criteria as this shall not be affecting the overall outcome of the bid as per Scope of Work/Similar Work.	Refer Corrigendum
12	Mapl World, Tech Ageis	5.10	17	Technical bids evaluation	Largest 'Similar Work' executed by the bidder in terms of Racks. ▪ Above 36 Racks: 20 Marks ▪ 26 to 35 Racks: 14 Marks ▪ 16 to 25 Racks: 7 Marks	**Mapl World**: Successfully completion of "similar work" of IT/ITES executed in government (departments/ boards/ **Tech Ageis**: Remove the "rack clause" Change to: 1 PO more than 90 cr : 20 marks 1 PO more than 38 Cr: 14 marks 1 PO more than 15 Cr : 7 marks	It will allow wider participation	As per RFP

13	HPE, Railtel	5.14.1	20	Performance security	As soon as possible, but not more than 20 days after the issue of Letter of Intent (LoI), the successful bidder shall furnish performance security @10% of the contract value to DGRPG as performance security.	**HPE**: As soon as possible, but not more than 20 days after the issue of Letter of Intent (LoI), the successful bidder shall furnish performance security @3% of the contract value to DGRPG as performance security. **Railtel**: As soon as possible, but not more than 20 days after the issue of Letter of Intent (LoI), the successful bidder shall furnish performance security 3% of the contract value to DGRPG as performance security.	**HPE**: The value of the PBG at 10% is quite high considering the nature of the tender. PBG of 3% is commensurate with the tender and hence we have requested for reduction of the PBG amount. **Railtel**: As per enclosed OM No. F.9/4/2020-PPD dt. 30.12.2021 issued by Ministry of Finance , Governement of India regarding Performance Guarantee, it is clarified that the Performance	Refer Corrigendum

14	HPE	5.14.2	20	Performance security	PBG shall remain valid for a period of 180 (one hundred eighty) days beyond the expiry of the contract. Whenever the contract is extended, Service Provider will have to extend the validity of PBG proportionately.	PBG shall remain valid for the period of the contract. Whenever the contract is extended, Service Provider will have to extend the validity of PBG proportionately.	The PBG is obtained by the customer for ensuring performance of the contract by the bidder. Therefore, the PBG should expire at the time of expiry of the contract and not beyond such expiry.	As per RFP

15	HPE	5.14.5	20	Performance security	DGRPG shall forfeit the performance security in full or in part in the following cases: 5.14.5.1 When the terms and conditions of contract are breached/ infringed. 5.14.5.2 When a contract is being terminated due to non-performance of the Service Provider. 5.14.5.3 The DGRPG incur any loss due to Service Provider’s negligence in carrying out the project implementation as per the agreed terms & conditions.	DGRPG shall forfeit the performance security in full or in part in the following cases: 5.14.5.1 When the terms and conditions of contract are materially breached/ infringed and the material breach/infringement is not cured within a period of 3 months from the date of notice in that regard. 5.14.5.2 When a contract is being terminated due to non-performance of the Service Providernd where such non-performance has crossed the maximum cap of liquidated damages/penalty. 5.14.5.3 The DGRPG incur any loss due to Service Provider’s negligence in carrying out the project implementation as per the agreed terms & conditions.	PBG should be only invoked if material breach is not cured after a 3 months' notice or the maximum cap on liquidated damages has been breached and the same has to be recovered from the bidder upon termination. Invocation of PBG should be only done as a last resort and for uncured material breach and not for any breach or non-performance.	As per RFP

16	HPE	6.3	23	Termination of contract for default	DGRPG can terminate the contract in the event of default of terms and conditions of this tender or the subsequent contract by the other party by giving 3 months' written notice. In such a case, the provisions under the Exit Management clause shall apply.	DGRPG can terminate the contract in the event of material default of terms and conditions of this tender or the subsequent contract by the other party by giving 3 months' written notice to cure such material default which remains uncured. In such a case, the provisions under the Exit Management clause shall apply.	The contract should be termination only if there is a material default by the bidder of terms of the tender or the contract and not for any breach. Further, the notice of 3 months provided to the bidder should be for cure of the material default which if cured shall result in continuation of the contract.	As per RFP

17	HPE	6.8.1.2	27	Resolution of disputes	Arbitration: In case dispute arising between the DGRPG and the Service Provider, which has not been settled amicably, the Service Provider can request the DGRPG to refer the dispute for Arbitration under Arbitration and Conciliation Act, 1996 and amendments thereof. Such disputes shall be referred to the Arbitrator which shall be “Administrative Secretary, DGRPG”. However, the Service Provider may request for changing the arbitrator, which shall be appointed by Hon’ble Punjab and Haryana High Court. The Indian Arbitration and Conciliation Act, 1996 and any statutory modification or re-enactment thereof, shall apply to these arbitration proceedings. Arbitration proceedings will be held at Mohali. The decision of the arbitrator shall be final and binding upon both the parties. All arbitration awards shall be in writing and shall state the reasons for the award. The expenses of the arbitration as determined by the arbitrator shall be borne equally by the DGRPG and the Service Provider. However, the expenses incurred by each party in	Arbitration: In case dispute arising between the DGRPG and the Service Provider, which has not been settled amicably, the Service Provider can request the DGRPG to refer the dispute for Arbitration under Arbitration and Conciliation Act, 1996 and amendments thereof. Such disputes shall be referred to a sole Arbitrator mutually appointed by the parties failing which such arbitrator shall be appointed by Hon’ble Punjab and Haryana High Court. The Indian Arbitration and Conciliation Act, 1996 and any statutory modification or re-enactment thereof, shall apply to these arbitration proceedings. Arbitration proceedings will be held at Mohali. The decision of the arbitrator shall be final and binding upon both the parties. All arbitration awards shall be in writing and shall state the reasons for the award. The expenses of the arbitration as determined by the arbitrator shall be borne equally by the DGRPG and the Service Provider. However, the expenses incurred by each party in connection with the preparation, presentation and litigation shall be borne by the party itself.	Any dispute referred to arbitration should be adjudicated by an arbitrator who is independent and not related to any of the parties. While we assume fairness and equity, the independece of “Administrative Secretary, DGRPG” may be questioned. Hence, we suggest that arbitration be conducted by a sole Arbitrator mutually appointed by the parties failing which such arbitrator shall be appointed by Hon’ble Punjab	As per RFP

18	HPE	6.11.2	28	Subcontracting by Data Centre Operator	Under all circumstances, the value of the works sub-contracted by the service provider should not exceed 40% of the Facility Management Services prices. It is clarified that the service provider shall be the principal employer for all claims arising from the liabilities statutory or otherwise, concerning the subcontractors, and shall, notwithstanding such sub-contract (or any approval thereof by the Authority) continue to be liable for any work or services provided by any subcontractors. The service provider undertakes to indemnify the Authority from any claims on the grounds stated hereinabove. The service provider shall not allow a sub-contractor to assign or enter into further secondary subcontract for any of the work to be carried out by the sub-contractor. For avoidance of doubt, service provider shall not be allowed to sub-contract the entire Project/work/Services.	Under all circumstances, the value of the works sub-contracted by the service provider should not exceed 40% of the Facility Management Services prices. It is clarified that the service provider shall be the principal employer for all claims arising from the liabilities statutory or otherwise, concerning the subcontractors, and shall, notwithstanding such sub-contract (or any approval thereof by the Authority) continue to be liable for any work or services provided by any subcontractors. The service provider undertakes to defend and settle any claims on the grounds stated hereinabove with prompt notification and cooperation by the Authortity with the bidder having sole contol of such defence. The service provider shall not allow a sub-contractor to assign or enter into further secondary subcontract for any of the work to be carried out by the sub-contractor. For avoidance of doubt, service provider shall not be allowed to sub-contract the entire Project/work/Services.	In the event that there is a claim from a sub-contractor or sub-contractor employees, then the bidder should be allowed to defend and settle such claims without having to indemnify the authority. Such defence shall be undertaken with prompt notification and cooperation by the authority.	Refer Corrigendum
19	HPE	6.11.1	28	Subcontracting by Data Centre Operator	The service provider may subcontract non-IT work but IT related work shall not be subcontracted.	The service provider may subcontract non-IT work and IT related work without dissolving any responsibility of the bidder for managing delivery and SLA.		As per RFP

20	HPE	6.11.2	28	Subcontracting by Data Centre Operator	Under all circumstances, the value of the works sub-contracted by the service provider should not exceed 40% of the Facility Management Services prices.	Under all circumstances, the value of the works sub-contracted by the service provider should not exceed 70% of the Facility Management Services prices.		Refer Corrigendum
21	HPE	6.12.1	29	Insurance	All the PSDC equipment's and services provided by the service provider shall be fully insured against loss or damage incidental to manufacture or acquisition, transportation, storage, delivery and installation.	All the PSDC equipment's and services provided by the service provider shall be fully insured against loss or damage incidental to manufacture or acquisition, transportation, storage, delivery and installation until the time and delivery of the installation. Once the equipment and services are installed, insuring such equipment shall be the responsibility of DGRPG.	The bidder's obligation to insure the products and services supplied should be upto the tome of installation of the products and not beyond considering the ownership and risk would transfer to the DGPRG. Upon installation, DGPRG should be responsible for obtaining insurance.	Refer Corrigendum
22	Sify	7.1.2	30	Scope of Work	Architecture of existing PSDC is as under	As per diagram, there are checkpoint NIPS & FW deployed in existing diagram. Kindly suggest, will be use existing FW & IPS along with new NGFW procured under this RFP scope?		As per RFP

23	Sify	7.2.3.4	32	Handing Over Taking Over (HOTO)	Data Privacy & Security	Kindly suggest what is the expectation in respect of data privacy? Are we expecting any security control?		Yes, we do expect all vendors to comply with our data privacy and security requirements, including appropriate security controls to safeguard any data shared with you. Please refer to the RFP document for further details.

24	Sify	7.3.1.6	34	Upgradation of the Data Centre	Service Provider shall install hot and cold aisles in the server farm area.	As per site condition, it will be either cold/hot aisle in the server farm. Kindly clarify.		The Service Provider is required to set up a specific layout in the server farm area that involves separating hot air exhaust from cool air intake in order to optimize cooling efficiency and maintain an appropriate temperature for the equipment. This layout is commonly referred to as "hot and cold aisles".

25	iVAlue,Sify	7.3.18.4	35	Security	Security - The entire system provides an end-to-end security blanket to protect applications, services, data and the infrastructure from intentional, unintentional or malicious attacks or theft from external (through internet) and internal (through intranet and or physical) hackers/thieves. Such attacks and theft should be controlled and well supported using Firewalls, IPS/IDS systems and infrastructure protection mechanisms. The virus and worm attacks should be well defended with Gateway level Anti-virus system, along with workstation level Anti- virus mechanism. SDC also endeavors to make use of the SSL/ VPN technologies to have secured communication between Applications and its end users. Furthermore, all the system logs properly stored & achieved for future analysis and forensics whenever desired as per data retention policy.	Providing end to end security PSDC must consider a dedicated database activity monitoring tool as suggested below:		As per RFP
26	iVAlue,Sify		35		DAM Suggested	The Solution should meet regulatory compliance such as RBI guidelines on cyber security, SOX, PCI DSS, Data Privacy Law, GDPR, Industry best practices etc.		As per RFP
27	iVAlue,Sify		35		DAM Suggested	Creation of an inventory through auto discovery of all databases and database users, deployed across the enterprise.		As per RFP
28	iVAlue,Sify		35		DAM Suggested	The proposed DAM solution should be able to monitor in scope database without dropping any log.		As per RFP

29	iVAlue,Sify		35		DAM Suggested	Discovery of sensitive data in input and Masking of sensitive data in output.		As per RFP
30	iVAlue,Sify		35		DAM Suggested	When scaling the solution, the solution must support a scale-out approach by having only to add more licenses as needed with the increase of databases.		As per RFP
31	iVAlue,Sify		35		DAM Suggested	The solution should provide optimum utilization of resources by using Load balancing between its devices, if it is using multiple boxes/gateways		As per RFP
32	iVAlue,Sify		35		DAM Suggested	The product should comply and support both IPv4 and IPv6		As per RFP
33	iVAlue,Sify		35		DAM Suggested	The solution must have temper-proof log storage capability.		As per RFP
34	iVAlue,Sify		35		DAM Suggested	The proposed solution required monitoring should be delivered while solution is enabled and in blocking mode		As per RFP
35	iVAlue,Sify		35		DAM Suggested	The solutions should support Virtual patching of database for known missing patches		As per RFP
36	iVAlue,Sify		35		DAM Suggested	The solution should support creation of policies/rules for enforcing access control and proper rights management on databases.		As per RFP
37	iVAlue,Sify		35		DAM Suggested	The solution must support Reporting of deviations to the policies and access control		As per RFP
38	iVAlue,Sify		35		DAM Suggested	Solution should continuously learn the user and application behaviour in respect of accessing database. Learning should be a continuous process and should not stop after a certain stage.		As per RFP

39	iVAlue,Sify		35		DAM Suggested	Solution should provide risk score of individual databases, based on combination of security alerts, discovery results, vulnerability assessment, sensitivity & confidentiality of data stored in the database.		As per RFP
40	iVAlue,Sify		35		DAM Suggested	Solution must monitor privileged user access or local SQL activity that does not cross the network such as Bequeath, IPC, Shared Memory, or Named Pipes		As per RFP
41	iVAlue,Sify		35		DAM Suggested	DAM solution should identify abnormal server and user behaviour and providing early detection of possible attacks using outliers. For example: • User accessing a table for the first time User selecting specific data in a table that he has never selected before • Exceptional volume of errors • Activity that itself is not unusual, but its volumeis unusual • Activity that itself is not unusual, but the time of activity is unusual.		As per RFP
42	iVAlue,Sify		35		DAM Suggested	Solution must support filtering/hiding of the bind variables of all the SQL activities captured		As per RFP
43	iVAlue,Sify		35		DAM Suggested	The solution should not store sensitive data in plain text in logs generated by the application (e.g. passwords)		As per RFP
44	iVAlue,Sify		35		DAM Suggested	Logs and audit-trail generated by the solution should not be editable by users/ administrator and should be read-only		As per RFP

45	iVAlue,Sify		35		DAM Suggested	The Proposed Solution should support automatic updates to the signature database and based on global threat intelligence, ensuring complete protection against the latest threats.		As per RFP
46	iVAlue,Sify		35		DAM Suggested	The Proposed Solution should support custom security rules. Administrators should be able to define rules for the positive or negative security model and to create correlation rules with multiple criteria.		As per RFP
47	iVAlue,Sify		35		DAM Suggested	The solution must be able to perform content scanning for regular expression and patterns and should monitor nested queries		As per RFP
48	iVAlue,Sify		35		DAM Suggested	Communication from Agent to management server must be encrypted		As per RFP
49	iVAlue,Sify		35		DAM Suggested	Solution must be able to monitor database which run on non-standard port		As per RFP
50	iVAlue,Sify		35		DAM Suggested	Solution should able to auto classify the database/database-objects based on sensitivity and confidentiality of data based on PII, SPDI, PCIDSS guidelines or customized parameters.		As per RFP

51	iVAlue,Sify		35		DAM Suggested	The solution should be capable of auto discovering sensitive/confidential data, like credit card Numbers, Aadhaar or any PII in the database and offers the ability for customization. The solution should be capable of auto discovering sensitive/ confidential data, like Aadhaar or any PII in the database and offers the ability for customization.		As per RFP
52	iVAlue,Sify		35		DAM Suggested	The solution should be able to auto discover privilege users in the database and should support user entitlement reviews on database accounts		As per RFP
53	iVAlue,Sify		35		DAM Suggested	The solution should be able to auto discover default passwords in the default DB accounts		As per RFP
54	iVAlue,Sify		35		DAM Suggested	Solution track the dormant accounts as per defined rule.		As per RFP
55	iVAlue,Sify		35		DAM Suggested	The solution should inspect both in-coming and out-going DB traffic, compare with the rules and generate alert.		As per RFP
56	iVAlue,Sify		35		DAM Suggested	Solution should detect attacks on network protocols, operating systems, as well as application layer DB activity.		As per RFP
57	iVAlue,Sify		35		DAM Suggested	Solution should capture and analyse all database activity, from both application user and privileged user accounts, providing detailed audit trails that shows the “Who, What, When, Where, and How” of each transaction.		As per RFP

58	iVAlue,Sify		35		DAM Suggested	The solution should provide full details needed for analysis of audited events: date and time, raw SQL, parameters used, end user name, source IP, source application, destination database instance, schema DB objects affected, command details, results generated, values affected etc. should be capable of capturing and reporting at a very granular level.		As per RFP
59	iVAlue,Sify		35		DAM Suggested	Solution should detect attacks attempting to exploit known vulnerabilities as well as common threat vectors and can be configured to issue an alert and\or terminate the session in real time		As per RFP
60	iVAlue,Sify		35		DAM Suggested	The solution should discover misconfigurations in the database and its platform and suggest remedial measures.		As per RFP
61	iVAlue,Sify		35		DAM Suggested	The solution should be capable of reporting missing patches and report the details of such patches and vulnerabilities associated with.		As per RFP
62	iVAlue,Sify		35		DAM Suggested	The solution should be able to virtually patch the know vulnerabilities automatically till a patch is installed for the same.		As per RFP
63	iVAlue,Sify		35		DAM Suggested	Solution should have capability to track execution of stored procedures, including who executed a procedure, what procedure name and when, which tables were accessed.		As per RFP

64	iVAlue,Sify		35		DAM Suggested	Solution should also able to detect any change happens in stored procedure		As per RFP
65	iVAlue,Sify		35		DAM Suggested	Solution should have capability to monitor local access & encrypted connections (Oracle ASO, SSL, IPSec etc.)		As per RFP
66	iVAlue,Sify		35		DAM Suggested	The solution should provide full details needed for analysis of audited events: *Date and time, raw SQL, parameters used, end user name, source IP, source application, destination database instance, schema DB objects affected, command details, results generated, values affected etc. should be capable of capturing and reporting at a very granular level*		As per RFP
67	iVAlue,Sify		35		DAM Suggested	The solution should provide facilities for scheduling of reports with respect to time, type of activity, nature of event, violation of specific rules, user, source of origin, DB instance etc.		As per RFP
68	iVAlue,Sify		35		DAM Suggested	Ability to mask or obfuscate Sensitive data in the result sets to the user.		As per RFP
69	iVAlue,Sify		35		DAM Suggested	The solution support creation of different type of security and audit policies such as rule, report based on heuristic and content based. These policies should support customization.		As per RFP
70	iVAlue,Sify		35		DAM Suggested	Ability to kill sessions for accessing sensitive data/policy violations and keeping all activity in the logs		As per RFP

71	iVAlue,Sify		35		DAM Suggested	The solution should be capable of blocking access real time, execution of commands which violate the rules/ policies, store the events securely and report the same in real time.		As per RFP
72	iVAlue,Sify		35		DAM Suggested	The Proposed Solution should support Monitoring Mode and blocking Mode of Deployment. In monitoring mode, solution can generate alerts for unauthorized activity. In blocking mode, solution must proactively block the queries including blocking of matching signatures for known attacks like SQL injection.		As per RFP
73	iVAlue,Sify		35		DAM Suggested	The solution should support installation of agents, update of agents, configurations updates, policy updates, start/ stop/restart etc at all the databases from management server centrally.		As per RFP
74	iVAlue,Sify		35		DAM Suggested	There should be no down-time of the OS or database for deployment of agents.		As per RFP
75	iVAlue,Sify		35		DAM Suggested	The agent should not require a reboot of OS and DB after installation / configuration. Only one agent to be installed, no third-party agents permitted. All agents regardless of deployment mode should be managed from the centralized management console. The solution should not use any 3rd Party software/support for any purpose		As per RFP

76	iVAlue,Sify		35		DAM Suggested	If the agent mal-functions or uninstalled or disabled on server, immediate alert to be issued.		As per RFP
77	iVAlue,Sify		35		DAM Suggested	If the communication between agent and the console is lost, immediate alert to be issued.		As per RFP
78	iVAlue,Sify		35		DAM Suggested	The solution should not use the native database audit functionality. The Solution should not employ native database transaction log auditing.		As per RFP
79	iVAlue,Sify		35		DAM Suggested	The solution should be able to support/monitor all database activities in Oss like AIX, UNIX, HP UNIX, Linux, Solaris, Windows and Databases like Oracle, MS-SQL, MySQL, postgress at a minimum.		As per RFP
80	iVAlue,Sify		35		DAM Suggested	DAM solution should support integration with the Big Data platform and Data warehouse such as Exadata etc		As per RFP
81	iVAlue,Sify		35		DAM Suggested	The solution should provide information of DB links and should have capability to monitor the activity of DB links		As per RFP
82	iVAlue,Sify		35		DAM Suggested	The solution should generate alert for any violation of security policy real time		As per RFP
83	iVAlue,Sify		35		DAM Suggested	All the reports should be generated at least time (within 120 seconds)		As per RFP
84	iVAlue,Sify		35		DAM Suggested	The solution should discover all the databases with details i.e. IP, type, OS, available in the customer network		As per RFP
85	iVAlue,Sify		35		DAM Suggested	The solution should also discover if any new database and DB objects created within the monitored network/systems.		As per RFP

86	iVAlue,Sify		35		DAM Suggested	The solution must allow administrators to add and modify policies.		As per RFP
87	iVAlue,Sify		35		DAM Suggested	The solution should log the actual client IP.		As per RFP
88	iVAlue,Sify		35		DAM Suggested	The solution should auto profile the activities to filter noise or known false positives and should generate alert if any violation		As per RFP
89	iVAlue,Sify		35		DAM Suggested	The solution support individual user access auditing for packaged applications like SAP, Peoplesoft etc., which the orginzation proposes to implement in future.		As per RFP
90	iVAlue,Sify		35		DAM Suggested	Separate policies should be applied for different databases configured in DAM		As per RFP
91	iVAlue,Sify		35		DAM Suggested	The solution should have pre-built templates for well-known security and audit policies.		As per RFP
92	iVAlue,Sify		35		DAM Suggested	Customer’s all databases are to be integrated without any limitation on the number of databases. Solution should support the deployment modes i.e. monitoring / blocking separately for each database.		As per RFP
93	iVAlue,Sify		35		DAM Suggested	The resource overhead (hardware, software) for the agent should not exceed 5% of the normal requirement of the CPU. There should be only one agent.		As per RFP
94	iVAlue,Sify		35		DAM Suggested	The solution should provide CPU, RAM, disk capping capabilities on agent-based solution		As per RFP

95	iVAlue,Sify		35		DAM Suggested	The solution should have capability to facilitate rule creation at a very granular level. Example: Which user can connect from which source, access what objects, have which rights, at what time window etc.		As per RFP
96	iVAlue,Sify		35		DAM Suggested	Rules also should allow blocking access depending upon different parameters like above.		As per RFP
97	iVAlue,Sify		35		DAM Suggested	The Proposed Solution should include a Web based single administration interface.		As per RFP
98	iVAlue,Sify		35		DAM Suggested	The Proposed solution should have an out-of-band management capability.		As per RFP
99	iVAlue,Sify		35		DAM Suggested	The Proposed Solution should be managed centrally for Both DC & DR Setup.		As per RFP
100	iVAlue,Sify		35		DAM Suggested	Management solution should support Role-Based Access Control or multiple user roles that facilitate separation of duties. i.e. Administrator (Super-User), Manager, read only etc.		As per RFP
101	iVAlue,Sify		35		DAM Suggested	The solution should support the following authentication mechanism for accessing the solution:		As per RFP
102	iVAlue,Sify		35		DAM Suggested	(i) In-built authentication in the solution		As per RFP
103	iVAlue,Sify		35		DAM Suggested	(ii) Kerberos authentication		As per RFP
104	iVAlue,Sify		35		DAM Suggested	(iii) LDAP/AD authentication		As per RFP
105	iVAlue,Sify		35		DAM Suggested	(iv) RADIUS authentication		As per RFP
106	iVAlue,Sify		35		DAM Suggested	The solution must be able to operate in FIPS (Federal Information Processing Standard) 140-2 compliance mode.		As per RFP

107	iVAlue,Sify		35		DAM Suggested	The customer should be able to deploy or remove the DAM solution from the network with no impact on the existing databases or the network architecture.		As per RFP
108	iVAlue,Sify		35		DAM Suggested	Support proper reporting and logging facilities.		As per RFP
109	iVAlue,Sify		35		DAM Suggested	Should be able to report events and alerts via standard mechanisms, for example, to a syslog or SNMP server or a SIEM solution.		As per RFP
110	iVAlue,Sify		35		DAM Suggested	The solution must support the creation of custom log messages and provide system variable placeholders mechanism to make this use case possible. For example, the Username placeholder looks like (${Alert.username})		As per RFP
111	iVAlue,Sify		35		DAM Suggested	The solution must support generation/ both predefined as well as custom built reports as per customer's requirements with both tabular views, pdf and data analysis graphical views.		As per RFP
112	iVAlue,Sify		35		DAM Suggested	The solution should have easy option to customize report without developing or require lot of customization/changes from scratch		As per RFP
113	iVAlue,Sify		35		DAM Suggested	Alert should be generated in case of violation of rules through SMTP (mail).		As per RFP
114	iVAlue,Sify		35		DAM Suggested	The solution should provide facilities for scheduling of reports with respect to time, type of activity, nature of event, violation of specific rules, user, source of origin, DB instance etc.		As per RFP
115	iVAlue,Sify		35		DAM Suggested	The solution should be able to generate the reports in PDF, Excel & CSV formats		As per RFP

116	HPE	7.3.2.1	36	Upgradation of the PSDC	In case of any downtime during upgradation, any alternate arrangement to maintain data center operations shall be borne by the successful bidder.	Down time should be in Change management process, duly approved by DGRPG	Since the application and process owner is DGRPG.	Refer Corrigendum
117	HPE, Sify	7.3.2.5.1	37	Upgradation of the PSDC	Upgradation of Rack Power of existing DC - Existing DC was planned with 42 Racks and 4 KVA load which is required to be augmented. Minimum new load to be considered is 10 KVA per rack with at least 15 min. backup, necessary non-IT Infra needs to be replaced and installed with 5 years support. Service providers should upgrade cables, PDU, containment, fiber runner, cooling etc. to meet the requirement without any downtime on working days.	**HPE** - Completed Infrastructure need to revised with new ,capacity not limited to Rack's capacity but its carrier cables, panels, PDUs, Sockets, UPS etc. DGRPG shall provide required downtime during change. **Sify**: As per our understanding, HT Panel, Transformer, DG, DG panel, LT panel as per required demand load and Tier-III requirement will be provided by Customer. Kindly confirm.	Complete overhauling of Basic infra will required comprehensive planning with cost and time.	**HPE** - Refer Corrigendum **Sify** - DGRPG shall be responsible for transformer level support, rest shall be provided by service provider.
118	Sify	7.3.2.5.2	37	Upgradation of the PSDC	Application Performance Monitoring & Network Behaviour Analyzer (APM & NBS)	Kindly share specs for APM. Also do you want APM from checkpoint only or third-party solution will work.		Refer Corrigendum
119	Sify	7.3.2.5.5	38	Upgradation of the PSDC	Next Generation Firewall (NGFW)	in case 12200 product is going end of life then can bidder propose same or different make/model of NGFW with same configuration?		As per RFP

120	Sify, UpTime Institute	7.3.2.5.8	39	Upgradation of the PSDC	Upgradation to Tier III - PSDC is currently a Tier II Data Centre. Service Provider shall undertake all the required upgradation activities, not included in the points above, so that PSDC is enhanced to Tier III standards. Service Provider shall also be responsible for getting "Uptime" certification for Tier III. Bidders shall provide separate rates for all the activities involved for Tier III upgradation in the financial bid including that of certification. Payment for the same will be made post PSDC Tier III certification.	**Sify**: Kindly confirm, whether Tier III uptime certification applicable for all phases like design, built and O&M. **UpTime Institute**:Please note that PSDC is not a Tier II Certified DC by Uptime Institute. You may mention it as Tier II Complaint for information purposes. We do not know the gaps in your current facility and thus estimation of work to be carried out as per Tier III by the Contractor might hamper the overall cost and there could be gaps in the actual budgeting Recommended Scope of Work to be included as a part of Certification work to be carried out by the Contractor or SI 1. Tier Certification of Design Documents - Design Certification 2. Commissioning Plan + Commissioning Script 3. Tier Certification of Constructed Facility Readiness - Support Service for the Main Construction Certification 4. Tier Certification of Constructed Facility - Contruction or Build Certification 5. Preliminary Operational Sustainability - Support Service for the Main Operational Sustaianbility Certification		As per RFP
121	Sify	7.3.2.5.6	39	Upgradation of the PSDC	Endpoint Security	1- Kindly suggest, can we propose single OEM solution for all end points? 2- Nos. of qty.		As per RFP
122	HPE	7.3.3.2	40	Final Acceptance Testing	Prerequisite for carrying out FAT activity: All components (IT & non IT) must be installed / upgraded at PSDC site as per the scope and the bid submitted by Service Provider.	Non-IT and IT infra to be considered separately for milestone.	There will be a delay in non-it infra readiness before the IT configuration.	As per RFP

123	HPE	7.4.6	42	Operation and Management of PSDC	Licensing: DCO has to provide/maintain all adequate number of licenses (for SDC users etc.) of software which shall be valid for the project period. The DCO has to produce evidence to DGRPG of the licenses taken over from the existing DCO.	How many users are there as of now and what is expected number of users at the fag end of project.		Users here means the team to be provided by DCO.
124	Sify	7.14.3	43	PSDC website	What kind of CCTV footage required? Can we change CCTV setup technically?	Integration of all systems on website is still to be accessed.	Period of 3 months is not realistic. Time duration can be given after due deligence.	Scope will be freezed after contract signing.
125	Sify	7.14.3	43	PSDC website	How rack space be displayed as "LIVE" on website?	Need to be clarified	After Mutual discussion needs to be added.	Scope will be freezed after contract signing.
126	Sify	7.14.3	43	PSDC website	Who will give storage and compute for CCTV footage systems?	Need to be clarified		Scope will be freezed after contract signing.
127	Sify	7.14.3	43	PSDC website	How many days of footage of CCTV required?	Integration of all systems on website is still to be accessed.	Period of 3 months is not realistic. Time duration can be given after due deligence.	Scope will be freezed after contract signing.
128	Sify	7.14.3	43	PSDC website	Who will define Rate card?	Integration of all systems on website is still to be accessed.	Period of 3 months is not realistic. Time duration can be given after due deligence.	Scope will be freezed after contract signing.

129	Sify	7.14.3	44	PSDC website	Invoicing needs to be done manually or Automated?	Integration of all systems on website is still to be accessed.	Period of 3 months is not realistic. Time duration can be given after due deligence.	Scope will be freezed after contract signing.
130	Sify	7.4.14.2.8	45	MIS reports	Patch release update	Kindly suggest is there any tool available for patch management?		Scope will be freezed after contract signing.
131	HPE	7.4.15.1.10	47	System Administration, Maintenance & Management Services	Troubleshoot problems with web services, applications software, desktop/server relationship issues and overall aspects of a server environment. Problems shall be logged in the Help Desk and resolved as per the SLAs defined in this tender.	Do you need this helpdesk to be setup onsite at the customer location/		Refer clause no.: 7.6.3
132	HPE	7.4.16.1.7	48	Network Management	Provide information on performance of capacity utilization of network devices installed in SDC.	What is current tool for network monitoring. Hope there is tool for getting the capacity utilisation reports.		CA Spectrum is being used.
133	HPE	7.4.17.3	48	Security Incident & Event Management	Monitoring of various devices / tools such as firewall, intrusion detection, content filtering and blocking, virus protection, and vulnerability protection	What is current tool for these moniotring activities.		"ArcSight" is being used.
134	Sify	7.4.19	51	IT Security Administration Services	IT Security Administration Services	Is there any ISMS process documentation available or not? Kindly suggest		To be taken from current DCO during HOTO process.

135	Sify	7.4.20	52	Virus Management	Virus Management	Is there any virus management documentation available or not? Kindly suggest		It's a part of complete ISMS repository (ISO27001) managed by current DCO.
136	Microfocus, Orbitindia, RahInfotech,Sify	7.4.25	54	Application Monitoring	7.4.25.1.8 Application Security Certificate 7.4.25.1.10 Subdomain and Domains registration on DGRPG request.	Please elaborate the requirement for these two categories.	We would like to understand the exact monitoring requirement and use cases so that we can propose the right fit solution.	1. The purpose is only monitorning of both the categories which is required for logs / reports /data/artifacts. 2. DCO is not expected to undertake security audit of department applications. 3. DCO will be responsible to manage & maintain DNS

137	HPE	9.1.5	76	Project Implementation and Payment Schedule	Operation and Maintenance of SDC after FAT (i.e. of existing portion of SDC as well as upgraded portion) Operations and Maintenance for 60 months (from the date of successful completion of FAT) T+66 0.5% of the price quoted for capex/upgradation and Tier III upgradation cost in the Financial bid per quarter from the date of starting of O&M phase subject to submission of Tier III Uptime certificate. 5% of the price quoted for Opex Cost for PSDC after FAT in the Financial bid	Bidder request that, O&M cost for 60 months to be paid monthly in arrears, NT 30 days		As per RFP
138	HPE	9	76	Project Implementation and Payment Schedule	Project Implementation and Payment Schedule	There is no delivery schedule mentioned in the RFP document. Project Start date, duration and project schedule, payment terms should be clearly established		Please refer clause no.: 9.1.
139	HPE	8	76	Project Implementation and Payment Schedule	Schedule and timelines	As mentioned T+3 is HOTO inclusive of upgradation. FAT and acceptance for non-it and IT is T+6 including the Tier III certification. The T+3 ok for HOTO, but T+6 is requested to increase T+11 (3 for Hoto, 3 for certification post Design approval from Agency and 3 months for overlapped period to deliver, install, test and commission of equipment followed by IT configuration. Note : the Downtime in existing PSDC purely derive the post material delivery. an assumption of 2 month is taken)		Refer Corrigendum

140	Sify	9.1	76	Project Implementation and Payment Schedule	Payment schedule for SDC upgradation	We request to amend the payment schedule for SC upgradation as follows 1. Supply / delivery of SDC upgradation equipment's - 70% of the price quoted for capex / upgradation cost (except for the Tier III upgradation cost) 2. Installation and Commissioning - 20% of the price quoted for capex / upgradation cost (except for the Tier III upgradation cost) 3.Final Acceptance Test -10% of the price quoted for capex / upgradation cost (except for the Tier III upgradation cost) 4. PSDC Tier III certification - 100% post Successful completion of Tier III Uptime certification of PSDC.	This project requires one time investment on IT / non IT equipment refresh / upgradation. Milestone based payment will help in balancing the cash inflow / outflow during implementation phase. Secondly successful bidder will be submitting PBG, hence withholding 10% of CAPEX investment will be additional burden on the cash inflow / outflow.	As per RFP

141	HPE	9.2	77	Project Implementation and Payment Schedule	Payments will be made subject to verification and clearance from the Third Party Agency (TPA) as and when appointed.	Payments will be made subject to verification and clearance from the Third Party Agency (TPA) as and when appointed. All payments to the bidder shall be made within 30 days from the date of invoice.	The RFP does not provide for a timeline by when the payments will be made. There has to be a specific timeline for payments and hence this change.	As per RFP
142	HPE	9.2	77	Project Implementation and Payment Schedule	Payment - verification and clearance from the Third Party Agency (TPA) as and when appointed	We will issue PI and issue the final invoice after the confirmation from TPA		As per RFP

143	HPE	10	78	SLA and Liquidated Damages	SLA and Liquidated Damages	We request that the following clause be added as a generic clause : Liquidated damages or penalties under the contract shall be subject to a maximum cap of 3% of the delayed portion of supply or services	Liquidated damages and penalties should be commensurate with the scope of work and type of work of the bidder. Hence, there has to be a maximum cap of 3% of the delayed services as LDs and penalties are levied only if services are delayed and should accordingly be levied to the extent of delayed supply or services.	As per RFP
144	HPE	10.6	79	SLA for Upgradation of PSDC	(Maximum amount of liquidated damages shall be 10% of upgradation cost)	Bidder request that, overall LD to be capped at 10% for including HOTO,		As per RFP
145	HPE	10.7	79	SLA for O&M of PSDC		Bidder request that, overall SLA to be capped at 10% of quarterly value during O&M phase		As per RFP
146	iValue, Sify	10.6	85	Security and Incident Management	Denial of Service Attack - Non-availability of any services shall be analyzed and forensic evidence shall be examined to check whether it was due to external DoS attack.	Thease days disributed denial of services attacks increasing day by day. To secure services outage requesting you to kind include DDoS protection as suggested below:		As per RFP

147	iValue, Sify		85		DDOS Protection Suggestion	Proposed appliance must be purpose built DDoS prevention system and should be stateless technology not having any kind of state limitation such as TCP connections etc.		As per RFP
148	iValue, Sify		85		DDOS Protection Suggestion	Proposed appliance should be a dedicated appliance based solution (not a part of Router, UTM, Application Delivery Controller, IPS, Load Balancer, Proxy based architecture or any Stateful Device)		As per RFP
149	iValue, Sify		85		DDOS Protection Suggestion	System should have High Performance Architecture with purpose built-in hardware to ensures that attack mitigation does not affect normal traffic processing.		As per RFP
150	iValue, Sify		85		DDOS Protection Suggestion	System should support Legitimate Traffic of 5 Gbps from Day 1 on the same appliance which should be scalable upto 40Gbps in future with license upgrade		As per RFP
151	iValue, Sify		85		DDOS Protection Suggestion	Solution should Detect misuse of application protocols in the network like HTTP/DNS/VoIP/Mail/VPN/File/Login		As per RFP
152	iValue, Sify		85		DDOS Protection Suggestion	Solution should be transparent bridge to pass 802.Q tagged frames and other control protocols VLAN, L2TP,IP in IP and GRE traffic.		As per RFP
153	iValue, Sify		85		DDOS Protection Suggestion	In inline mode system must not modify MAC or IP addresses of passed frames		As per RFP
154	iValue, Sify		85		DDOS Protection Suggestion	Solution should inspect ,detect and mitigate IPV4 & IPv6 Attacks		As per RFP
155	iValue, Sify		85		DDOS Protection Suggestion	Solution should support all 64k TCP and UDP ports		As per RFP
156	iValue, Sify		85		DDOS Protection Suggestion	Solution should support for all 255 protocols at layer 3		As per RFP

157	iValue, Sify		85		DDOS Protection Suggestion	Solution should support L3-L7 IP-inside-GRE Inspection		As per RFP
158	iValue, Sify		85		DDOS Protection Suggestion	System should prevent malware propagation attacks		As per RFP
159	iValue, Sify		85		DDOS Protection Suggestion	Should support standard network MTU.		As per RFP
160	iValue, Sify		85		DDOS Protection Suggestion	Proposed appliance should support Maximum DDoS Flood Prevention Rate up to 35 Million packet per seconds. This performance figure must be mentioned in public facing datasheet.		As per RFP
161	iValue, Sify		85		DDOS Protection Suggestion	System should support Multiple Segment protection up to 6 Segments		As per RFP
162	iValue, Sify		85		DDOS Protection Suggestion	The device operating system should be hardened and the responsibility shall fall on OEM to ensure the same		As per RFP
163	iValue, Sify		85		DDOS Protection Suggestion	System should support, In-Line, Out-of-Path deployments modes from day 1		As per RFP
164	iValue, Sify		85		DDOS Protection Suggestion	The system should support deployment on a "logical link bundle" interfaces through Link aggregation protocols like LACP (802.1AX and 802.3ad)		As per RFP
165	iValue, Sify		85		DDOS Protection Suggestion	DDoS Mitigation System should support Symmetric and Asymmetric Traffic flows		As per RFP
166	iValue, Sify		85		DDOS Protection Suggestion	System should have a Scalable Clean Throughput License approach for Legitimate Traffic. System should support Clean Throughput License Scalability upto 40 Gbps on the same appliance with a license upgrade. 5Gbps clean throughput license to be provided from day 1		As per RFP
167	iValue, Sify		85		DDOS Protection Suggestion	Solution should be truly stateless should be quoted with two stand alone appliances to create a redundant architecture.		As per RFP

168	iValue, Sify		85		DDOS Protection Suggestion	System should support 8x10G fibre bypass capable protection ports from day 1 and should support 2x40G fibre port for future scalability within the same appliance. All ports should support internal fail open and fail close configuration without the use of external bypass switch dependency.		As per RFP
169	iValue, Sify		85		DDOS Protection Suggestion	The appliance should support Hardware and Software Bypass Capability with both fail open and fail closed modes in all protection ports (including Copper and Fiber). The hardware bypass for all protection interface types (Copper and Fiber) should be In-Built in the Appliance.		As per RFP
170	iValue, Sify		85		DDOS Protection Suggestion	Proposed appliance should have High performance architecture with purpose builtin hardware to mitigate against the sophisticated threats and should not be ASIC to avoid dependency on the ASIC chips for future upgrades.		As per RFP
171	iValue, Sify		85		DDOS Protection Suggestion	Should support latency less than 85 microseconds. Latency should be documented in datasheet		As per RFP
172	iValue, Sify		85		DDOS Protection Suggestion	Should Support dual redundant Hot-Swappable AC power supplies from day one		As per RFP
173	iValue, Sify		85		DDOS Protection Suggestion	System should have 2 x AC redundant, hot swap capable power supplies with AC Power rating of 100 to 240 VAC, 12/6 A max		As per RFP
174	iValue, Sify		85		DDOS Protection Suggestion	Devices must be rack-mountable in standard 42U Rack		As per RFP

175	iValue, Sify		85		DDOS Protection Suggestion	Solution should support Hardware and Software Bypass capability to achieve faster network convergence in Resilient Deployment		As per RFP
176	iValue, Sify		85		DDOS Protection Suggestion	Device should be fully integrated with an organization’s existing security stack.		As per RFP
177	iValue, Sify		85		DDOS Protection Suggestion	Should have ready API for SDN environment integration/ Anti-DDoS system for attack mitigation in custom portal		As per RFP
178	iValue, Sify		85		DDOS Protection Suggestion	Integration with RADIUS and TACACS+		As per RFP
179	iValue, Sify		85		DDOS Protection Suggestion	Solution must support REST API management		As per RFP
180	iValue, Sify		85		DDOS Protection Suggestion	Device should integrate with existing SIEM engine seamlessly through Syslog messages (CEF,LEEF)		As per RFP
181	iValue, Sify		85		DDOS Protection Suggestion	Solution should support SNMP v2/v3 MIB and Traps		As per RFP
182	iValue, Sify		85		DDOS Protection Suggestion	DDoS solution should integrate with Network performance & monitoring solution.		As per RFP
183	iValue, Sify		85		DDOS Protection Suggestion	System should have capability to consume and integrate with 3rd Party feeds (IOCs) via STIX/TAXII inbuilt integration capability		As per RFP
184	iValue, Sify		85		DDOS Protection Suggestion	Supports Integration with SOAR		As per RFP
185	iValue, Sify		85		DDOS Protection Suggestion	The proposed solution should support integration with an external Threat Intelligence Platform (TIP)		As per RFP
186	iValue, Sify		85		DDOS Protection Suggestion	Proposed Anti-DDoS Appliance should have In-Built GUI based Monitoring, Configuration Management, Diagnostics and Reporting capabilities without the need of a Central Management System		As per RFP

187	iValue, Sify		85		DDOS Protection Suggestion	The system must have a dedicated management port for Out-of-Band management; Management interfaces must be separated from traffic interfaces. System management must not be possible on traffic interfaces, management interfaces must not switch traffic.		As per RFP
188	iValue, Sify		85		DDOS Protection Suggestion	Device management interface must be firewalled internally.		As per RFP
189	iValue, Sify		85		DDOS Protection Suggestion	The system must support configuration via standard up to date web browsers.		As per RFP
190	iValue, Sify		85		DDOS Protection Suggestion	The system must support configuration via standard up to date web browsers. System user interface must be based on HTML		As per RFP
191	iValue, Sify		85		DDOS Protection Suggestion	Solution must support TLS 1.3 management GUI		As per RFP
192	iValue, Sify		85		DDOS Protection Suggestion	System should support CLI access over console port and SSH		As per RFP
193	iValue, Sify		85		DDOS Protection Suggestion	System must have supporting of tools for central monitoring		As per RFP
194	iValue, Sify		85		DDOS Protection Suggestion	Solution should support Configuration and Login Audit trails		As per RFP
195	iValue, Sify		85		DDOS Protection Suggestion	Solution should support Role/User Based Access Control and reporting functionality.		As per RFP
196	iValue, Sify		85		DDOS Protection Suggestion	System should have mechanism to upgrade the firmware and application		As per RFP
197	iValue, Sify		85		DDOS Protection Suggestion	Quoted OEM should have Technical support in India		As per RFP
198	iValue, Sify		85		DDOS Protection Suggestion	Bidder/OEM to provide support in real-time during malware outbreak, DDoS attacks to identify and mitigate attack		As per RFP

199	iValue, Sify		85		DDOS Protection Suggestion	OEM Should have eLearning platform pertaining to Anti DDoS platform and the access will have to provided to stake holders		As per RFP
200	iValue, Sify		85		DDOS Protection Suggestion	OEM to provide onsite training to stakeholders for relevant job functions		As per RFP
201	iValue, Sify		85		DDOS Protection Suggestion	OEM Anti-DDoS Solution should be deployed in India in at least 5 PSU/Private/ Government/BFSI Customer reference in India in last 3 year and should provide evidence of the same		As per RFP
202	iValue, Sify		85		DDOS Protection Suggestion	OEM Anti-DDoS Solution should be deployed and used by at least 4 Tier 1 (class A) Internet service providers (ISPs) in India to protect their own Core infrastructure from DDoS attacks		As per RFP
203	iValue, Sify		85		DDOS Protection Suggestion	The proposed DDoS solution should not reach End of Support within 5 years from the date of submission of bid. If this happens, the bidder is bound to provide the then prevalent higher model at no additional cost.		As per RFP
204	iValue, Sify		85		DDOS Protection Suggestion	Incase of DDOS Attack OEM should be involved to mitigate/ Optimise the traffic to safe guard the services		As per RFP
205	iValue, Sify		85		DDOS Protection Suggestion	Solution should provide DDoS attacks log backup and Filterable/Exportable Attack Log		As per RFP
206	iValue, Sify		85		DDOS Protection Suggestion	Solution should provide Email alerts and comprehensive reporting including Custom, on-demand, on-schedule and/or on-Attack Threshold reports in multiple formats		As per RFP

207	iValue, Sify		85		DDOS Protection Suggestion	Solution should be able to offer granular drill down reports based on hosts, sources, applications etc.		As per RFP
208	iValue, Sify		85		DDOS Protection Suggestion	Solution should provide the traffic statistics related to Application / Protocols (Per Resource Group)		As per RFP
209	iValue, Sify		85		DDOS Protection Suggestion	The solution shall provide real time dashboard displaying statistics on data such as total traffic, passed/blocked, top IPs/services/domains, attack types, top sources by IP location (Geo IP) and blocked sources, etc.		As per RFP
210	iValue, Sify		85		DDOS Protection Suggestion	Customised Reports should be supported		As per RFP
211	iValue, Sify		85		DDOS Protection Suggestion	The proposed system must support automatic cloud signalling to signal to upstream ISPs or managed service provider who is providing anti-DDoS scrubbing service for very large DDoS attack mitigation.		As per RFP
212	iValue, Sify		85		DDOS Protection Suggestion	The proposed solution should support Integration with OEM or External ISP/MSSP Cloud based Scrubbing		As per RFP
213	iValue, Sify		85		DDOS Protection Suggestion	System should have native Integration with most of the Top ISP/MSSP in India for Cloud-based mitigation		As per RFP
214	iValue, Sify		85		DDOS Protection Suggestion	DDoS Appliance must not have any limitations in handling the number of concurrent session for DDoS attack traffic - Knowing nature of solution and should be clearly mentioned in public facing datasheet		As per RFP
215	iValue, Sify		85		DDOS Protection Suggestion	System supports behavioural-based application-layer HTTP and HTTPS DDoS protection		As per RFP

216	iValue, Sify		85		DDOS Protection Suggestion	OEM should have their own Threat Research Team that should provide a Threat Intelligence feed as part of the solution. Threat Intelligence Feed should contain IOC to block Emerging Threats, Active DDoS vectors, Cyber Threats like Malware, APTs, Botnet C&C, Scanning and Brute-force attacks. This feed should be automatically updated in the appliance at a configurable interval.		As per RFP
217	iValue, Sify		85		DDOS Protection Suggestion	Should support user customizable/user defined Signature or Filters or Payload/Header based regular expressions		As per RFP
218	iValue, Sify		85		DDOS Protection Suggestion	System should allow to write manual ACL's to block IP's		As per RFP
219	iValue, Sify		85		DDOS Protection Suggestion	Solution must support searching for IPs which have matched IOCs/Blocked Hosts to understand if organisation was targeted		As per RFP
220	iValue, Sify		85		DDOS Protection Suggestion	System must have an In-Built updated IP reputation feed that has IOC for Active DDoS vectors, Botnets, etc. that are actively propagating DDoS attack vectors anywhere in the world. It should be automatically updated at a configurable interval to block and protect network against active attackers		As per RFP
221	iValue, Sify		85		DDOS Protection Suggestion	System should have options for Blacklist and White list IP Address		As per RFP
222	iValue, Sify		85		DDOS Protection Suggestion	System should restrict the IP address from specific segment like from TOR network		As per RFP

223	iValue, Sify		85		DDOS Protection Suggestion	Proposed appliance should be able to block traffic based on Geo location feed that is updated automatically at configurable intervals		As per RFP
224	iValue, Sify		85		DDOS Protection Suggestion	The system should be capable to detect and mitigate both inbound and outbound attacks.		As per RFP
225	iValue, Sify		85		DDOS Protection Suggestion	Anti-DDoS Appliance should support Automated AI Analytics Engine, Behavioural Analysis, Challenge-response methods to detect and mitigate Zero day DoS, DDoS attacks		As per RFP
226	iValue, Sify		85		DDOS Protection Suggestion	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. Solution should also support packet Anomaly Protection.		As per RFP
227	iValue, Sify		85		DDOS Protection Suggestion	System should protect from TCP Out-Of-State attacks		As per RFP
228	iValue, Sify		85		DDOS Protection Suggestion	System should Protect from multiple attack vectors on different layers at the same time with combination OS, Network, Application, and Server side attacks		As per RFP

229	iValue, Sify		85		DDOS Protection Suggestion	System should support suspension/dynamic suspension of traffic from offending source based on a signature detection, host behavioural analysis, malformed packets, payload expression matching		As per RFP
230	iValue, Sify		85		DDOS Protection Suggestion	The system must support Connection limit option to limit number of new connection on per source basis or in range or equivalent		As per RFP
231	iValue, Sify		85		DDOS Protection Suggestion	The system must allow Network Security policies to be changed while the policy is in active blocking/running mode and should not affect running network protection.		As per RFP
232	iValue, Sify		85		DDOS Protection Suggestion	Should detect and Mitigate attacks at Layer 3 to Layer 7.		As per RFP
233	iValue, Sify		85		DDOS Protection Suggestion	System should have countermeasures & challenge response based approach for immediate mitigation of flood attacks—protecting against unknown DDoS attacks without manual intervention. The system should not depend only on signatures for mitigation of DDoS attacks.		As per RFP
234	iValue, Sify		85		DDOS Protection Suggestion	System must be able to detect and mitigate Spoofed SYN Flood attacks and should support different mechanisms like: a) TCP Authentication b) TCP Out of Sequence Authentication c) HTTP Authentication - Redirect d) HTTP Authentication - soft reset e) HTTP Authentication - JavaScript		As per RFP

235	iValue, Sify		85		DDOS Protection Suggestion	System must be able to detect and block from Flood based attacks on Network and Applications like - TCP, UDP, ICMP, DNS, HTTP		As per RFP
236	iValue, Sify		85		DDOS Protection Suggestion	System DNS protection should employ challenge/response mechanism.		As per RFP
237	iValue, Sify		85		DDOS Protection Suggestion	Solution should support deployment for all DNS flood detection and mitigation (especially for random sub-domain attack)		As per RFP
238	iValue, Sify		85		DDOS Protection Suggestion	System must be able to detect and block HTTP and HTTPS GET/POST Flood and should support mechanisms like: a) HTTP and HTTPS Header Regular Expressions b) HTTP and HTTPS Rate Limiting c) Rate-based Blocking		As per RFP
239	iValue, Sify		85		DDOS Protection Suggestion	System should Protect from Brute Force/reflection/dictionary & amplification attacks or equivalent		As per RFP
240	iValue, Sify		85		DDOS Protection Suggestion	System should detect and Mitigate different categories of Network Attacks viz. Volume based, Protocol, Application attacks etc.		As per RFP
241	iValue, Sify		85		DDOS Protection Suggestion	System should be able to provide (Layer 4 to Layer 7) Challenge action apply to suspicious/all source		As per RFP
242	iValue, Sify		85		DDOS Protection Suggestion	Should detect and Mitigate from Low/Slow scanning attacks		As per RFP
243	iValue, Sify		85		DDOS Protection Suggestion	Solution should support blocking inbound scanning and known brute force attempts		As per RFP

244	iValue, Sify		85		DDOS Protection Suggestion	Solution should support mitigation of Burst Attacks using mechanisms like Rate-Based Blocking, Flexible Rate-based blocking, Signature or equivalent		As per RFP
245	iValue, Sify		85		DDOS Protection Suggestion	The system must limit number of simultaneous TCP connections on a per-client basis		As per RFP
246	iValue, Sify		85		DDOS Protection Suggestion	Solution should support Automatic adaptive thresholds estimation for critical L3, L4 and L7 parameters		As per RFP
247	iValue, Sify		85		DDOS Protection Suggestion	System must be able to detect and block Zombie Floods		As per RFP
248	iValue, Sify		85		DDOS Protection Suggestion	System provides behavioural-DoS protection using real-time signatures, challenge/response mechanism		As per RFP
249	iValue, Sify		85		DDOS Protection Suggestion	Supports over 3 Million IOC Blocking via integration with 3rd Party TIP		As per RFP
250	iValue, Sify		85		DDOS Protection Suggestion	The system must support the dropping of idle TCP sessions if client does not send a user-configurable amount of data within a configurable initial time period and should dynamically blacklist the offending sources.		As per RFP
251	iValue, Sify		85		DDOS Protection Suggestion	Should support IOC Types - IP Address, Fully Qualified Domain Names, URLs		As per RFP
252	iValue, Sify		85		DDOS Protection Suggestion	System protects from DDoS attacks behind a CDN by surgically blocking the real source IP address		As per RFP
253	iValue, Sify		85		DDOS Protection Suggestion	Solution should support SSL renegotiation & Cipher Anomalies Attack Mitigation		As per RFP
254	iValue, Sify		85		DDOS Protection Suggestion	System should Mitigate Encrypted attacks and should support more then 96,000 SSL CPS measured with 2048-bit key		As per RFP

255	iValue, Sify		85		DDOS Protection Suggestion	System protects against SSL/TLS Encrypted DoS and DDoS threats both at the SSL/TLS Layer and HTTPS layer		As per RFP
256	iValue, Sify		85		DDOS Protection Suggestion	System should provide protection from known attack tools that attack vulnerabilities in the SSL layer itself with a separate SSL Decryption module on device or out of path		As per RFP
257	iValue, Sify		85		DDOS Protection Suggestion	System should have out-of-path or on device SSL inspection		As per RFP
258	iValue, Sify		85		DDOS Protection Suggestion	Should have capability to identify malicious SSL traffic based on behaviour analysis, payload inspection		As per RFP
259	iValue, Sify		85		DDOS Protection Suggestion	Proposed Solution should detect SSL encrypted attacks at Key size 2K without any hardware changes.		As per RFP
260	iValue, Sify		85		DDOS Protection Suggestion	Should support protect against attacks that exploit SSL or TLS on application servers such as Web, Mail, or secure VPN servers		As per RFP
261	HPE	11.1.1	89	Payment Terms	Payment to the Service Provider shall be made in Indian Rupees through NEFT / RTGS only on quarterly basis.	We request that the clause be modified as follows: Payment to the Service Provider shall be made in Indian Rupees through NEFT / RTGS only on quarterly basis. All payments to the bidder shall be made within 30 days from the date of invoice.	The RFP does not provide for a timeline by when the payments will be made. There has to be a specific timeline for payments and hence this change.	As per RFP

262	HPE	11.1.8	90	Payment Terms	Payments shall be subject to deductions of any amount for which Service Provider is liable under the contract.	We request that the clause be replaced with the following clause: Any liquidated damages or penalties levied on the bidder shall be recovered from the bidder after completion of the contract.	Any deductions from the payments to the contractor shall lead to cash flow and revenue recognition issues and hence should be recovered after completion of the contract.	As per RFP
263	HPE	11	90	Payment Terms	Payment terms is missing	Bidder request to release the payment within 30 days of invoice		As per RFP
264	Sify	Annexure - A	100	List of Existing IT Assets in PSDC	As per inventory mentioned in Annexure - A, there are some items which shall be End Of support from OEM during the contract period. Hence back to back OEM AMC can not be provided for entire contract period. We understand that such item shall be replaced with new item by PSDC before getting EOSL from OEM. Please confirm.	Please keep this point separate from present RFP. On situational basis finacials and technical possibilities will be decided.		Refer Corrigendum
265	Sify	Annexure - A	100	List of Existing IT Assets in PSDC	In case, PSDC doesn't replace the item/device /system after EOSL from OEM, bidder to provide it's own/third party AMC on best efforts basis. During such period software/ firmware update, upgrade etc shall not be available. Pls confirm.	Please keep this point separate from present RFP. On situational basis finacials and technical possibilities will be decided.		Refer Corrigendum

266	Sify	Annexure - A	100	List of Existing IT Assets in PSDC	On software licenses point - we understand that bidder shall be responsible for all the software licenses mentioned in the RFP. In case any additional software license required due to change of architecture or device or system shall be procured separately by PSDC. Pls confirm.	Please keep this point separate from present RFP. We will take care of licences which are in preview of present time of RFP.		Yes
267	Microfocus	Annexure - B	150	EMS/NMS Specifications for 05 Years warranty and AMC suppor	The proposed EMS solution should be an integrated, modular and scalable solution from single OEM (i.e. all EMS components from single OEM) to provide comprehensive fault management, performance management, traffic analysis and business service management, IT service desk\ helpdesk \trouble ticketing system & SLA monitoring functionality and to meet all requirements mentioned in tender.	Please rephrase the statement as: 1. The proposed EMS solution should be an integrated, modular and scalable solution from single OEM (i.e. all EMS components from single OEM) to provide comprehensive fault management, performance management, traffic analysis, IT service desk\ helpdesk \trouble ticketing system & SLA monitoring functionality and to meet all requirements mentioned in tender.	Since Business Service Management (APM) is not the standard feature of EMS and there are APM specific OEM in the market, hence requesting Business Service Management to be removed from this compliance point.	APM is seprate requirement which need to be integrated with Unified EMS Tool dashboards for logging & reporting purpose.
268	Microfocus, Orbitindia, RahInfotech, Sify	Annexure - B	150	EMS/NMS Specifications for 05 Years warranty and AMC suppor	Proposed solution should have Out-of-the-Box connectors/ probes to integrate with multiple EMS solutions, including industry standard solutions from top 10 market leaders for EMS and should also provide mechanisms (XML, APIs etc.) to integrate with other EMS and NMS solutions, to provide an integrated topology and event views and reports to the operator.	Please rephrase the statement as: Proposed solution should have Out-of-the-Box connectors/ probes/Rest API's to integrate with multiple EMS solutions, including industry standard solutions from top 10 market leaders for EMS and should also provide mechanisms (XML, APIs etc.) to integrate with other EMS and NMS solutions, to provide an integrated topology and event views and reports to the operator.		Refer Corrigendum

269	Microfocus, Orbitindia, RahInfotech, Sify	Annexure - B	150	EMS/NMS Specifications for 05 Years warranty and AMC suppor	Proposed EMS/NMS solution must be ISO 27001:2013 certified to ensure security compliances.	**Microfocus**: To ensure the proposed software is secure, it should have **ISO 27034** certification from a verification or certification agency from Schellman/ KPMG/ PwC/ Ernst & Young/ Deloitte recognized. **OrbitIndia**: To ensure the proposed software is secure, it should have ISO 27034 certification from a verification or certification agency from Schellman/ KPMG/ PwC/ Ernst & Young/ Deloitte recognized. **Sify**:To ensure the proposed software is secure, it should have ISO 27034 certification from a verification or certification agency from Schellman/ KPMG/ PwC/ Ernst & Young/ Deloitte recognized.	ISO 27034 standard helps organizations integrate security controls in their software through their software development life cycle, by defining security frameworks & vulnerability management processes. So, a software developed adhering to ISO 27034 standard when used, it protects customer assets from potential cyber breaches & security threats while complying with the Application security	Refer Corrigendum

270	Microfocus, Motadata, Orbitindia, RahInfotech, Sify, TechBridge, Everestims, iValue	Annexure - B	150	EMS/NMS Specifications for 05 Years warranty and AMC suppor	The proposed EMS/NMS solution must be an industry standard, enterprise grade solution recognized by leading analysts (IDC/Gartner/ Forrester) in ITSM, NPMD & AI Ops reports.	**MicroFocus**: The proposed EMS/NMS solution must be an industry standard, enterprise grade solution recognized by leading analysts (IDC/Gartner/ Forrester) in ITSM and NPMD. **Motadata**: The proposed EMS/NMS solution must be an industry standard, enterprise grade solution recognized by leading analysts (IDC/Gartner/ Forrester) in any Published reports. Documentary proof needs to be provided at the time of bid. **Sify**: The proposed EMS/NMS solution must be an industry standard, enterprise grade solution recognized by leading analysts (IDC/Gartner/ Forrester) in ITSM and NPMD.	**Motadata**: The report type specified here are very specific to Single OEM, and it is restricting recognied Make in India OEMs,so that we request you to please remove Specific Type of report as OEM qualification criteria. Requesting you to modify clause as per suggestion so that Reputed and recognized Make in India OEM also can participate for this RFP and authority can get competetive product with cost advantages.	Refer Corrigendum

271	Microfocus, RahInfotech, Sify, BMC, OrbitIndia, TechBridge, iValue	Annexure - B	151	EMS/NMS Specifications for 05 Years warranty and AMC suppor	Proposed NMS solution must have at least 3 deployments in Central Government/ Public Sector/State Govt./PSU`s and Large Enterprise, out of which one should be in a DC environment, monitoring & managing 10,000+ network nodes in each of such deployments.	**Microfocus**: Proposed NMS solution must have at least 3 **deployments in Central Government/ Public Sector/State Govt./PSU`s,** out of which one should be in a DC environment, monitoring & managing 10,000+ network nodes in each of such deployments. **Sify**: Proposed NMS solution must have at least 3 deployments in Central Government/ Public Sector/State Govt./PSU`s, out of which one should be in a DC environment, monitoring & managing 10,000+ network nodes in each of such deployments. **BMC**: Proposed EMS solution must have at least 2 deployments in Central Government/ Public Sector/State Govt./PSU`s and Large Enterprise, out of which one should be in a DC environment, monitoring & managing 10,000+ network **nodes/servers/endpoints** in each of such deployments. **OrbitIndia**: Proposed NMS solution must have at least 3 deployments in Central Government/ Public Sector/State Govt./PSU`s, out of which one should be in	**BMC**: EMS not only includes network monitoring but it also includes server monitoring and endpoint monitoring. Hence request Dept. to kindly consider server and endpoint counts under the implementation citation. Also request department to ask for 2 such deployments to ensure maximum participation from leading OEMs.	Refer Corrigendum

272	Microfocus, OrbitIndia, RahInfotech, Sify	Annexure - B	150	EMS/NMS Specifications for 05 Years warranty and AMC support:	EMS - Generic Query	Requesting customer to provide the following volumetric for Infrastructure volumetric count? Please confirm the infrastructure volumetric count: 1. No. of network devices to be monitored (SNMP/ICMP)? 2. Total no. of Physical servers? 3. Total no of Virtual Servers? 4. Total nos. of DB OS instances to be monitored? 5. Total nos. of Middleware OS instances to be monitored? 6. Number of application business critical transactions to be monitored? 7. How many Page Views (in Million) for real user monitoring? 8. Total nos. of Helpdesk (HD, Change, KM, SLM etc.) agents logging into the helpdesk system? 9. Helpdesk Analyst Type - Concurrent or Named? 10. Total no. of Client OS instances (desktops/laptops) for asset management & tracking? 11. Any specific Integrations with EMS/NMS solution? 12. Total node counts for Integration with	**Reason:** This will provide all the qualified EMS OEM's to participate equally technically and commercially.	As per RFP
273	Microfocus, OrbitIndia, RahInfotech, Sify	Annexure - B	150	EMS/NMS Specifications for 05 Years warranty and AMC support:	EMS and Helpdesk Solution Architecture Query	Please clarify if EMS and Helpdesk solution is to be designed in DC (Standalone) or DC with HA (active - passive) or DC with HA (active - passive) and DR (Redundant)?		As per RFP

274	Microfocus, Orbitindia, RahInfotech, Sify	Annexure - B	150	EMS/NMS Specifications for 05 Years warranty and AMC support:	2. Proposed solution should have Out-of-the-Box connectors/ probes to integrate with multiple EMS solutions, including industry standard solutions from top 10 market leaders for EMS and should also provide mechanisms (XML, APIs etc.) to integrate with other EMS and NMS solutions, to provide an integrated topology and event views and reports to the operator.	Please provide the Top 10 Market leaders solution names for EMS so that we can check whether we have Out-of-the-Box connectors/ probes to integrate with to be proposed EMS solution.		Please refer point - 8, Page - 150 of EMS & related Corrigendum.
275	Motadata	Annexure - B	154	Technical Specifications - IT Components C) Network Management System (NMS)	IV Multiprotocol Label Switching Service (MPLS) Monitoring: IV Multiprotocol Label Switching Service (MPLS) Monitoring: 1. Should monitor MPLS service availability and inventory, in addition to traditional Layer-3 Virtual Private Networks (L3 VPN), L2 VPN, core traffic engineering, and pseudo-wire management. 2. Should improve uptime with continuous MPLS-specific core, Layer-2 and Layer-3 discovery, monitoring, and alerting. 3. Should provide inventory view of L3 VPNs, detailed views for an L3 VPN, including VRFs and VRF details. 4.Should provide out of the box Reporting such as: LSR reports Site reports (VRF) Site-to-site quality-of-service reports VPN reports	Requesting you to please remove this functional requirement.	As per RFP requirements and BOQ there is no need specified for MPLS based services and Hardwares. But in NMS specifications its mentioned so requesting you to please remove this requirements as its not required as overall scope of work, this will add up unnecessory cost to project.	As per RFP

276	NetScout, Progress	Annexure - B.C	154	Network Traffic Flow Analysis System	It shall be able to capture, track & analyses traffic flowing over the network via different industry standard traffic capturing methodologies viz. NetFlow, jflow, sFlow, IPFIX etc.	**NetScout**: Total no. of flows per min need to be mentioned for the sizing parameter of the solution. So that we can proposed solution with correct sizing. **Progress**: Total through put and no. of flows per second required to be mentioned for the sizing parameter of the solution. So that we can proposed solution with correct sizing.		The total number of flows per minute can vary depending on the size and complexity of the network, the types of applications and protocols being used, and the traffic patterns and volume. So after understaning scope requirements, current ICT Infrastructure and architechture bidder are advised to propose solution accordingly after proper AS-Is study. The

277	Microfocus, Orbitindia, RahInfotech, Sify	Annexure - B.D	155	Helpdesk and IT Service Management	The proposed Helpdesk tool must be ITIL certified on at least 6 processes.	**Microfocus**: The proposed IT Service Management solution should be built on ITIL framework and must be officially certified on the current ITIL 4 best practices on at least 10 processes by Pink Elephant. The ITIL4 processes that are relevant and needs to be assessed to meet the minimum functional criteria are Incident management, Problem Management, Change Enablement, Service Configuration management, Service Catalog Management, Release Management, Service Desk, Knowledge Management, IT Asset Management and Service Request Management. The certification copy to be submitted along with the formal technical response. **OrbitIndia**: The proposed IT Service Management solution should be built on ITIL framework and must be officially certified on the current ITIL 4 best practices on at least 10 processes by Pink Elephant. The ITIL4 processes that are relevant and needs to be assessed to meet the minimum functional criteria are Incident management, Problem Management, Change Enablement, Service	**Microfocus**: The differences that distinguish ITIL 4 from the older versions are the inclusion of additional best practices and new material on integration. ITIL 4 focuses more on the concepts of costs, outcomes, risks, and value. Please refer to the following weblink to view list of ITIL 4 Certified OEMs, there are handfull of best in breed solution available: https://www.pinkelephant.com/en-us/PinkVERIFY/PinkVERIFY-ITIL-4-Toolsets. **OrbitIndia**: The	Refer Corrigendum

278	Cisco	Annexure B.D.14.1	156	Application Performance Management	Request to Add critical features of APM	Proposed solution should be able to auto discover experience journeys for the users and provide below details : a) Performance metrics for each step in a user journey b) Performance metrics from one step to the next c) Top incoming and outgoing traffic data for each step d) Drop-off rates e) Refresh traffic and performance data		As per RFP
279	Cisco	Annexure B.D.14.1	156	Application Performance Management	Request to Add critical features of APM	Proposed APM 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		As per RFP

280	Cisco	Annexure B.D.14.1	156	Application Performance Management	Request to Add critical features of APM	Proposed solution shoud offer 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		As per RFP

281	BMC	14.1 IV	156	Application Performance Management	Application Performance Management	Request department to remove APM requirement from EMS and put it as a separate requirement	Request Department to remove this requirement from EMS and seek separate requirement under the tender as APM is altogether a different technology and the leading APM OEMs are different from EMS/NMS OEMs hence combining APM under EMS will lead to a favourable situation for a particular OEM.	APM can be a separate tool and must be integrated with Unified EMS Tool dashboards for logging & reporting purpose.

282	Microfocus, OrbitIndia, RahInfoTech,Sify, NetScout, Progress	Annexure - B.D	156	Application Performance Management	Storage of historical data is for problem diagnosis, trend analysis etc.	**MicroFocus**: This particular clause is favouring specific OEM's APM solution and requiring Diagnostic configuration management, which is not a generic APM specifications. Hence requesting you to please delete this clause. **OrbitIndia**: This particular clause is favouring specific OEM's APM solution and requiring Diagnostic configuration management, which is not a generic APM specifications. Hence requesting you to please delete this clause. **Sify**: This particular clause is favouring specific OEM's APM solution and requiring Diagnostic configuration management, which is not a generic APM specifications. Hence requesting you to please delete this clause. **NetScout**: Sizing parameter is missing, For how long you would need historical data. For example 6 month historical data etc. Please ammend the clause as " 6 month Storage of historincal data is for problem diagnosis,trend analysis etc. **Progress**: Sizing parameter needs to be provided in detail. In terms of solution type like		Refer Corrigendum

283	Microfocus, OrbitIndia, RahInfoTech,Sify, NetScout, Progress	Annexure - B.D	156	Application Performance Management	Should drill down from slow, end-user transactions to the bottlenecked component, method or SQL statement, helping to solve memory, exception and other common problems	**MicroFocus**: This particular clause is favouring specific OEM's APM solution and requiring Diagnostic configuration management, which is not a generic APM specifications. Hence requesting you to please delete this clause. **OrbitIndia:** This particular clause is favouring specific OEM's APM solution and requiring Diagnostic configuration management, which is not a generic APM specifications. Hence requesting you to please delete this clause. **Sify**: This particular clause is favouring specific OEM's APM solution and requiring Diagnostic configuration management, which is not a generic APM specifications. Hence requesting you to please delete this clause. **NetScout**: As the requirement is to monitor the application on the network performance and not the code level. request you to ammend the clause as " **Should drill down from slow, end-user transactions to the bottlenecked component, front end , backend related issues over network helping to solve memory, exception and other common**		Refer Corrigendum
284	NetScout, Progress	Annexure - B.D	156	Application Performance Management	End to end Management of applications (J2EE/.NET based)	**NetScout**: Not a function of application performance management. Request you to ammend the clause as" **end to end monitoring on the network for the application and its performance".** **Progress:** Should be removed		Refer Corrigendum

285	NetScout, Progress	Annexure - B.D	156	Application Performance Management	Determination of the root cause of performance issues whether inside the Java / .Net application in connected back-end systems or at the network layer.	**NetScout**: As per our understanding the rquirement is to monitor the applications performance at the network level irrespective of the coding language of the application . Pls confirm. Progress: Should be removed		Yes
286	NetScout, Progress	Annexure - B.D	156	Application Performance Management	Data, reports and views from the synthetic monitoring solution should be able to be incorporated into common dashboard views along with real user monitoring and infrastructure monitoring.	**NetScout**: Hope the understanding is that Synthetic monitoring Solution should be integrated with application monitoring solution. Please confirm. **Progress**: Should support end user monitoring.		Yes, as per RFP.

287	Cisco, NetScout, HealSoftware, RahInfotech	Annexure B.D.14.1	157	Application Performance Management	Sniffer Solution should support store and replay session information for the real user along with snapshots and text pattern events.	**Cisco :** Snipper solution is a legacy approach of monitoring application performance which used to provide limited insights into the performance bottleneck. Does ability to capture details real user sessions activities along with capturing mobile session snapshots will suffice the monitoring requirement. Also, what is expected as a part of text pattern events. **NetScout**: Solution will be able to replay the session information for the trasactions for any user. For every request /response in between user and server it will provide the detailed session analysis and will provide insight/snapshot of that transaction. **HealSoftware, Rah Infotech**: The point seems restrictive to specific 1 or 2 OEM's while Replaying any recorded session is not a basic functionality of an APM solution, while 1 or 2 APM OEM exhibit this type of functionality which actually can not be utilized in practical scenario since session details data and other critical unique data can not be reposted in production.	**HealSoftware, Rah Infotech**: We here by request you to please remove this specific point to allow bidders to offer more competitive APM OEMs and fulfill MII (LC) procurement guidelines as well.	Refer Corrigendum
288	Cisco	Annexure B.D.14.1	157	Application Performance Management	Summary Reports for specific groups: Reports displaying per group of resources the group aggregations for a set of metrics (for example, per City, the maximum traffic or the total traffic).	Can we use the combination of standard report and real time dashboard view to deliver these set of reports?		As per RFP.

289	Microfocus, OrbitIndia, RahInfotech, Sify, NetScout, Progress	Annexure - B.D	157	Application Performance Management	The proposed solution should expose performance of individual SQL statements within problem transactions	**Microfocus**: This particular clause is favouring specific OEM's APM solution and requiring Diagnostic configuration management, which is not a generic APM specifications. Hence requesting you to please delete this clause. **OrbitIndia**: This particular clause is favouring specific OEM's APM solution and requiring Diagnostic configuration management, which is not a generic APM specifications. Hence requesting you to please delete this clause. **RahInfotech**: This particular clause is favouring specific OEM's APM solution and requiring Diagnostic configuration management, which is not a generic APM specifications. Hence requesting you to please delete this clause. **Sify**: This particular clause is favouring specific OEM's APM solution and requiring Diagnostic configuration management, which is not a generic APM specifications. Hence requesting you to please delete this clause. **NetScout**: not a function of application performance management. This requires separate database monitoring system. However database queries over network		Refer Corrigendum

290	Microfocus, OrbitIndia, RahInfotech, Sify, NetScout, Progress	Annexure - B.D	157	Application Performance Management	The proposed solution should be JVM & JDK independent, thereby enabling to manage applications on any Java Virtual Machine.	**Microfocus**:This particular clause is favouring specific OEM's APM solution and requiring Diagnostic configuration management, which is not a generic APM specifications.Hence requesting you to please delete this clause. **OrbitIndia**: This particular clause is favouring specific OEM's APM solution and requiring Diagnostic configuration management, which is not a generic APM specifications. Hence requesting you to please delete this clause. **RahInfotech**: This particular clause is favouring specific OEM's APM solution and requiring Diagnostic configuration management, which is not a generic APM specifications. Hence requesting you to please delete this clause. **Sify**: This particular clause is favouring specific OEM's APM solution and requiring Diagnostic configuration management, which is not a generic APM specifications. Hence requesting you to please delete this clause. **NetScout**: Not a function of application performance management request you to remove the clause.		Refer Corrigendum

291	NetScout, Progress	Annexure - B.D	157	Application Performance Management	Should automatically detect all components touched by a business process across layers and traces them with no user intervention	**NetScout**: Hope the understanding is that - Synthetic testing will provide all the component from user to the business application and Real traffic/packet capture based solution would draw a dependancy map between all the dependent applications.Please confirm. **Progress**: Should support end user monitoring		As per RFP
292	NetScout, Progress	Annexure - B.D	157	Application Performance Management	Should support J2EE, .NET, SAP, SOA or Siebel Applications	**NetScout**: Hope the understanding is that Solution should monitor any application being a network based packet capture solution where any application can be monitored over the network for its performance and issues.Please confirm. **Progress**: Should be removed. Solution should support on basis of transaction and TCP connection.		Refer Corrigendum
293	NetScout, Progress	Annexure - B.D	157	Application Performance Management	Solution should monitor application performance, availability and usage volume. It should provide breakdown of user experience by location, username, browser, OS,	**NetScout**: OEM specific language request you to ammend the same as " Solution should monitor application performance, availability and usage volume. It should provide breakdown of user experience by location, username. It should also provide visibility on browser and OS used by user" **Progress**: OEM specific language request you to ammend the same as " Solution should monitor application performance, availability and usage volume. It should provide breakdown of user experience by location, username. It should also provide visibility on browser and OS used by user"	Solution should monitor application performance, availability and usage volume. It should provide breakdown of user experience by location, username. It should also provide visibility on browser and OS used by user.	Refer Corrigendum

294	NetScout, Progress	Annexure - B.D	157	Application Performance Management	Solution should support mobile native applications to collect various metrics for mobile networks, such as device type, operating system, mobile carrier, and installed application version. Supported platforms should include iPhone and Android device	**NetScout**: not a function of application performance management request you to ammend the clause as " Solution should support mobile native applications monitoring and should be 24/7 packet capture based solution monitoring each and every packet for its performance over the network without any need of the agent to be installed on the end servers" **Progress**: Solution should support mobile native applications monitoring .		Refer Corrigendum

295	Fortinet, Innspark, Sify, iValue	Annexure B.E	158	Security Incident Management Solution (SIEM)	Solution should encompass log, packet and end point data with added context and threat Intelligence. Should provide complete network visibility through deep packet inspection high speed packet capture and analysis.	**Fortinet**: Solution should encompass log, packet and end point data with added context and threat Intelligence. **Microfocus**: Intelligent next generation SIEM must be able to detect any anomalies, report in real time and take action as programmed having SIEM AND SOAR capabilities. Solution must be Three tiered Physically segregated consisting of Collection layer, Log Management Layer and Correlation layer. **Sify**: Solution should encompass log, packet and end point data with added context and threat Intelligence. **iValue**: As Packet capture solution is a altoghether different technology and have to be asked as a seperate requirement or solutions. Hence we request you to separate the packet capture requirement from SIEM solution as it'll limit competition from renowned SIEM OEM's. Hence request to remove the packet capture requirement from SIEM and sought it as seperate solution. **Innspark**:Kindly requesting to amend this clause as "Solution should encompass log, packet and end point with added context and threat Intelligence. Solution	**Fortinet**: Restrictive Point: Favouring single OEM. us to take part in the tender. Most of the OEM doesn't support packet capture. So request you to ammend the clause as suggested. **Innspark**: Deep Packet Inspection in SIEM Solution is favourable to a specific OEM. Having technical requirements specific to a single OEM will result in unfair advantage and limits the participation of other OEM's who	Refer Corrigendum

296	innspark	Annexure - B.E	158	Security Incident Management Solution (SIEM)	Security Incident Management Solution (SIEM)	Request for addition of Clause : "The solution should allow creating dynamic dashboards with any key that is a part of the log."	This will enable the PSDC analysts to operate efficently and effectively. This will ensure that the analyts will be able to create dedicated dashboards as per the requirements.	As per RFP
297	innspark	Annexure - B.E	158	Security Incident Management Solution (SIEM)	Security Incident Management Solution (SIEM)	Request for addition of Clause : "The solution should have a custom reporting framework which should allow the anslyst to create reporting dashboards"	This will enable the PSDC analysts to operate efficently and effectively. This will ensure that the analyts will be able to create dedicated dashboards as per the requirements.	As per RFP

298	innspark	Annexure - B.E	158	Security Incident Management Solution (SIEM)	Security Incident Management Solution (SIEM)	Request for addition of Clause : "The solution should have out of the box security posture dashboards which helps PSDC to asses the current security posture of the organization. These dashboards should be interactive and should allow drill down"	This will help the PSDC to have a single pane glass visibility into entire security events happening in the PSDC network. PSDC network, being a versatile network should have these kind of interactive security posture dashboards which will help in achieveing 100% visibility.	As per RFP

299	innspark	Annexure - B.E	158	Security Incident Management Solution (SIEM)	Security Incident Management Solution (SIEM)	Request for addition of Clause : "The solution should have out of the box security posture dashboards which helps ICG to asses the current security posture of the organization. These dashboards should be interactive and should allow drill down"	PSDC is going to be home for various critical applications which will be accessible from public. This increases the exposure and also the risk factor of getting lots of attacks. Inoder to ensure that PSDC is equipped with latest cutting edge detection mechnisms, it is important to ensure that the solution will have necessary out of the box detection models in place.	As per RFP
300	innspark	Annexure - B.E	158	Security Incident Management Solution (SIEM)	Security Incident Management Solution (SIEM)	Request for addition of Clause : "The solution should include integrated threat intelligence feeds which gets updated daily and contains IOC including IPV4, IPV6, domains, email, hash etc. "	This will help PSDC Analysts to have updated threat intelligence Feeds which will ensure to prevent attacks.	As per RFP

301	innspark	Annexure - B.E	158	Security Incident Management Solution (SIEM)	Security Incident Management Solution (SIEM)	Request for addition of Clause : "The solution should have native integration with CERT-In CMTX, NCIIPC and other regulatory body provided threat feeds"	CERT-In & NCIIPC feeds provides latest IOCs. It is important to automate the integration with these feeds to ensure that PSDC will be able to detect any matches without any manual intervention	As per RFP
302	Microfocus, Sify	Annexure B.E	158	Security Incident Management Solution	Additional Point	**Microfocus:** SIEM solution must support in-memory correlations or near real-time correlations. Correlations rules must trigger before writing logs in database. **Sify**: SIEM solution must support in-memory correlations or near real-time correlations. Correlations rules must trigger before writing logs in database	**Microfocus**: This feature will ensure protection against sophisticated attack & to take preventive action. **Sify**: This feature will ensure protection against sophisticated attack & to take preventive action.	As per RFP

303	Microfocus, Sify	Annexure B.E	158	Security Incident Management Solution	Additional Point	**Microfocus:** SIEM solution must use data security by encrypting sensitive data with correlation capabilities on those encrypted fields. **Sify**: SIEM solution must use data security by encrypting sensitive data with correlation capabilities on those encrypted fields	**Microfocus**: This feature will help protecting sensitive data while performing all correlation to provide 100% coverage on security analytics. **Sify**: This feature will help protecting sensitive data while performing all correlation to provide 100% coverage on security analytics.	As per RFP

304	Microfocus, Sify	Annexure B.E	158	Security Incident Management Solution	Additional Point	**Microfocus:** Solution should have integration with threat intelligence feed (i.e. Virus Total, MISP etc) as well its own threat intelligence platform to have collaborative IOCs to enrich information for security analyst decision. **Sify**: Solution should have integration with threat intelligence feed (i.e. Virus Total, MISP etc) as well its own threat intelligence platform to have collaborative IOCs to enrich information for security analyst decision	**Microfocus**: This ensure out of the box integration capabilities to keep up-to-date IOCs for all unknows and better setup response actions or remediation steps. **Sify**: This ensure out of the box integration capabilities to keep up-to-date IOCs for all unknows and better setup response actions or remediation steps.	As per RFP

305	Microfocus, Sify	Annexure B.E	158	Security Incident Management Solution	Additional Point	**Microfocus:** This ensures no surplus license cost to bidder/customer for SOAR while avail full loaded SOAR functionality throughout project tenure or active entitlement of the contract. If SOAR is not a primary requirement then native SOAR can be installed in future with just adding additional hardware. **Sify**: This ensures no surplus license cost to bidder/customer for SOAR while avail full loaded SOAR functionality throughout project tenure or active entitlement of the contract. If SOAR is not a primary requirement then native SOAR can be installed in future with just adding additional hardware.	**Microfocus**: Next Gen SIEM/ SOC should have SOAR capabilities. SOAR licenses should be native with SIEM and does not require any individual licenses for any SOAR capabilities (i.e. security analyst, playbooks etc). **Sify:** Next Gen SIEM/ SOC should have SOAR capabilities. SOAR licenses should be native with SIEM and does not require any individual licenses for any SOAR capabilities (i.e. security analyst, playbooks etc).	As per RFP
306	TechBridge	Annexure B.E	158	Security Incident Management Solution	All necessary dedicated hardware (with min 12TB storage in raid 5/6) for Security Incident Management Solution should be provided.	This clause is proprietary which is the restricting the wider OEM participation. Request to authority to kindly remove this clause.		As per RFP

307	Fortinet, Microfocus, Sify	Annexure B.E	159	Security Incident Management Solution (SIEM)	The SIEM & Log Monitoring solution should be from a different OEM than the Prevention Security solutions like F/W, IPS, HIPS, AV, DLP and Encryption, application security	**Fortinet**: Pls remove this Point. **Microfocus**:Point needs to be deleted or need to be rephrase as "The SIEM & Log Monitoring solution should be from a different OEM other than the Prevention Security solutions like F/W, Packet Capture, IPS, HIPS, AV, DLP. So that it can detect threats missed by other existing tools using the security defence in depth strategy." **Sify**:Pls remove this Point. **Sify**: Point needs to be deleted or need to be rephrase as "The SIEM & Log Monitoring solution should be from a different OEM other than the Prevention Security solutions like F/W, Packet Capture, IPS, HIPS, AV, DLP. So that it can detect threats missed by other existing tools using the security defence in depth strategy."	**Fortinet**: Restrictive Point: Since the point is restricting us to take part in the tender. Most of the leading Firewall security players offer mutliple product in the cyber security space. Specification are favouring SIEM OEM and giving an edge against other OEMS so we recommend you to ammend or delete the clause where every OEM has equal participation in the RFP. Also give better price benefit to organization. **Microfocus**:	Refer Corrigendum

308	Fortinet, Sify	Annexure B.E	159	Security Incident Management Solution (SIEM)	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 logs should be time stamped, compressed to optimize storage utilization. There should be no limitation on number of devices to be supported. Any addition in no. of devices should have no cost impact on department.	**Fortinet**: 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 logs should be time stamped, compressed to optimize storage utilization. **Sify**: 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 logs should be time stamped, compressed to optimize storage utilization.	**Fortinet**: Restrictive Point: Every OEM has its own set of architecture and licensing model. So we recommend you to share the total no of device count from day one with future expansion scope so that we can factor the device count accordingly. **Sify**: Restrictive Point: Since the point is restricting us to take part in the tender. Most of the leading Firewall security players offer mutliple product in the cyber security space.	As per RFP

309	Fortinet, Sify	Annexure B.E	159	Security Incident Management Solution (SIEM)	The solution should provide an integrated SOC dashboard and Incident analysis system that could provide a single view into all the analysis performed across all the different data sources including but not limited to logs and packets. The Tool should have role-based access control mechanism and handle the entire security incident lifecycle.	**Fortinet**: The solution should provide an integrated SOC dashboard and Incident analysis system that could provide a single view into all the analysis performed across all the different data sources. The Tool should have role-based access control mechanism and handle the entire security incident lifecycle. **Sify**: The solution should provide an integrated SOC dashboard and Incident analysis system that could provide a single view into all the analysis performed across all the different data sources. The Tool should have role-based access control mechanism and handle the entire security incident lifecycle.	**Fortinet**:Restrictive Point: Favouriong Single OEM. Request you to please ammend the point and make it generic so that we can take part in the RFP. **Sify**: Restrictive Point: Favouriong Single OEM. Request you to please ammend the point and make it generic so that we can take part in the RFP	As per RFP

310	Fortinet, Innspark, Microfocus, Sify, iValue	Annexure B.E	160	Security Incident Management Solution (SIEM)	Solution should support minimum 30,000 EPS scalable to 50,000 at correlation, management and collection layer and packet capture solution should support upto 1GBPS line rate for capturing from network.	**Fortinet**: Solution should support minimum 30,000 EPS scalable to 40,000 at correlation, management and collection layer. **Innspark**:Packet Capture Solution is a requested feature along with SIEM, Kindly requesting to have a dedicated Network Detection and Response Solution. **Microfocus**: Solution must be Sized for 30000 Sustained, 50000 Peak EPS without queuing or dropping any logs. SOAR Solution must support all devices as SIEM and no restriction on Admins. It must collect all flows from network without any limitation. The solution should be able to integrate with the existing components and the new proposed components in the infrastructure.The solution should support seamless migration of data from existing SIEM solution and should support executing reports on the data collected and managed by the existing SIEM solution. The proposed solution should have a seamless Incident management and ticketing capability to generate and manage automated tickets for the alert events generated by the correlation engine. **Sify**: Solution	**Fortinet**: Restrictive Point: Favouring Single OEM. Request you to please ammend the point and make it generic so that we can take part in the RFP. **Innspark**: Since PSDC is a critical infrastructure , we request you to consider having a dedicated Network Detection and Response to have an indepth view of the entire network traffic. **Microfocus:** Next Gen SIEM/ SOC should have SOAR capabilities. and asked spec is favouring to single OEM.	Refer Corrigendum

311	Fortinet, Microfocus, Sify, iValue	Annexure B.E	160	Security Incident Management Solution (SIEM)	The solution should be storing both raw logs as well as normalized logs. Should store RAW packet DATA for 7 days and normalized packet data for 120 days for forensics.	**Fortinet**: The solution should be storing both raw logs as well as normalized logs. Should store RAW log for 7 days and normalized log for 120 days for forensics. **Microfocus**: The SIEM solution must be able to store both the raw event log as well as the parsed event log/normalized data. Storage should be sized to provide 3 Months online and 3 Months Offline log storage at central site. Both raw logs and normalized logs should be made available. **Sify**: The solution should be storing both raw logs as well as normalized logs. Should store RAW log for 7 days and normalized log for 120 days for forensics. **Sify**: The SIEM solution must be able to store both the raw event log as well as the parsed event log/normalized data. Storage should be sized to provide 3 Months online and 3 Months Offline log storage at central site. Both raw logs and normalized logs should be made available. **iValue**: We request department to sought for solution which must have a log collection and archive architecture that supports online log retention for 90 Days and offline log	**Fortinet**: Restrictive Point: Favouring Single OEM. Request you to please ammend the point and make it generic so that we can take part in the RFP. **Microfocus**: Every SIEM tool has different ways to meet log retention requirement. To make it optimized for log retention, SIEM tool uses different compression algorithms and compression ratio which leads to variable storage requirement. Solution should be storage agnostic and can be	Refer Corrigendum

312	Fortinet, Sify, iValue	Annexure B.E	160	Security Incident Management Solution (SIEM)	All necessary dedicated hardware (with min 12TB storage in raid 5/6) for Security Incident Management Solution should be provided.	**Fortinet**: All necessary dedicated hardware (with min 70TB storage in raid) for Security Incident Management Solution should be provided. **Sify**: All necessary dedicated hardware (with min 70TB storage in raid) for Security Incident Management Solution should be provided. **iValue**: Certain functionalities in existing clause are vendor specific, change requested to make requirement more generic "All necessary hardware (with min 12TB storage in raid 5/6) for Security Incident Management Solution should be provided."	**Fortinet**: Since the hard asked in the tender is very less as compared to the EPS count asked in the tender so we recommend you to ask more number of hardisk. **Sify**: Since the hard asked in the tender is very less as compared to the EPS count asked in the tender so we recommend you to ask more number of hardisk.	As per RFP

313	Fortinet, Sify	Annexure B.E	160	Security Incident Management Solution (SIEM)	The system should provide an integration with third party tools proposed by solution provider such as EMS, BMS, and other deployed ICT Infrastructure within PSDC for log collections, SIEM functionality and its management etc.	**Fortinet**: The system should provide an integration with third party tools. **Sify**: The system should provide an integration with third party tools	**Fortinet**: Restrictive Point: Please make it generic so that we can take part in the same or ask the same in bidder scope. Since the complete implementation and integration is part of bidder. **Sify**: Restrictive Point: Please make it generic so that we can take part in the same or ask the same in bidder scope. Since the complete implementation and integration is part of bidder.	As per RFP

314	Sify	Annexure - B.F	160	Antivirus Specifications	Antivirus Specifications	1- Kindly suggest, mentioned 300 qty. are for server security? 2- Who will provide underlying infra for managing the HIPS solution?		1. Bidders are advised to visit PSDC with a planned schedule, before submission & preparation of bids to understand the scope of work and to design their implementation approach & methodology" 2. Infra will be provided by DGRPG
315	TechBridge	Annexure B.E	160	Security Incident Management Solution	Additional Clause need to add	As per the gartner, SOAR should be integral part of the Next Gen SIEM. so please add the SOAR solution requirement as well in the SIEM		As per RFP
316	iValue	Annexure - B.F.2	160	Antivirus Specifications	Should support Firewall, Anti-Malware, Integrity Monitoring, Application Control and Recommended scan features in single module with agentless and agent based capabilities along with broader range of Operating Systems support i.e. MS Windows, Red Hat Enterprise Linux, CentOS Linux, Oracle Linux, SUSE Linux, Ubuntu Linux, Debian Linux**, Solaris and AIX**.	Linux has multiple flavours it is not practical any OEM can support all the Linux Platforms, hence requesting you to change the specs as below “Should support multiple Windows, linux OS with maximumfeature parity ”		Refer Corrigendum

317	iValue	Annexure - B.F.9	161		Host IPS should be capable of recommending rules based on vulnerabilities with the help of **virtual patching** and should have capabilities to schedule recommendation scan and entire features of solution should be **agentless**.	The tersm Virtual pathing is a OEM Specific Termonology. We kindly request you to change the specification as per below "Host IPS should be capable of recommending rules based on vulnerabilitie and should have capabilities to schedule recommendation scan "		Refer Corrigendum
318	iValue	Annexure - B.F.11	161		Host based IPS should **support virtual patching both known and unknown vulnerabilities** until the next scheduled maintenance window.	The tersm Virtual pathing is a OEM Specific Termonology. We kindly request you to change the specification as per below " The solution should be able to protect machines from expoitation activities using AI-ML or any similar technology"		Refer Corrigendum
319	iValue	Annexure - B.F.12	161		Should provide automatic recommendations against existing vulnerabilities, dynamically tuning IDS/IPS sensors (Selecting rules, configuring policies, updating policies) provide automatic recommendation of removing assigned policies if vulnerability no longer exists.	OEM Specific spec, kindly requesting customer to give opportunity for other also to qualify.		As per RFP
320	iValue	Annexure - B.F.16	161		Should be Common Criteria EAL 4 and FIPS 140-2 validated.	Kindly requesting customer to change the specs as "Should be Common Criteria EAL 2 above and FIPS validated. "		As per RFP
321	iValue	Annexure - B.F.19	161		Proposed solution should be Leader in Server Security Market as **per IDC latest report**.	Kindly requesting customer to change the specs as "Proposed solution shoud be a leader in GARTNER / FORESTER / IDC in last 3 years of report"		Refer Corrigendum

322	iValue	Annexure - B.F.20	161		Should offers common management console managing all physical, virtual and cloud servers supporting both window as well **as Linux platform.**	Every OEM has own process of Hardening of management cosole also FIPS is already asked in the earlier specifications. Hence requesting customer to change the specs as "Should offers common management console managing all physical, virtual and cloud servers with FIPS Compliance"		As per RFP
323	Cisco, Paloalto Networks, iValue	Annexure B.G	162	Next Generation Firewall	The solution should have atleast 4 X 100/1000/10G Cu, 16 X 1G/10G SFP/ SFP+, 4 X 40G/100G QSFP28 from day 1 with all SFP included. All below requirements should be available from day 1 onwards.	**Cisco** - Change To: request to change "at least 6 X 100/1000G Cu , 8 X 1G/10G/25G SFP/ SFP+ , 4 X 40GG QSFP from day 1 with all SFP included. All below requirements should be available from day 1 onwards. **Paloalto Networks**: Please specify the quantity of Single Mode LR and Multi-Mode SR transceivers required for internal connectivity. Also, Please specify whether 40G or 100G transceivers has to be provisioned from day 1. **iValue**: The solution should have atleast 8 X 1G Cu , 16 X 1G/10G SFP/ SFP+ , 4 X 100G QSFP28 from day 1 with all SFP included and minimum 1 free slot for future expansion. All below requirements should be available from day 1 onwards	**Paloalto Networks**: Module clarifications is required considering the revamped setup although existing architecture can easily work on SR Multi-Mode modules for both SFP+ and 40G/100G ports. **iValue**: Certain functionalities in existing clause are vendor specific, change requested to make requirement more generic and allow other bidders to participate.	Refer Corrigendum

324	Cisco, Checkpoint , Paloalto Networks, Sify, SISL	Annexure B.G	162	Next Generation Firewall	The appliance hardware should be a multicore CPU architecture with a hardened 64 bit operating system to support higher memory and should support minimum of 64 GB of RAM or more.	**Cisco** :- Request to change as " The appliance hardware should be a multicore CPU architecture with a hardened 64 bit operating system to support higher memory and should support minimum of 128 GB of RAM or more". **CheckPoint**: The appliance hardware should be a multicore CPU architecture with a hardened 64 bit operating system to support higher memory and should support minimum of 128 of RAM or more. **Paloalto Networks**: Considering the Hardware benchmarking defined in the RFP ask, Please request for 128GB minimum RAM provisioned in the Hardware from day 1. **Sify**: The appliance hardware should be a multicore CPU architecture with a hardened 64 bit operating system to support higher memory and should support minimum of 128 of RAM or more. **SISL**: The appliance hardware should be a multicore CPU architecture with a hardened 64 bit operating system to support higher memory and should support minimum of 64 GB 128 of RAM or more.	**CheckPoint**: The productivity of your firewall depends heavily on the efficiency of the firewall memory. If the firewall memory is not high enough, it can become a painful bottleneck for the firewall. This means that the processing of the CPU or the central processing unit has to wait for the execution. This latency prevents the firewall from reaching its actual working potential. Request to reconsider the RAM sizing as suggested.	Refer Corrigendum

325	Cisco, Fortinet, Paloalto Networks, Sify	Annexure B.G	162	Next Generation Firewall	Firewall Solution throughput should have at least 50 Gbps.	**Cisco** : Request to remove it as this is stateful firewall throughout and RFP already asks for Threat Prevention throughput which makes this redundant and contradictory. **Fortinet**: Firewall Solution throughput should have at least 150 Gbps. **Paloalto Networks**: Next Generation Firewall Solution throughput should have at least 50 Gbps with App-ID/AVC/Application Control and Logging enabled considering 64KB HTTP/appmix transactions. **Sify**: Firewall Solution throughput should have at least 150 Gbps.	**Fortinet**: Since the number of ports asked in the tender are on the higher side and Firewall throughput number is very less so please ammend the same and ask for more number of throughput. **Paloalto Networks**: Some vendors might interpret Firewall throughput to be RAW Firewall throughput and considering NGFW appliance, majority of flows traversing through appliance will be Layer 7 So, Please mention	As per RFP

326	Cisco, Paloalto Networks	Annexure B.G	162	Next Generation Firewall	Firewall Solution should have at least 5 Lakh new sessions per second	**Cisco :** Request to change as" Firewall Solution should have at least 200 Lakh New sessions per second measured with NGFW and App ID enabled" Since the ask is for NGFW the connections parameters should also be measured with same. Hence requesting change. **Paloalto Networks**: Firewall Solution should have at least 5 Lakh New Layer 4 sessions per second or minimum 3,70,000 new Layer 7 sessions per second	**Paloalto Networks**: Few leading OEMs calculate sessions on Layer 4 which is not the correct way of benchmarking NGFW appliances considering SDC setup where it will be catering to traffic flows destined for e-citizen based applications. There is degradation of at least 80% on session calculations when same Layer 4 sessions are computed for 1 byte HTTP sessions	Refer Corrigendum

327	Cisco, Paloalto Networks	Annexure B.G	162	Next Generation Firewall	Firewall Solution should have at least 32M maximum sessions and concurrent sessions	**Cisco :** Request to change as " Firewall Solution should have at least 32M Maximum sessions or 5M maximum sessions measured with NGFW and App ID enabled" Since the ask is for NGFW the connections parameters should also be measured with same. Hence requesting change. **Paloalto Networks**: Firewall Solution should have at least 32M Maximum Layer 4 sessions and concurrent sessions or minimum 5 Million Layer 7 concurrent sessions	**Paloalto Networks**: Few leading OEMs calculate sessions on Layer 4 which is not the correct way of benchmarking NGFW appliances considering SDC setup where it will be catering to traffic flows destined for e-citizen based applications. There is degradation of at least 80% on session calculations when same Layer 4 sessions are computed for 1 byte HTTP sessions	Refer Corrigendum

328	Cisco, Checkpoint , Paloalto Networks, Sify, SISL	Annexure B.G	162	Next Generation Firewall	Redundant power supply is available along with 1200 W AC or DC (1:1 fully redundant) , 100–240 VAC (50–60 Hz)	**Cisco :** Request to remove it as this should be per OEM's recommendation on the appliance. Different appliances/vendors will have different power ratings. **CheckPoint**: Request to either delete the clause or make changes as suggested below: Redundant power supply is available along with 1300 W AC or DC (1:1 fully redundant) , 100–240 VAC (47-63Hz) **Paloalto Networks**: Please don't mention 1200W PSU rating. **Sify**: Request to either delete the clause or make changes as suggested below: Redundant power supply is available along with 1300 W AC or DC (1:1 fully redundant) , 100–240 VAC (47-63Hz) **SISL**: Request to either delete the clause or make changes as suggested below: Redundant power supply is available along with 1300 W AC or DC (1:1 fully redundant) , 100–240 VAC (47-63Hz)	**CheckPoint**: Every OEM have their own hardware capability with different enviromental conditions (defined within the guidelines) so either delete the clause and make it generic for other OEMs to comply. **Paloalto Networks**: Every OEM has their own Hardware architecture and PSU calculations. Mentioning 1200W will be OEM specific and will restrict other OEMs to participate.	Refer Corrigendum
329	Cisco	Annexure B.G	162	Next Generation Firewall	Firewall solution based on 3U space design form factor	**Cisco :** Request to change as "Firewall solution based on 1RU or higher space design form factor" Requesting change as this clause doesn’t change functional requirement but allows more vendor participation. Hence requesting change.		Refer Corrigendum

330	Cisco, Checkpoint , Fortinet, Paloalto Networks, Sify, SISL	Annexure B.G	162	Next Generation Firewall	Firewall Solution should have at least 2TB log capability	**Cisco :** Request to change as "Firewall Solution should have at least 800GB log capability" Since there is a firewall management console which would do logging, reporting and management such high logging on firewall is not required and is favouring a particular vendors appliance. Hence requesting change. **CheckPoint**: Management Solution should have at least 2TB log storage. **Fortinet**: Solution should have at least 8TB log capability with dedicated log appliance. paloalto Networks: Please mention either within the appliance or offered as a solution with Central Management and Reporting Server if required **Paloalto Networks**: Please mention either within the appliance or offered as a solution with Central Management and Reporting Server if required. **Sify**: Management Solution should have at least 2TB log storage. **Sify**: Solution should have at least 8TB log capability with dedicated log appliance. **SISL**: Management Solution should have at least 2TB log storage.	**CheckPoint**: Management server stores firewall logs, therefore the logging capability or requirement should be explicitly define with management server or log server. **Fortinet**: Restrictive Point: Every OEM has its own set of architecture and point is favouing single OEM. So we suggest you to please make it generic and ask the reports on separate appliance with higher harddisk. **Paloalto**	Refer Corrigendum

331	Cisco, Paloalto Networks, iValue	Annexure B.G	162	Next Generation Firewall	Proposed Solution must support User identification and control such as VPNs, WLAN controllers, captive portal, proxies, Active Directory, eDirectory, Exchange, Terminal Services, syslog parsing, XML API	**Cisco :** Request to change as "Proposed Solution must support User identification and control such as VPNs, captive portal, proxies, Active Directory, directory, Exchange, XML API etc". In network user authentication is through AD or LDAP which passes the information, WLAN, Syslog are not user authentication protocols/engines they are just information. hence requesting change. **Paloalto Networks**: Please remove WLAN controllers. **iValue**: Internal user database, Native LDAP, Microsoft Active Directory, RADIUS, TACACS+, Microsoft Exchange, Client Certificates"	**Paloalto Networks**: This is an OEM specific clause. **iValue**: Certain functionalities in existing clause are vendor specific, change requested to make requirement more generic	Refer Corrigendum
332	Cisco, Paloalto Networks	Annexure B.G	162	Next Generation Firewall	Should have more than 10,000 (excluding custom signatures) IPS signatures or more.	**Cisco :** Request to change as "Should have more than 25,000 (excluding custom signatures) IPS signatures or more" As IPS is the primary inspection engineer and it inspects traffic by pattern matching and behavioural analysis. It is important to have a higher signature count so that threats can be detected and stopped. Hence requesting change. **Paloalto Networks**: Should have more than 20,000 (excluding custom signatures) IPS signatures or more.	**Paloalto Networks**: Wider signature reference will ensure better security efficacy for the critical SDC infrastructure	As per RFP

333	Cisco, SISL, CheckPoint, Fortinet, Paloalto Networks, Sify, iValue	Annexure B.G	162	Next Generation Firewall	Solution must be scalable management of minimum up to 30,000 hardware and all VM-Series Firewalls; role-based access control; logical and hierarchical device groups; and templates	**Cisco:** Request to change as "Solution must be scalable management of minimum up to 50 hardware and all VM-Series Firewalls; role-based access control; logical and hierarchical device groups; and templates" Current clause is favouring a particular OEM.Hence requesting change. **SISL, CheckPoint, Sify**:Solution must be scalable management of minimum up to 25 to 50 hardware and all VM-Series Firewalls; role-based access control; logical and hierarchical device groups; and templates. **Fortinet**: Remove the Point. **Paloalto Networks**: Please provide clarification on this clause as there is no clarity on the exact ask. **iValue**: Solution must be scalable management of minimum up to 500 hardware and all VM-Series Firewalls; role-based access control; logical and hierarchical device groups; and templates	**SISL, CheckPoint, Sify**: Firewalls are placed at Internet Layer and Intranet layer in data center. With HA configuration and integration with anti-apt devices too the maximum requirement should not exceed more than 10-20 devices and considering the future scalbility we can re-size the requirement between 25 to 50. This clause is one OEM specific and restricting participation. Hence reconsider the sizing. **Fortinet**: Restrictive Point:	Refer Corrigendum

334	Fortinet, Sify	Annexure B.G	162	Next Generation Firewall	The proposed solution must have atleast 240 GB SSD RAID1 at storage level	**Fortinet**: Remove the point. **Sify**: Remove the point.	**Fortinet**: Restrictive Point Since you have already asked for 2 TB log storage so request you to please remove the same and ask dedicated log appliance for the reports. **Sify:** Restrictive Point Since you have already asked for 2 TB log storage so request you to please remove the same and ask dedicated log appliance for the reports.	Refer Corrigendum

335	Fortinet, Paloalto Networks, Sify	Annexure B.G	162	Next Generation Firewall	Firewall Solution Threat Prevention throughput should have at least 30 Gbps.	**Fortinet**: Firewall Solution Threat Prevention throughput should have at least 30 Gbps from single device. **Paloalto Networks**: Firewall Solution Threat Prevention throughput should have at least 30 Gbps considering 64KB HTTP transaction size. **Sify**: Firewall Solution Threat Prevention throughput should have at least 30 Gbps from single device	**Fortinet**: TPT number should be achieved from single Box stacking should not be allowed. **Paloalto Networks**: Considering NGFW platforms, throughput benchmarking should be defined otherwise throughput will degrade with varied packet size and this will impact the appliance performance. Defining Packet size will ensure the platform baselining during throughput	As per RFP

336	Fortinet, Sify	Annexure B.G	162	Next Generation Firewall	Firewall Solution should have inbuilt redundant hot-swappable power supply and in built hot-swappable/replaceable fans/ tray/ modules	**Fortinet**: Firewall Solution should have inbuilt redundant hot-swappable power supply /swappable/replaceable fans/ tray/ modules. **Sify**: Firewall Solution should have inbuilt redundant hot-swappable power supply /swappable/replaceable fans/ tray/ modules.	**Fortinet:** Restrictive Point: Every OEM has its own set of architecture and we offer redundant hotswappable Power supply. But for fans we have fixed architecture. So request you to please ammend the point. **Sify**: Restrictive Point: Every OEM has its own set of architecture and we offer redundant hotswappable Power supply. But for fans we have fixed architecture. So request you to please ammend	As per RFP
337	Sify	Annexure - B.G	162	Next Generation Firewall (NGFW)	Next Generation Firewall (NGFW)	Kindly confirm, do we need to propose additional NGFW other than mentioned in section 7.3.2.5.5?		As per RFP

338	SISI, CheckPoint, Sify	Annexure - B.G.17	162	Next Generation Firewall (NGFW)	Solution should capable and support Inline malware prevention automatically enforced through payload-based signatures, updated daily	Need clarification	Is the sandbox functionality required on-prem or on cloud?	As per RFP
339	SISI, CheckPoint, Sify	Annexure - B.G.21	162	Next Generation Firewall (NGFW)	Proposed solution will able to provide accurate identification and classification of all devices on a network, including never-before-seen devices.	Need clarification	Kindly help us to understand the use case of IoT.	As per RFP
340	SISI, CheckPoint, Sify	Annexure - B.G.28	162	Next Generation Firewall (NGFW)	Firewall solution should have manual NAT and Auto-NAT, Remote access VPN (SSL, IPsec, clientless); mobile threat prevention and policy enforcement based on apps, users, content, device, and device state	Firewall solution should have manual NAT and Auto-NAT, Remote access VPN (SSL, IPsec, clientless); mobile threat prevention and policy enforcement based on apps, users, content/ device/ device state.	This clause is one OEM specific and restricting participation. Hence request to change the language for wider participation.	As per RFP
341	SISI, CheckPoint, Sify	Annexure - B.G.30	162	Next Generation Firewall (NGFW)	Solution must have minimum operating temperature from 0° to 50° C	Solution must have minimum operating temperature from 0° to 40° C	Every OEM have their own hardware capability with different enviromental conditions (defined within the guidelines) so either delete the clause and make it generic for other OEMs to comply.	Refer Corrigendum

342	SISI, CheckPoint, Sify, iValue	Annexure - B.G.34	162	Next Generation Firewall (NGFW)	Solution should support GUI, CLI, XML-based REST API	Solution should support GUI, CLI and REST API.	JSON is parsed into a ready-to-use JavaScript object and XML is much more difficult to parse than JSON. This clause is one OEM specific and restricting participation. Hence request to change the language for wider participation.	As per RFP.
343	SISI	Annexure B.G	162	NGFW	For firewall OS, CVE (Common Vulnerabilities and Exposures) must be available/disclosed on public web sites.		Justification: Considering the state data center environment, it is imperative to know the Common Vulnerabilities and Exposures (CVE) of the OEMs to mitigate the vulnerabilities by taking appropriate actions	As per RFP

344	Wijungle, iValue	Annexure A.G.10	162	NGFW	Firewall solution based on 3U space design form factor	**Wijungle**: Firewall solution based on 2U/3U space design form factor. **iValue**: Firewall solution based on 2U/3U space design form factor	**Wijungle**: The requested specification device available in 2U rack so please allow this value also. **iValue**: Certain functionalities in existing clause are vendor specific, change requested to make requirement more generic	As per RFP
345	Fortinet, Sify	Annexure B.G	163	Next Generation Firewall	Solution must support Networking feature such as dynamic routing (RIP, OSPF, BGP, multiprotocol BGP), DHCP, DNS, NAT, route redistribution, ECMP, LLDP, tunnel content inspection	Solution must support Networking feature such as dynamic routing (RIP, OSPF, BGP, multiprotocol BGP), DHCP, DNS, NAT, route redistribution, ECMP, LLDP, tunnel content inspection /Deep packet inspection	Please make it more generic since theterminology used is specific to single OEM	Refer Corrigendum

346	Fortinet, Sify, iValue	Annexure B.G	163	Next Generation Firewall	Proposed Solution must support Virtual systems such as logical, separately managed firewall instances within a single physical firewall, with each virtual system’s traffic kept separate	**Fortinet,Sify**:Proposed Solution must support 10 Virtual systems and scalable to 100 Virtual Systems such as logical, separately managed firewall instances within a single physical firewall, with each virtual system’s traffic kept separate. **iValue**: Proposed Solution must support 25 Virtual systems and upgradable to 100 for logical, separately managed firewall instances within a single physical firewall, with each virtual system’s traffic kept separate"	**Fortinet, Sify**: Since you have asked for Virtual Systems feature but didn't mentioned any number for the same. so we request you to please ask 10 Virtual license from day one. So that if you want to use Virtual system feature you don't need to buy any license for it and have finacial impact to the organisation. **iValue**: Different OEMs provide different ways for logical segregation. It will be benefitial for bidders to provide	Refer Corrigendum
347	iValue	Annexure - B.G.22	163	Next Generation Firewall (NGFW)	Proposed Solution must have Iot Device security feature which support ML-based anomaly detection	Request to remove.	This clause is specific to OEM. Request to remove.	As per RFP

348	iValue	Annexure - B.G.24	163	Next Generation Firewall (NGFW)	Proposed solution must have Third-party threat intelligence for automated prevention and automated features to update IoCs (Such as API , Automated, Manual etc)	"Proposed solution must have Third-party threat/native intelligence for automated prevention and automated features to update threat information."	This is OEM specific and would request to amend the clause.	As per RFP
349	iValue	Annexure - B.G.25	163	Next Generation Firewall (NGFW)	Firewall must support Quick detection of C2 or data theft employing DNS tunneling	"Firewall must support Quick detection of C2 or data theft by employing employing data loss prevention either by integrating with third party DLP or from the same OEM in future."	Data theft can be prevented using data loss prevention solution because data loss prevention solution provides mechanisms to identify the data and prevent it from exfilterating.We would request to amend the clause mentioned.	As per RFP

350	iValue	Annexure - B.G.27	163	Next Generation Firewall (NGFW)	Firewall should have bidirectional control over the unauthorized transfer of file types and Social Security numbers, credit card numbers, and custom data patterns	Request to remove.	This is data loss prevention requirement. We understand that RFP has not asked for separate data loss. We would like to know wether data loss is required or not, If not then this becomes a OEM specific and request to remove the clause.	As per RFP
351	iValue	Annexure - B.G.35	164	Next Generation Firewall (NGFW)	The firewall should be supported Third party log analyzer tools and Log server and SIEM /event correlation module for NGFW & Anti APT.	"The firewall should be supported integration with thirdparty Log server or SIEM"	All firewall expect a select few Firewalls OEMs proved correlation modules. Correlation modules are functionality of SIEM solutions. Firewall devices provide integration with SIEM for forwarding events in the syslog format.	As per RFP

352	iValue	Annexure - B.G.43	164	Next Generation Firewall (NGFW)	The management platform must be a dedicated OEM appliance for Centralized Management, Logging and Reporting.	"The management platform must be a dedicated/same OEM appliance/software/VM for Centralized Management, Logging and Reporting."	Not all OEM offer management as appliance. We would request an amendment to this clause.	As per RFP
353	iValue	Annexure - B.G.40	164	Next Generation Firewall (NGFW)	The proposed solution should support Active-Active or Active-Standby and should be proposed with N+1.	Certain functionalities in existing clause are vendor specific, change requested to make requirement more generic "The proposed solution should support Active-Active or Active-Standby and must support high availability and load balancing between multiple ISPs, including VPN connections,Multi-Link VPN link aggregation, QoS-based link selection,admin should be able to manipulate the sensitivity of an application based on jitter,packetloss & latency"		As per RFP
354	iValue	Annexure - B.G.42	164	Next Generation Firewall (NGFW)	The Management platform must be accessible & integreable via a web-based/tool based interface as per scope.	Certain functionalities in existing clause are vendor specific, change requested to make requirement more generic.		As per RFP
355	Sify	Annexure - B Non It Components	168	Supply, installation, testing and commissioning of BMS	RACK PDU (5 points per unit) - 34+8	Request you to share the detailed specs for PDU as specification are not mentioned in tender Document .	For the state of Art SDC data center it is recommended to have Intellegent PDU with less form factor and having C-13 and C-19 sockets,so that data can be fetch in DCIM for Monitoring.	Refer Corrigendum

356	Sify	DCIMS	214	Architecture	e. Datacenter Inventory Management to include Cage, space, Management. It should be scalable to include Capacity Planning and Thermal Imaging options.	Request you to add the Detailed+E4 Capacity planning detailed specs as mentioned below:- 3D View with ability to see where and how assets are placed and connected inside the Racks. View device data within the physical layout for instant access to device details and asset attributes, and overview of data center operations. **Risk planning for proactive incident management:** It should give insights into how incidents (such as cooling or equipment failures) may impact your devices and infrastructure to optimize risk planning. **Predictive Analysis/What If Analysis & Hypothetical Provisioning/Modelling to ease decision making** (such as: where is the best place to put a new server, Am I having sufficient power, cooling & space to place new equipment, etc.) **Audit trail:** Track all cage and facility equipment changes over the data center lifecycle, ensuring transparency and easy identification of requirements for predictive maintenance. **Get an overview of current space and power capacities. Analytics :** Leverage		As per RFP

357	HPE	Annexure - A/7.4.42	101 & 102/ 65		AMC of IT infrastructure in PSDC	Majority of HPE products like Bl460c blade server, c7000 chassis, storage currently installed in SDC are nearing end of support life(EOSL) and further 5 year AMC extension will be a challenge. Request authority to allow SI for tech refresh for EOSL models with latest generation infrastructure on pay per use model where customer will have the option to procure infra. with no upfront payment and pay quarterly for Infra as a service. Pay as you go or rental model is now available with all leading OEM's in market.		Refer Corrigendum
358	HPE	NA	NA		NA	Place of delivery, Bill to and Ship to locations are not clearly established in the RPF document		Plz refer clause no.: 3.1.14
359	Sify	NA	NA		General Query	We request that a company that have undergone business restructuring / demerger, Parent / Subsidiary companies incorporation/ project experience / financial credentials should be considered subject to parent company holds controlling stake in bidder or if bidder holds 100% equity in subsidiary company	We request for this clause inclusion to allow qualified and experienced bidders to participate but are new company that have been incorporated / formed due to business restructuring in the parent company.	As per RFP
360	Cisco				Request to clarify	Can we propose a SaaS based APM platform offering hosted out of AWS Mumbai region.		As per RFP

361	Cisco				Request to clarify	Is there a requirement for APM solution to offer container based monitoring solution to future proof the investment made on APM solution.		As per RFP
362	HPE				New Clause	We request addition of the following clause as a new clause: In the event of expiry of the contract or termination of contract for any reason including the reasons under clauses 6.3, 6.4 or 6.5, DCRPG shall make payments for all products and services supplied by the Bidder till the date of expiry or termination.	The bidder is entitiled to receive payments for all products and services supplied by the Bidder till the date of expiry or termination irrespective of whether the termination is for material default, insolvency or convenience since the bidder would have provided the products/services and DCRPG can use those products/services.	As per RFP

363	HPE	Limitation of Liability			New clause	We request that the following clause be added as a new clause to the contract for the purposes of limiting the liability of the bidder: To the full extent permitted by law, the Service Provider shall not be liable to DGPRG in respect of any Claim for loss of profits, business, revenue, anticipated savings, goodwill, data or contracts or any type of special, indirect, economic, punitive or consequential loss (including loss or damage suffered as a result of any claims brought by a third party) even if such loss was reasonably foreseeable or the Service Provider had been advised of the possibility of the Service Provider incurring the same. The Service Provider's cumulative liability to DGPRG under any contract for all claims made under or in connection with the contract whether arising under contract (including under any indemnity), negligence or any other tort, under statute or otherwise at all will not exceed the total contract value in aggregate of the contract.	We request that the service provider's cumulative liability for any type of liability be capped to a maximum of the total contract value so that it is commensurate with the payments under the contract. We also request that any indirect or consequential damges should be excluded considering the same would not be foreseeable by the service provider.	As per RFP
364	Paloaltonetworks			**Additional Clarification**	Please define what security services are desired on the NGFW appliance from day 1 including the feature capabilities and this should be clearly specified in the RFP specifications			As per RFP

365	Sify, UpTime Institute				Actual Scope of Work to be included in the scope of the Contractor / SI to define the nature of duties and deliverables	Request for Proposal (RFP) / Tender From M/S Uptime Institute (or) their Authorized Indian Representatives / Partners / Collaborators to Procure Tier – III Certification Services of Design Certification, Construction Certification Readiness Program, Construction Certification, Construction Monitoring, Commissioning Plan, Commissioning Script and Operations Certification Readiness Program, Operations Certification, across all phases of Project for Client's Name Data Center to be located at Mohali, Punjab, India Including all Civil & MEP Services & Works on EPC basis. The Entire Development is to be Designed adhering to the local body / building norms / NBC 2016 along with compliance to Uptime Tier – III (with Tier – III Certification in all four stages i.e. During Design, Build, Commissioning and Operation of Data Centre) across all phases of the project along with ancillary services supporting the Main Certification for the Data Centre works and services.		As per RFP

366	Sify,UpTime Institute	7.3	33	SDC Upgradation Scope of Work w.r.t. Tier III Certification Recommended norms for achieving Tier III Certification	Recommendations from Uptime Institute to achieve Tier III Certfication, kindly have them included in the RFP to ensure complaince as per Tier III norms. This will define the actual upgradation cost for e.g. Cost for Testing & Commissioning	1. As you are aware, the Data Center facility shall observe Integrated System Testing on 100% Live Simulated Load condition based on preplanned Commissioning Script basis the Final IT load capacity to evaluate the performance of each and every system and sub-system to verify against the design and performance criteria and shall be witnessed / validated directly by Uptime. Uptime shall mandatorily witness and approve specific tests based on preplanned test scripts to evaluate the performance of each and every system at full load (simulated heat load banks) to verify against the design performance criteria 2. For the IT Load of more than 4 kW / Rack, it is recommended for follow continuous cooling to avoid any temperature variance during power change-over 3. Computer Room temperature should be maintained as per latest ASHRAE TC9.9 Class A1 Server 4. Change of Data Center Room Temperature should be as per latest ASHRAE TC9.9 guideline		As per RFP

367	NetScout, Progress	Missing critical APM clause		Missing critical APM clause	New Suggestion	Solution should analyse and investigate the traffic from various Private Cloud, Containers, Dockers & other virtual Infrastructure for security analytics. Virtual and physical network functions in Private cloud environments as either a software agent within a multi-tenant Virtual Machine (VM) or a stand-alone, purpose-built VM. The solution must offer Monitoring in a Private Cloud deployment using industry standard ecosystems, including deployment flexibility to install in either. •Microsoft Hyper-V •VMware's ESX, NSX-V & NSX-T •Openstack •Ubuntu/KVM	Its an important function to monitor every activity related to performance of the applications running over network. Solution will be covering every microparameter for packet capture so that exact information related to the point of application performance/delay/ issues can be detected and investigated	As per RFP

368	NetScout	Missing critical APM clause		Missing critical APM clause	New Suggestion	Solution should have DNS monitoring feature - Solution should provide visibility for A-AAAA, PTR-NAPTR and Put/Post queries. - Solution should provide latency Variation over time with DNS application usage. It will should give idea of how latency varies if DNS query varies. - Solution should provide performance variation over Latency. To get an idea on numbers of request, FAST, Degraded, Slow and timeouts with DNS application latency if any. Solution should provide DNS applicatoin failures overview for accessing the DNS application health. - Solution should provide error code distribution for defined period for A-AAAA, PTR-NAPTR and SRV, To get a detailed idea on error message which are getting generated in between specific client-Server communication transaction.	Practically we have seen that majority of the issues comes due to the DNS application which effects every application of the envirnment. It is always recommended to monitor the DNS application performance over the network which is currently missing. Pls add the clause as suggested	As per RFP

369	NetScout	Missing critical APM clause		Missing critical APM clause	New Suggestion	Solution should support Synthetic (or Active) testing using test agents to do the service tests as mentioned below , -Web Tests , VoIP Tests -Bandwidth –TCP and UDP Test -Verify VPN availability -FTP Tests, Latency Tests -Loss Tests, Ping Tests -Port availability Tests, Port Latency Tests -Custom Tests, Business Transaction Tests -HTTP, HTTPS, DNS, FTP, and Other Network Service Tests .	Practically Synthtic testing should not be limited to only web application as in a DC environment there are multiple applications which are critical and should be monitored.request you to add the clause as suggested.	As per RFP
370	NetScout	Missing critical APM clause		Missing critical APM clause	New Suggestion	Solution should have in-depth database monitoring. * Should provide visibility for DB Connect, DB Query * Should provide visibility for Latency, Requests and Failures for DB Connect, DB Query. * Solution should provide latency Variation over time with database application usage. To get the idea of how latency varies if Usage (bps) varies for DB Connect, DB Query.	Databases are the major issues when it comes to the application performance as these are moslty the backend of the application. Major monitoring funtionality of the database is missing which helps in troubleshooting the actual causes of the application performance. request you to add the clause as suggested.	As per RFP

371	NetScout	Missing critical APM clause		Missing critical APM clause	New Suggestion	The solution should provide detailed packet decode and analysis for a wide range of industry standard protocols and applications, providing detailed decoding of web-based applications protocols, and services. 10 Gbps of traffic to be captured from day 1	only flow or sythentic testing are not enough to find the root cause of any performance issue being just that samples of some perticular time interval where to investigate the same packet captures are required which could give every visibility aspect of the network for the perticular application. request you to add the clause as suggested	As per RFP
372	iValue, Sify	Annexure - B.E		Security Incident Management Solution (SIEM)	Suggested	The proposed solution must be able to index all data from any application, server or network device including logs, configurations, messages, traps and alerts, metrics and performance data without any custom adapters for specific formats so that the analyst can have end to end visibility of the ecosystem.		As per RFP
373	iValue, Sify	Annexure - B.E		Security Incident Management Solution (SIEM)	Suggested	The proposed solution must be able to build an unstructured index or store data in it's original format without any rigid schema.		As per RFP

374	iValue, Sify	Annexure - B.E		Security Incident Management Solution (SIEM)	Suggested	The proposed solution must be able to support predictive analytics to predict future values of single or multi-valued fields. This will help security analytics to predict the attack patters or specific attacks using multiple fields in the alerts or logs.		As per RFP
375	iValue, Sify	Annexure - B.E		Security Incident Management Solution (SIEM)	Suggested	The proposed solution should natively have ML capabilities and should not have separate engine/compute requirements for running ML models.		As per RFP
376	iValue, Sify	Annexure - B.E		Security Incident Management Solution (SIEM)	Suggested	The proposed solution should give visualization of operational health of the Windows, Linux & Unix environment through a single dashboards customizable to service-groupings in your environment		As per RFP
377	iValue, Sify	7.3.2.5.4	38	Layer-3 Switch (Core)	Layer-3 Switch (Core) - PSDC is using HP core switch in HA mode which is required to be upgraded. The proposed switch should have at least 48 nos. 10G/25 SFP+ ports 4 x 40G/100G QSFP+ QSFP28 uplink ports and should support 1 RJ-45 serial console port,1 RJ-45 out-of-band management port and 1 USB port.	The Switch should support line rate & non-blocking Layer 2 switching and Layer 3 routing		Refer Corrigendum

378	iValue, Sify				PSDC is using HP core switch in HA mode which is required to be upgraded. The proposed switch should have at least 48 nos. 10G/25 SFP+ ports 4 x 40G/100G QSFP+ QSFP28 uplink ports and should support 1 RJ-45 serial console port,1 RJ-45 out-of-band management port and 1 USB port.	There switch should not have any single point of failure like power supplies and fans etc should have 1:1/N+1 level of redundancy and must be hot swappable.		Refer Corrigendum
379	iValue, Sify					Switch and optics must be from the same OEM		As per RFP
380	iValue, Sify					Device should have IPv6 ready logo cert with IPv4 and IPv6 dual stack support		
381	iValue, Sify					Switch should have the following interfaces:		
382	iValue, Sify					a. 48*1/10/25G SFP+ port populated with 40* 10/25G multirate SR, 4*10G BaseT, 4*1G BaseT (if OEM does not have a SFP which supports 10 and 25G both, then 40 numbers of 10G SR & 16 numbers of 25G SR SFPs may be supplied)		
383	iValue, Sify					b. 8 *100GbE QSFP ports populated 6*100G SR SFP & 2*100G 5 Meter DAC cable		
384	iValue, Sify					Switch should support IEEE Link Aggregation for redundancy across two switches in active-active mode		
385	iValue, Sify					The switch should support 256k IPv4 prefix routes or above		
386	iValue, Sify					The switch should support hardware-based load balancing at wire speed using LACP and multi chassis ether channel/LAG		
387	iValue, Sify					Switch should support minimum 4Tbps of throughput capacity		

388	iValue, Sify					Switch should support minimum 256,000 no. of MAC addresses		
389	iValue, Sify					Switch should support Jumbo Frames up to 9K Bytes on all Ports		
390	iValue, Sify					Support storm control to prevent degradation of switch performance from storm due to network attacks and vulnerabilities		
391	iValue, Sify					Switch should support Policy Based Routing		
392	iValue, Sify					Switch should provide multicast traffic reachable using:		
393	iValue, Sify					a. PIM-SM		
394	iValue, Sify					b. PIM-SSM		
395	iValue, Sify					c. PIM-BiDir		
396	iValue, Sify					d. Support RFC 3618 Multicast Source Discovery Protocol (MSDP)		
397	iValue, Sify					e. IGMP V.2 and V.3		
398	iValue, Sify					Switch should support Multicast routing		
399	iValue, Sify					Switch should support for BFD For Fast Failure Detection		
400	iValue, Sify					Switch should support VXLAN with EVPN control plane		
401	iValue, Sify					Switch must support symmetric VXLAN integrated routing and bridging with EVPN active-active multihoming support.		
402	iValue, Sify					Should support 8 queues per port, priority queuing, round-robin queuing		
403	iValue, Sify					Should support QoS classification, policing and shaping, DSCP and COS.		
404	iValue, Sify					Should support WRED, Explicit Congestion Notification, priority flow control, data centre bridging.		

405	iValue, Sify					Switch should support control plane i.e., processor and memory Protection from unnecessary or DoS traffic by control plane protection policy		
406	iValue, Sify					Switch should support for external database for AAA using:		
407	iValue, Sify					a. TACACS+		
408	iValue, Sify					b. RADIUS		
409	iValue, Sify					Switch should support for Role Based access control (RBAC) for restricting host level network access as per policy defined		
410	iValue, Sify					Switch should support MAC ACLs		
411	iValue, Sify					Should support Standard & Extended ACLs using L2, L3 and L4 fields		
412	iValue, Sify					Switch should support minimum IEEE 1588 PTP transparent and boundary clock mode		
413	iValue, Sify					Should support telnet, ssh, https, SNMPv3, TWAMP, event manager, scheduler and configuration rollback for ease of operations and management		
414	iValue, Sify					Visibility & Automation: All Network switches and SFP's should be from same OEM and should be provided along with software from Switch OEM (for all network switches) for unified monitoring, provisioning and telemetry solution from the same OEM. Should support telemetry with time-series database view, traffic flow analytics, PSIRT/BUG visibility, configuration compliance, endpoint tracking, POAP/ZTP, device resource utilization, auto topology view, alerts.		

415	iValue, Sify					Should have advance mechanisms for in-depth troubleshooting and monitoring like packet capture on the device, GRE encapsulated port mirroring, targeted filtered mirroring, realtime streaming telemetry, microburst congestion detection and reporting, TWAMP, sFlow/IPFIX.		
416	iValue, Sify					device should support on-device execution of python script, bash script and docker containers for automation and programmability support		
417	iValue, Sify					Switch should support onboard Packet Capture using Wireshark/tcpdump in real time for traffic analysis and fault finding		
418	iValue, Sify					All relevant licenses for all the above features and scale should be quoted along with switch		
419	iValue, Sify					Device should support same OS image as other network switches in network for simplified operations and management.		
420	Vertiv, HPE	Non It Components	212	Data Center Infrastructure Management Systems (DCIMS) / Cluase no. C	The system shall monitor SNMP/Modbus TCP devices and manage Inventory for at least 4 Racks.	The software solution shall support any vendor agnostic facility device to be integrated under monitoring using standard SNMP(v1/v2/v3), Modbus TCP/IP & BacNet over IP. DCIM being critical Monitoring tool should support all 3rd party integration along with IT protocols i.e SNMP, Mobus, BacNet etc.		Refer Corrigendum

421	Vertiv	Non It Components	212	Data Center Infrastructure Management Systems (DCIMS) / Cluase no. C.1	Any Modbus to Ethernet gateways needed to bridge existing Modbus points to DCIM monitoring system will be under the DCIM vendor scope. Commonly accepted protocol is Modbus / Modbus Tcp. Connectivity/wiring to the relevant proposed gateways will be under bidder scope hence Customer will share with DCIM vendor the connectivity schematic along with communication protocols for various I/O points needed for KPI reporting on common Portal.	Request you to kindly share the Final IO summary to size the number of gateway required		As per RFP
422	Vertiv	Non It Components	212	Data Center Infrastructure Management Systems (DCIMS) / Cluase no. C.2	Proposed DCIM solution OEM should be engaged in the development of data center infrastructure management systems whose products have been in satisfactory use in similar service for a minimum of 7 years under the same OEM name, any change of ownership and name change for OEM will be treated as disqualification.	Proposed DCIM solution OEM should be engaged in the development of data center infrastructure management systems whose products have been in satisfactory use in similar service for a minimum of 10 years. Request you to kindly add - The OEM should have installed similar kind of DCIM solution for more than 100 racks in any 3 PSU/Banks/Government Institution who are registered in India and vendor should be able to provide supporting proof of the same.	DCIM being critical Monitoring tool for DC must have OEMs in this field with minimum 10 years to understand the pain points of IT/DC and address the same.	As per RFP

423	Vertiv	Non It Components	212	Data Center Infrastructure Management Systems (DCIMS) / Cluase no. C.4	DCIM software OEM should have own dedicated Business Units within the company to handle the following: a. Datacenter Lifecycle services for Performing Regular Datacenter Audits and also help in Improving the throughput of implemented OEM solutions at client end including DCIM. b. Global scale Datacenter Service & Support Team for Implementation and troubleshooting DCIM d. Dedicated DCIM support BLOG for all clients who buy DCIM to provide anytime query escalation to Global DCIM product experts of the DCIM bidder. e. Cloud Based Datacenter Remote Monitoring Services to offer second layer of intensive coverage over Threshold Violations, Rules, Alerts arising within the DCIM. This system should have a	Request you to kindly remove point "e". AS Cloud based DC Remote monitoring is Not recommended in Data Centres because of threat of data breach. Request you to kindly Include following The software solution shall also be subject to owner’s policies for security without effect on the Server or Client operation. ·System must support import of certificate, use self-sign certificate or upload a certificate. ·The system shall not deploy protocols inherently susceptible to intrusion. ·The system shall strip all unnecessary files and services from the Web service to protect the owner from intrusions. ·Must support the ability to add security certificates via the user interface. The solution shall come as a package which includes application & a stable database.		As per RFP

424	Vertiv		212	Data Center Infrastructure Management Systems (DCIMS) / Cluase no. D.1	Proposed DCIM solution should be designed such that it can scale up to integrate Building side Infrastructure devices using SNMP, Modbus® TCP protocol or in cases where Building side devices cannot talk over IP, proposed DCIM solution can utilize Modbus to Modbus TCP gateways for cross Integrations.	Include "DCIM proposed is scalable to 5000 devices monitoring, supports SNMP V1, V2 , V3 , modbus TCP/IP, BacNet/IP & also restful API support."	DCIM being critical Monitoring tool should support all 3rd party integration along with IT protocols i.e SNMP, Mobus, BacNet etc.	As per RFP
425	Vertiv		212	Data Center Infrastructure Management Systems (DCIMS) / Cluase no. D.2	DCIM platform should also be capable of pushing monitored device information to any Third-Party NMS system using SNMP INFORM/REQUEST procedures	Supports RestFul API , it is recommended to pull data from NMS thus ensuring layered security , however from Vertiv DCIM Push and pull both are supported (a pre-requisitie for NMS is it should accept and open its interface to accept pushed data)	DCIM being critical Monitoring tool should support all 3rd party integration along with IT protocols i.e SNMP, Mobus, BacNet etc.	As per RFP

426	Vertiv		212	Data Center Infrastructure Management Systems (DCIMS) / Cluase no. D.3	DCIM solution should be able to push DCIM monitored points to any third party BMS system using Modbus TCP out channel.	DCIM being critical Monitoring tool should support all 3rd party integration along with IT protocols i.e SNMP, Mobus, BacNet etc. Also backup and restore is one of the vital paratmerters, Request you to kindly include the same. Supports RestFul API , it is recommended to pull data from BMS thus ensuring layered security , however from DCIM Push and pull both are supported (a pre-requisitie for BMS is it should accept and open its interface to accept pushed data) , * during Design OEM to ensure that the gateway used in instrrumentation are multi client support thus multiple system can pull data when needed. Software solution must support one click backup and restore option, thus enabling user to revert to last known good configuration of application, this feature will help operation team to bring system online as quickly as possible during any breakdown or revert to known configuration in case of any manual changes to be revert to last good working application config.		As per RFP

427	Vertiv		213	Data Center Infrastructure Management Systems (DCIMS) / Cluase no. D.4	Proposed DCIM system should be modular in nature that provides us flexibility to purchase and expand enhanced modules according to our future need. The DCIM should be able to run on a physical, virtualized server and offer Cloud based option for parallel high critical infra monitoring.	Request you to kindly remove "and offer Cloud based option for parallel high critical infra monitoring."DCIM is complete package , includes APP + DB all in one , DCIM can be deployed on Physical as well as virtual server. Cloud based DC Remote monitoring is Not recommended in Data Centres because of threat of data breach. Also cloud based offering is different application for such custom request cannot be sized in RFP stage (scale of cloud , connectivity, SLA, location of cloud , Cost and such factors varies from cloud to cloud)		As per RFP
428	Vertiv		213	Data Center Infrastructure Management Systems (DCIMS) / Cluase no. D.5	DCIM vendor should have both Perpetual-Capex and Pay as You Use-SaaS, style licensing for DCIM solution.	Request you to kindly remove Pay as You Use Saas and include "DCIM sofware and license is perpetual in nature and license is provided to customer as perpetual (no Pay as use license is applciable)."		As per RFP
429	Vertiv		213	Data Center Infrastructure Management Systems (DCIMS) / Cluase no. D.6	On Premise -Monitoring setup for DCIM side should be created in such a way that all Infrastructure Site monitoring should happen using a single Monitoring system installed as Physical/Virtual appliance at one site.	please provide a site survey and detail IO summary of infra to be covered under DCIM		As per RFP

430	Vertiv		213	Data Center Infrastructure Management Systems (DCIMS) / Cluase no. D.8	To ensure a proper redundancy of the DCIM setup all software components should be VMWARE enabled so that customer can install the same onto VMWARE platform and utilize the capabilities of VMWARE Redundancy architecture for Disaster Recovery where needed.	Vmware must be provided by the customer. Request you to kindly confirm scope for VMware, Request you to kindly Include Software solution proposed should support user to deploy HA or DC/DR (high availability or redundancy) architecture, with 100% guaranteed uptime.		As per RFP
431	Vertiv		213	Data Center Infrastructure Management Systems (DCIMS) / Cluase no. D.9	Proposed system shall offer web services (WSDL, REST, SOAP) to allow integration of the DCIM system to third party Customization platforms. Vendor must submit a detailed Schema documentation for the same.	Request you to kindly remvo WSDL, SOAP. As WSDL & SOAP is separate services and not part of DCIM scope.		Refer Corrigendum
432	Vertiv		213	Data Center Infrastructure Management Systems (DCIMS) / Cluase no. D.10	DCIM server/VM system should allow integration of client email server via SMTP channel as well as it should support integration to SMS Gateway servers by utilizing the HTTP post Method.	Customer must have a SMS gateway? · System must support https · File type supported must be PEM		Refer Corrigendum

433	Vertiv		213	Data Center Infrastructure Management Systems (DCIMS) / Cluase no. D.11	Proposed DCIM system should also have (an option which customer can add in future) of Cloud based analytics system and Remote Monitoring Services that proactively minimizes downtime and reduces break-fix resolution time through smart alarming, remote troubleshooting and visibility into client device lifecycle. It will help the OEM to:	Request you to kindly remvoe Cloud based analytics system & Remote monitoring servcies. Cloud based analytics system & Remote monitoring servcies is Not recommended in Data Centres because of threat of data breach.		As per RFP

434	Vertiv		214	Data Center Infrastructure Management Systems (DCIMS) / Cluase no. F.1	Proposed DCIM should be created in separate installations to maintain sanctity of data as follows: a. Gateway/Convertor Devices: Required for connecting to third party BMS/ third party BMS controllers/field devices and building side device Integrator system. b. Monitoring layer: Responsible for polling SNMP and Modbus TCP based Infrastructure devices inside the Datacenter like Rack Mount PDU, EMS systems etc. c. Portal for Report and KPI display to integrate with Operations and Monitoring Layers of Datacenter. D. Option of adding Cloud based data lake for Machine Learning and Advance Analytics for key critical Infrastructure	Request you to kindly remvoe EMS Systems etc, and remove D. Option of adding Cloud based data lake for Machine Learning and Advance Analytics for key critical Infrastructure UPS devices to monitor UPS wear and tear. Cloud based data lake for machine lerning...EMS is Enterprise management system is not a part of DCIM , it is a part of IT assets (CPU,Memory, HDD,etc). Cloud DCIM is not recommended and supported. Also Cloud based system & remote monitoring services is not recommended in Data Centres because of treat of Data Breach.		As per RFP

435	Vertiv		214	Data Center Infrastructure Management Systems (DCIMS) / Cluase no. F.5	DCIM Monitoring Layer server/VM system should allow integration of client email server via SMTP channel.	Request you to kindly Include Dependent on access level, manage the event through acknowledgements, deletions, sorting rules and viewing alarm notes. · Alarm console and alarm pop up window · Audible system sound alert for alarm condition · E-mail		As per RFP

436	Vertiv		214	Data Center Infrastructure Management Systems (DCIMS) / Cluase no. F.7	DCIM Monitoring Layer should allow for Auto Timed/Scheduled Report Emailing to selected audience on required key performance indicators. These Reports should be mailed to relevant users as CSV format.	Request you to kindly Include **IT Assets:** The solution includes an asset database. IT Assets are representations of a physical rack assets that will be associated to IT Racks within the software. These assets are created within a dedicated assets feature. The assets feature contains a detailed list view of assets. The asset feature shall provide the following capabilities: · Asset database which is sortable, filterable and searchable by key asset data · Add assets – manually or via CSV import · Edit assets individually or by group · Support of assets within assets (blade server enclosures, as an example) · Export & import of existing asset database · Ability to assign IT assets to IT racks		The bidder can propose better solution according to their approach & methodology over and above the minimum requirements given in this RFP.

437	Vertiv		215	Data Center Infrastructure Management Systems (DCIMS) / Cluase no. F.8	Proposed Monitoring system should have option of in-built integration to 24x7 Remote Monitoring Services from the same OEM who is providing the DCIM. This service shall be enabled SaaS based pricing option to us, so that the service can be enabled or disabled on need basis. This service should offer us APP based notifications of any critical alerts and support from OEM support team on APP Chat to troubleshoot the device issues.	Request you to kindly remove this point. Saas based pricing option etc. Built ins Remote monitoring services is not a Part of DCIM software , this is a Separate service (customer must purchase this service separately , the contract and pricing for this service is a separate line item and not a part of intial RFP)		As per RFP

438	Vertiv		215	Data Center Infrastructure Management Systems (DCIMS) / Cluase no. F.9	To ensure data security for any vendor proposing cloud Based solution following rules would apply: 1. Flow of information over IP will be allowed using HTTPS TLS 1.2 encrypted outbound connections on port 443. 2. All connections from the Cloud based monitoring gateway to OEM DCIM Monitoring cloud should be validated using an industry standard 2048-bit RSA certificate and data is encrypted in transit using 128-bit AES encryption. 3. To prevent unauthorized or even malicious access to OEM -DCIM Cloud system, all parts of the cloud engine should be protected by state-of-the-art firewalls. In addition, this cloud network should be configured to only allow access from specific sources (using Access Control Lists), and only a limited	Request you to kindly remove point F.9. Cloud based service. Cloud based analytics system & Remote monitoring servcies is Not recommended in Data Centres because of threat of data breach.		Refer Corrigendum
439	Vertiv		215	OEM Qualifications	ISO9001, ISO 14001, ISO 50001	50001 OEM Specific. Request you to kindly remove 50001 and Allow ISO 9001 & 14001 , please add 27001 for ISMS security which is a must for larger participation		Refer Corrigendum

440	Vertiv			Addional Points		**Tenancy :** Proposed solution must support active directory or LADP integration. Proposed solution must have an inbuilt feature to support multiple internal departments by mapping them against tenant ID, thus it should provide information regarding power used, capacity used by a internal department or users	This is an important feature for Restriction, permission, read - write for different users, authentications etc.	As per RFP

441	Vertiv			Addional Points		**Configuration of operators:** User names and passwords: . Permissions: The Permissions field allows administrators to set access level for different users. Permissions include the following options: o Read/Write: Full read access and full write access to the entire system. o Read Only: Full read access but no writes or changes may be done. o Read/Acknowledge: Full read but no write or changes may be done, except to alarm database for acknowledging alarms. System owner shall have the ability to assign combinations of roles and privileges to users that define access levels. o User password expiration o Auto-log off period	This is an important feature for Restriction, permission, read - write for different users, authentications etc.	As per RFP

442	Vertiv			Addional Points		**Events and Alarms:** Events and alarms associated with a specific system, area or equipment shall be displayed on the main site view and/or within an embedded alarm console. The solution must have native capability to alarm on all connected devices. The alarm system shall have multiple alarm types depending on the severity level. Users must be able to drill down through views to locate alarm sources. The alarm should be accessible from the device level. Events, alarms and reporting actions shall have the following capabilities: **Alarm Console:** Capable of displaying the following information for each alarm that has occurred in the system: Alarm State (with associated status color), Site, Device, Circuit, Tenant, Point, Point Type, Point Unit, Source, Last Alarm, Acknowledge Requested, Acknowledge State, Last Acknowledgment, Last Acknowledged By, Last Return to Normal, Last Update, Alarm Class, Warning Class, Message and Notes. The Alarm Console must also	This is an important feature for Restriction, permission, read - write for different users, authentications etc.	As per RFP

443	Vertiv		Page no. 37	Minimum existing infrastructure to be upgraded / 7.3.2.5.1	Upgradation of Rack Power of existing DC - Existing DC was planned with 42 Racks and 4 KVA load which is required to be augmented. Minimum new load to be considered is 10 KVA per rack with atleast 15 min. backup, necessary non-IT Infra needs to be replaced and installed with 5 years support. Service providers should upgrade cables, PDU, containment, fiber runner, cooling etc. to meet the requirement without any downtime on working days.	IPDU Specifications is not mentioned in the RFP, Request you to kindy Consider the 3 phase IPDU in the solutoin, as rack load to be revised to 10KVA , new or existing PDU must support min. 10KVA or 11KW Load . Please share the technical specifications for IPDUs		Refer Corrigendum
444	Vertiv			Addional Points		Rack technical specifications is missing in the RFP, Request you to kindly share the rack specification		As per RFP
445	Vertiv		201	UPS Critical Load (point I)	The UPS should be provided with phase sequence correction at input	Request you to kindly change this clause as "The UPS should be provided with phase sequence correction/detector at input		As per RFP
446	Vertiv		202	UPS Critical Load (point K.E)	Maintenance bypass -In maintainence bypasss the load is supplied with unconditioned power from the manual maintenance bypass input switch provided in a separate enclosure with each UPS	Request you to kindly add "Maintenance bypass should be part of the frame."		As per RFP

447	Vertiv			UPS Critical Load (point N)	The UPS shall be provided with oscilloscope for measuring and recording input/output voltage & current waveforms in the event of any abnormal or alarming situation arises. In-case it is not available within the UPS, then two numbers of 3 Phase Power Meters (one at Input & one at Output) shall be provided along with the UPS system which can capture the Waveforms Triggered during the failure event.	This is vendor specific specification , Request you to kindly change this without oscilloscope.		As per RFP
448	Vertiv			UPS Critical Load (point P)	UPS shall have built-in feature to test UPS at 100% Load without the need of any external Load Bank. Incase this feature is not available within the UPS, Vendor shall provide an External Load Bank equal to UPS Capacity which will be kept at the site till the end of Warranty period.	Request you to kindly consider "Load bank shall be provided for FAT/SAT only, which is on chargable basis."		As per RFP
449	Vertiv		196	Precision Air Conditioner / Compressor	PAC should be equipped with Latest-generation hermetic scroll compressors	As Per Latest Technology Varible Scroll Compressor Should be considerd for energy effcient Solution . Request you to kindly consider the Varible Scroll Compressor.		Refer Corrigendum
450	Vertiv				There should be a minimum 2 compressors and minimum 2 circuits per PAC.	Request you to kindly consider as "Should be as per OEM Design" . With latest Variable Scroll technology Dual Compressor not required , Additional Capital Expenditure.		As per RFP
451	Vertiv		196	Precision Air Conditioner /	Each circuit is composed of, as standard, a fluid intake complete with a Rota lock on-off cock	This is OEM Specific, Request you to kindly remove change this as - Should be as per OEM Design No Compulsion of Rota Lock .		Refer Corrigendum

452	Vertiv		197	Refrigerating circuits (air-cooled DX versions)	Circuit should also include Liquid Line Solenoid Valve (LLSV) & Non-Return Valve (NRV) in the discharge line for inherent capability to take care of long length piping between indoor & outdoor units and for safe operation of compressors.	Can Be installed in low Side externally , if piping length is Long , Not necessirily required inside the unit .		As the site is live so required minimal brazing work at site so please provide factory fitted.
453	Vertiv		197	Electronic Expansion Valve	Electronic Expansion Valve (EEV) controlled by the microprocessor with special software created and tested by the manufacturer shall be provided.	Request you to kindly allowe Both EEV and TXV.		Refer Corrigendum
454	Vertiv		197	Electrical Heating	Electric heating with aluminum-finned heating elements (minimum 15 Kw rating in multistage arrangement),	Electric Heater Capacity Should be as per OEM Design. Such High Capcity Heater not required . Probally Heater is being utilized during de humdification process. Not energy effcient solution.		Refer Corrigendum
455	Vertiv		198	Humidifier	Immersed-electrode humidifier (minimum 8kg/hr rating) for modulating sterile steam production with the automatic regulation of the	Latest Genration infrared humdifier Should be allowed , Which is independent of water Quality and consumes nominal power , and is not consumable . Rating should be as per oem Design .		As per RFP

456	Progress			Missing critical APM clause	New Suggestion	Monitoring and analysis of DNS traffic – items like type of query, domain, returned value, reply. These statistics are reported using standard technology (IPFIX).	Practically we have seen that majority of the issues comes due to the DNS application which effects every application of the envirnment. It is always recommended to monitor the DNS application performance over the network which is currently missing. Pls add the clause as suggested	As per RFP

457	Progress			Missing critical APM clause	New Suggestion	Solution should have in-depth database monitoring. * Should provide visibility for DB Connect, DB Query * Should provide visibility for Latency, Requests and Failures for DB Connect, DB Query. * Solution should provide latency Variation over time with database application usage. To get the idea of how latency varies if Usage (bps) varies for DB Connect, DB Query.	Databases are the major issues when it comes to the application performance as these are moslty the backend of the application. Major monitoring funtionality of the database is missing which helps in troubleshooting the actual causes of the application performance. request you to add the clause as suggested.	As per RFP

458	Progress			Missing critical APM clause	New Suggestion	The solution should provide detailed packet decode and analysis for a wide range of industry standard protocols and applications, providing detailed decoding of web-based applications protocols, and services. 10 Gbps of traffic to be captured from day 1	only flow or sythentic testing are not enough to find the root cause of any performance issue being just that samples of some perticular time interval where to investigate the same packet captures are required which could give every visibility aspect of the network for the perticular application. request you to add the clause as suggested	As per RFP
459	Progress			Missing critical APM clause	New Suggestion	Solution should support Native deployment option for Google Cloud. Support for processing of mirrored traffic in Google Cloud.	Public Cloud integration and support is major challenge with solution. Solution should support public cloud integration from day one.	As per RFP

460	Progress			Missing critical APM clause	New Suggestion	Solution should support Native deployment option for Amazon AWS. Support for processing of mirrored traffic in Amazon AWS. Ability to collect, process and visualize AWS VPC flow logs which contain information about the traffic captured in Amazon Virtual Private Cloud.	Public Cloud integration and support is major challenge with solution. Solution should support public cloud integration from day one.	As per RFP
461	Progress			Missing critical APM clause	New Suggestion	A single instance of the system can be configured to monitor the traffic of multiple customers (tenants) independently without mutual interactions. Visibilities to flow-sources and profiles are defined for each tenant. Tenant administrators manage users and roles within a tenant.	Public Cloud integration and support is major challenge with solution. Solution should support public cloud integration from day one.	As per RFP
462	Progress			Missing critical APM clause	New Suggestion	Solution allows monitoring the communication between application servers and database servers (Oracle, MSSQL, PostgreSQL, MySQL, MariaDB).	Databases are the major issues when it comes to the application performance as these are moslty the backend of the application. Major monitoring funtionality of the database is missing which helps in troubleshooting the actual causes of the application pe	As per RFP

463	Progress			Missing critical APM clause	New Suggestion	Solution allows defining monitoring metric groups only for a selected subset of transactions (e.g. a group for PHP files, multimedia files, a part of clients and users).	Databases are the major issues when it comes to the application performance as these are moslty the backend of the application. Major monitoring funtionality of the database is missing which helps in troubleshooting the actual causes of the application	As per RFP
464	Progress			Missing critical APM clause	New Suggestion	Solution allows filtering of the list of individual transactions using various criteria (e.g. IP address of the user, response time, SLA, user name, start and end of the transaction and others). This provides information about which group of users communicated with the application, what was the response of the application, for which users and transactions was the application unavailable, etc.	SLA are the major issues when it comes to the application performance. This helps providing route cause of the application issue.	As per RFP

465	Progress			Missing critical APM clause	New Suggestion	Solution should detect anomalies in DNS, DHCP, SMTP, multicast traffic and non-standard communications.	Identifying the security issue which is impacting application performance and exposing application to outside unathorized user is major challenge now days to degrade the performance and security issue. Solution should have capability to identify the basic vulnerbility posture used by different malisious activity.	As per RFP

466	Progress			Missing critical APM clause	New Suggestion	The system uses built-in IP and host reputation databases for the detection of security incidents (e.g. communication with botnet command & control servers, phishing server access, etc.). IP and host reputation databases are provided by the vendor and updated at least once per 24 hours. The system allows drawing on other sources of IP and host reputation data for the automatic detection of security incidents.	Identifying the security issue which is impacting application performance and exposing application to outside unathorized user is major challenge now days to degrade the performance and security issue. Solution should have capability to identify the basic vulnerbility posture used by different malisious activity.	As per RFP
467	Progress			Missing critical APM clause	New Suggestion	Support for HTTP, VoIP SIP, DNS, Samba/CIFS, DHCP, SMTP, POP3, IMAP and MS SQL (TDS) protocols.	Solution should support different application type as well.	As per RFP
468	HPE	General		General	New Suggestion	SLD (Single line diagram of electrical & BMS is required.		As per RFP
469	HPE	General		General	New Suggestion	Present DC Layout (CAD) format with all rack power ratings is required.		As per RFP

470	HPE	General		General	New Suggestion	For making this datacenter UPTIME Tier 3 rated we will need to change a lot of components inside Datacenter as current built facility is noncomplying as per UPTIME requirements for a Tier 3 datacenter. Some examples to state are that a few non-compliant material is used in existing datacentre built like no fire rated doors, multiple openings, multiple windows in DC , non-Compliant POI room, staging rooms and non-protected spaces wide all facility are there. Existing partitions need to be re-designed as per Tier 3 .		As per RFP
471	HPE	General		General	New Suggestion	As per tender clause : 7.3.2.5.8, we need to upgrade the existing PSDC from Tier II to Tier III. We understand that this is not limited to technical and electrical, All required enhancements of the physical infrstaructure including civil and interiors will need to be carried out and will be suggested as part of vendor response.		As per RFP
472	HPE	General		General	New Suggestion	As per site visit existing DC is having 42 racks of 4 KW each. As this now needs to be converted to 10 KW. This will need replacement of all Electrical panels, UPS, cabling and PDUs. This will required a considearble time initially for the datacenter setup.		As per RFP

473	HPE	General		General	New Suggestion	Current network passice cabling is not a structured cabling as all current racks are hybrid with no specific category of Network rack,Storage rack wise segregation. This necessisates new design of the passive cabling in lieu of existing setup without involving any down time of current datacenter except of the change window while actual migration of the IT infra to new racks after the DC build.		As per RFP

474	HPE	7.4.13	43	PSDC Website	The selected bidder shall develop a dedicated website for Punjab State Data Centre (PSDC) for providing digital e-services delivery platform within 3 months of signing of contract	The selected bidder shall develop a dedicated website for Punjab State Data Centre (PSDC) for providing digital e-services delivery platform within 6 months of signing of contract	The website development will need a lot of requirement gathering time which will need PSDC inputs and a feedback and acceptance after this is developed and completed. Initial 3 months of period is not sufficient. This time should be changed from 3 months to 6 months. Also any delay p[enalty on this website development shopuld be waved off for any tasks pending due to inputs not recieved from PSDC	Refer Corrigendum

475	HPE	7.3.2.5.7	39	IBMS	Integrated Building Management System (IBMS) - PSDC is using IBMS for monitoring of all non-IT equipment (energy meter, DG set parameter, UPS parameter, FAS, WLD, VESDA etc.) using Siemens software (DIGIGOCC) and same is required to be upgraded.	Integrated Building Management System (IBMS) - PSDC is using IBMS for monitoring of all non-IT equipment (energy meter, DG set parameter, UPS parameter, FAS, WLD, VESDA etc.) using Siemens software (DIGIGOCC) and same is required to be upgraded/ replaced with latest version of same make or any other tool covering all functionalities.		Refer Corrigendum
476	HPE		212	DCIM	Proposed DCIM solution OEM should be engaged in the development of data center infrastructure management systems whose products have been in satisfactory use in similar service for a minimum of 7 years under the same OEM name, any change of ownership and name change for OEM will be treated as disqualification.	Proposed DCIM solution OEM should be engaged in the development of data center infrastructure management systems whose products have been in satisfactory use in similar service for a minimum of 7 years. The OEM has product development team in India and Make in India product will be preferred.		As per RFP

477	HPE	D11	213	DCIM	Proposed DCIM system should also have (an option which customer can add in future) of Cloud based analytics system and Remote Monitoring Services that proactively minimizes downtime and reduces break-fix resolution time through smart alarming, remote troubleshooting and visibility into client device lifecycle. It will help the OEM to: - resolve issues remotely - improve time to resolution - lower your cost of maintenance - understand wear and tear - predict failures - improve utilization of your infrastructure	Proposed DCIM system should also have (an option which customer can add in future) of Cloud based analytics system and Remote Monitoring Services that proactively minimizes downtime and reduces break-fix resolution time through smart alarming, remote troubleshooting and visibility into client device lifecycle. it should have data points report of device as below: -Alarms for Device -Alarm for floor - Alarms Report by Group of Devices -Battery Discharge -Data points Report of Devices by Floor -Consumption Report by Device -Energy Consumption Report by Group -Consumed Capacity -Report Device by Manufacturer -Device by UDP -Device Inventory -Device Inventory by Asset Class -Rack Inventory -Rack Space Availability -Space Area Summary -Card Capacity -Alarms by Device -Device by Manufacturer		As per RFP
478	HPE			Helpdesk		Asset Management need to provide in the helpdesk tool		It's a part of EMS tool / Helpdesk.
479	HPE			Helpdesk		Change Management need to provide in the helpdesk tool		As per RFP
480	HPE			Helpdesk		Problem Management need to provide in the helpdesk tool		As per RFP

481	HPE			Helpdesk		Maintenance Management need to provide in the helpdesk tool		As per RFP
482	UpTime Institute	New Suggestion		Recommended Trainings	Training & Education for relevant staff	AOS Trained Staff - Minimum 3-5 nos in order to O&M as per Tier Standards ATS Trained Staff - Minimum 1-3 nos (Management Team of PSDC) ATD Trained - Bidder to have ATD Certified Designer from Uptime Institute on Board in order to Design as per Tier Standards		As per RFP