BOBCARD
CREDIT REIMAGINED

RFP for procurement of Servers, Network and Software component and Implementation.

RFP NO: CO: BOBCARD/ IT RFP / 2024-25, RFP Dated: 23rd October, 2024.

Sr. No.	Pg No	Point No	Tender Original Clause		Clarification	Request for Change / Modification / Addition / Deletion	BOBCARD Responses
1	Annexue 02 Technical Evaluation Criteria	1	The bidder should have supplied and installed similar to proposed hardware in last three (3) financial years, i.e. 2021-2022, 2022-23, 2023-24 (Bidder to provide details in Annexure K and submit PO / Contract details)		1. Please let us know if experience before last 3 years would be considered? Please allow to share the PO copies of last 5 years as well. 2. We understand that bidder should have supplied similar hardware in the past, please confirm. 3. Please let us know whether solution expereince mentioned on different PO's would be consiered. for eg, bidder might submit separate PO for firewall experience, separate po for IPS expereince, separate PO for WAF experience, etc.	Addition	The bidder should have supplied and installed proposed OEM hardware in last three (3) financial years, i.e. 2021-2022, 2022-23, 2023-24 (Bidder to provide details in Annexure K and submit PO / Contract details) yes we can consider separate PO.
2	Annexue 02 Technical Evaluation Criteria	2	The bidder should have deployed and configured proposed software as per OEM standard on proposed hardware in last three (3) financial years, i.e. 2021-2022, 2022-23, 2023-24 (Bidder to provide details / submit PO / Contract details)		1. We understand that bidder should have supplied similar solutions in last 3 years, please confirm? 2. Please let us know if experience before last 3 years would be considered? Please allow to share the PO copies of last 5 years as well.	Addition	The bidder should have deployed and configured proposed software as per OEM certified and standard hardware in last three (3) financial years, i.e. 2021-2022, 2022-23, 2023-24 (Bidder to provide details / submit PO / Contract details)
3	Annexue 01 Eligibility Criteria	4	The Bidder should be profitable organization for all three financial years mentioned in above.		Request you to amend the clause as belows -The Bidder/ group/subsidiary should be profitable organization for all three financial years mentioned in above.	Request for Modification	The Bidder should be profitable organization in atleast 2 out of 3 financial years mentioned in above. 2023-24 is mandatory
4	Annexue 01 Eligibility Criteria	5	Documents to be submitted Copy of the order and / or Certificate of completion of the work. The Bidder should also furnish user acceptance report.		Request you to amend the clause as belows -Copy of the order and / or Certificate of completion of the work. Explaination - Since This is new technology we have adopted two or three year back. We have implemented few project on this new technology and its under implementation phase hence request you allow submission of ongoing projects	Request for Deletion	No Change
5	Annexue 01 Eligibility Criteria	6	Client references and contact details (email/ landline/ mobile) of customers for whom the Bidder has executed similar projects in India. (Start and End Date of the Project to be mentioned) in the past (At least 3 client references are required)		Requst to amend the below clause as belows - Client references and contact details (email/ landline/ mobile) of customers for whom the Bidder has executed similar projects in India. (At least 2 client references are required)		No Change
6	Annexue 01 Eligibility Criteria	7	Certification Requirements Documents to be submitted - Copy of latest ISO Certification and relevant IT Certification required to provide the products/services mentioned in the RFP.		Please clarify which ISO Certification needs to be provided		ISO 27001 latest
7	Annexue 01 Eligibility Criteria	Annexure 01 - Eligibility Criteria	Bidder should have experience of minimum 3 years in providing the Proposed Products/Services mentioned in the RFP.		Kindly modify the clause as mentioned below: Bidder should have experience of providing the Proposed Products/Services mentioned in the RFP.	Change	No Change
8	Appendix 03 Bill of Material	4	WAF + LoadBalancer		Do we need to provide separate appliance for WAF and Loadbalancer or we need to provide WAF + Loadbalancer in one integrated appliance. Kindly confirm?	Clarification	Bidder is can chose either of the both option
9	Appendix 03 Bill of Material		IPS & IDS		Do we need to provide separate appliance for IPS or we need to provide Firewall + IPS in one integrated appliance. Kindly confirm?	Clarification	IPS will be separate Appliance

10	8	5	BOBCARD will perform its own Vulnerability assessment/ Penetration testing (VAPT), Security assessment & Risk assessment audit on the entire solution before go live/twice in year and the bidder needs to fix all the vulnerabilities/risks highlighted in the reports at no extra cost to BOBCARD.		Do we need to quote separately for this service BOB CARD team has already a service provider assigned for this activity	Clarification	BOBCARD has already on boarded service provider for VAPT & risk assessment
11	9	17	In case of the Go-Live delays by the Bidder, the financial Penalty as per the BOBCARD policy will be imposed on the Bidder at 0.5% of the total contract value per month of delay, to the maximum of 5% of the total contract value as per the agreement between the BOBCARD and the successful Bidder.		Kindly cap the overall penalty to: 0.1% of the total contract value per month of delay to maximum of 0.5% of the total contract value	Modification	No Change
12	9	18	Bidder should follow BOBCARD policy on Change, Patch & Incident management process.		Do you have ITSM for bidder need to factor the ITSM in this rquirement	Clarification	BOBCARD have its own ITSM
13	9	2.2 Tenure	The tenure of the contract initially would be for 1 year from the date of the issuance of first purchase order. BOBCARD can further extend to 2 years at its at mutually agreed terms.		Considering the investment that bidder would make to provide the requirement of BOB CARD, cannot be recovered from 1 year contract period. Hence, we request BOB Card to provide the PO for initial conract period of 3 years	Change	Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
14	10	2.5 Training	The Bidder is required to provide training to the BOBCARD team on the proposed solution in RFP for Procurement of Servers, Network & Software components, provide a training schedule and furnish training details as per the RFP requirements for all major components.		Will the training be onsite or remote. If onsite training is required, then please let us know the location of training. Also, please let us know the number of employees who would be attending this training	Clarification	One time Training need to be provided in BOBCARD Office in person for implemented solution.
15	10	3.1 Project Scope	The successful bidder shall provide all necessary back-to-back support from OEM(s) for delivery, installation, configuration, testing, operationalisation and support of the respective Hardware and Software components (appliances, softwares etc.).		Please let us know if bidder need to factor OEM professional services for implementation, configuration and testing	Clarification	No Change. Bidder need to factor OEM support to meet the SLA .
16	12	11	The resolution time for the hardware/software related issues should be 4 hours, there should be 24*7*365 support from the OEM for all the supplied products through this RFP.		As the hardware and software issue resolution would be dependent on the OEM product, the resolution can be provied only on best effor basis. Hence we request BOB CARD to remove this clause as this is not practically achievable	Deletion	No Change.
17	13		The successful bidder should provide necessary support for closing VAPT and RA findings which will be conducted by BOBCARD.		Any dependency on the patching of the infrastrucrure would not be in scope of the bidder. Kindly add this point in the clause	Addition	Application dependency will be taken care by BOBCARD. Rest clause will be remain same.
18	17	4.Service Levels	2hrs onwards to 8hrs During Business hours, in a single day Penalties: 2.5% of Quarterly Support Cost		Kindly modify the penalty to 0.2% of quarterly support cost	Modification	No Change
19	17	4.Service Levels	Greater than 8hrs During Business hours, in a single day Penalties: 5% of quarterly support cost		Kindly modify the penalty to 0.5% of quarterly support cost	Modification	No Change

20	39	9.13 Monitoring and Audit	Compliance with security best practices may be monitored by various periodic security audits performed by or on behalf of the Company. These audits may include, but are not limited to, a review of: access and authorization procedures, physical security controls, backup and recovery procedures, security controls and program change controls.		Being in payment card industry, BOB would be regulated by RBI, PCI compliances. While the RFP mentions the requirement of security controls like Firewall, IPS, WAF, Loadbalancer ; please let us know whether other controls like DAM, FIM, HSM, SOC, NAC, etc to meet the PCI DSS compliance would be required or not. We have not seen this security controls mentioned in the RFP	Clarification	Not relevant question to this RFP
21	9	2.1	Bidder should follow BOBCARD policy on Change, Patch & Incident management process.		Hope the required tools will be provided by BOBCARD	Bidder should follow BOBCARD policy on Change, Patch & Incident management process using the existing tools of BOBCARD	Bidder should follow BOBCARD policy on Change, Patch & Incident management process using the existing tools of BOBCARD
22	Appendix-1	1	The proposed solution should be a Hyperconverged infrastructure (HCI) with 5 years comprehensive warranty		Do we need to supply HCI software with 5 year warranty or 3 year	Statements are contridicting in RFP and Appendix-1	3 year warranty + 2 year AMC mentioned in BOM
23	Appendix-3	5	One year support cost of on site L3 resource (1 server & Virtual platform)		How many onsite resource need to be provided and what would be the support hours		Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
24	Appendix-3	3	Software to be installed on servers		Do we need to provide the YoY virtualisation software cost for 3 years		one time Installation cost and YoY virtualisation software cost for 5years
25	13	17	The initial term of this contract shall be 3 years and may be extended to another 2 years subject to satisfactory performance by successful bidder and OEM(s).		What is the contract duration, 1 Year or 3 year	Statements are contridicting in RFP	Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
26	13	15	On call support for issues related to performance or breakdown of device/network. BOBCARD IT will log a call with successful bidder.		Please elaborate how the on call support need to be provided		Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
27	13	18	The Successful bidder shall assign project manager and associated support personnel for this project.		Project Manager need to be provided during implementation period or post implementation period		Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live. Till to support of 1 year
28	15	Golive-1	Before the final Go-Live the Successful bidder has to complete the development/ customization of the application as per the Technical Specifications agreed with the BOBCARD.		Please elaborage the scope of development/customization of the application		Before the final Go-Live the Successful bidder has to complete the development/ customization of the proposed Software and Hardware as per the Technical Specifications agreed with the BOBCARD.
29	15	KT-4	All applications and services are implemented as per the intent of this RFP.		Please elaborate the scope of application implementation		All proposed Software, Hardware and services are implemented as per the intent of this RFP.
30	Appendix-3 Optional Commercial	4	MySQL License		Should MySQL be a Opensource or Enterprise edition?		We need paid version only along with support.
31	8	2.1	BOBCARD will perform its own Vulnerability assessment/ Penetration testing (VAPT), Security assessment & Risk assessment audit on the entire solution before go live/twice in year and the bidder needs to fix all the vulnerabilities/risks highlighted in the reports at no extra cost to BOBCARD		We assume the VAPT tool will be provided by BoB Card (Bank)		BOBCARD has already on boarded service provider for VAPT & risk assessment
32	37	9.5	Data Migration - The selected Bidder will assist the company in migration exercise without any cost to the company.		What would be the size of the Data to be migrated?		As mentioned in this addendum

33	37	9.5	Data Migration - The selected Bidder will assist the company in migration exercise without any cost to the company.		Is there any Application Migration included as a part of this?	Please confirm any Application Migration also in the scope? or Support only for the Data migration	Yes, Migration of existing environment to new implemented setup
34	12	Sec - 3.1 Point# 4	The propose hypervisor/ Virtualization platform should support Window & Linux virtual machine. Also, support for Kubernetes platform.		Are there any current applications running on Kubernetes Platform? Or any pipeline to run applications in Containers??		No, it will be in near future
35	11	3.1 Project Scope Point #1	The supplied Hardware and Software shall be of the latest versions and should not be end of life / end of support for the next 7 years.		Request the start Date for 7 Yrs mention in the clause be specified. Is it RFP Date or Date of PO Issuance/GoLive Date or something else?	Right tenure will help align the final BOM and any discrepent inpurs will impact pricing , so requesting clarification	The supplied Hardware and Software shall be of the latest versions and should not be end of life / end of support for the next 5 years from the date of delivery
36	12	3.1 Project Scope Point #4	All Software licenses effective date shall be effective as on Go-LIVE sign off or put in use for BOBCARD operations.		Contract Start period is mentioned as PO Issuance while the SW licenses effective date is mentioed as GoLive Sign off Dates as noticed. Request Bank to keep this synchronized if this is genuine or clarify the intent	Right tenure will help align the final BOM and any discrepent inpurs will impact pricing , so requesting clarification	License effectiveness should be start from the software is ready to use. License cost will not impact to BOBCARD due to implementation delay. No license activate without informing BOBCARD.
37	12	3.1 Project Scope Point #12	Hardware RMA (Return Merchandise Authorization) should be within 24 hours		Request this be modified as below Hardware RMA (Return Merchandise Authorization) should be within 24 hours on Next business Day Basis.	RMA for a request raised on Friday may be honored by Monday due to the weekend in between , so requesting to keep this clearly specified.	Hardware RMA (Return Merchandise Authorization) should be within 24 hours on Next business Day Basis.
38	19	5.3 Price Comparisons Point #c iv	End of Sales/ End of support: The Vendor has to ensure that any application, related software supplied / put to use as part of this RFP should not have reached end of support. In the event if any equipment supplied / put to use by the vendor reaches end of support, within the contract period from the date of use, the vendor has to replace the equipment/ software at no additional cost to the Company before end of support.		End of Life/End of Sale Clause here should specifiy the start date as to if PO issuance, RFP Date or any other . Further the tenure within which EOS/EOL should not happen must be mentioned like 7 years in clause Project Scope point #1	Right tenure will help align the final BOM and any discrepent inpurs will impact pricing , so requesting clarification	The supplied Hardware and Software shall be of the latest versions and should not be end of life / end of support for the next 5 years from the date of delivery
39	9	2.2 Tenure	The tenure of the contract initially would be for 1 year from the date of the issuance of first purchase order. BOBCARD can further extend to 2 years at its at mutually agreed terms.		Contract Tenure mentioend as 1 Year from PO Issuance here while its 3 years in clause 3.1 Point 17/ Pls clarify the right tenure?	Right tenure will help align the final BOM and any discrepent inpurs will impact pricing , so requesting clarification	Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
40	13	3.1 Project Scope Point #17	The initial term of this contract shall be 3 years and may be extended to another 2 years subject to satisfactory performance by successful bidder and OEM(s).		Mentioned here is 3 years of initial contract and in 2.2 section the contract mentioned is 1 Year/ pls clarify the right tenure	Right tenure will help align the final BOM and any discrepent inpurs will impact pricing , so requesting clarification	Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live

41	30	7.2 Evaluation Methodology for Eligible Bidder Commercial Bid Evaluation	The key considerations of the TCO would be the total payouts for entire project through the contract period of 5 years.		Mentioned here is 5 years contract but in 2.2 the tenure of contrat is 1 Year, pls clarify the number to consider	Right tenure will help align the final BOM and any discrepent inpurs will impact pricing , so requesting clarification	Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
42	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Server Prod > HCI Rack Servers > 1	Total QTY is 14		Clarifictaion Needed: 1. Please provide split of quantity of servers / Nodes per location. 2. Kindly specify the number of clusters and nodes per cluster also.	clarifiction will help arrive at the boq rightly	This will be shared with only elected bidder
43	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Server Prod > HCI Rack Servers > 7	Each Rack Server Controller Cards / Controller Drive should be provided in HA mode in RAID -1.		Request Change: Each HCI Server should be configured with two BOOT drives with hardware RAID Controller. For NVMe storage drives: Provides as per Certifed HCI Node with NVMe configuration	From the HCI Rack server or Pre configured HCI NODE - RAID Controller card is not required for NVMe drives. Also, is this ask for Boot drive with RAID Controller?	Yes, we need boot drive for HCI hypervisor provided in HA mode in RAID -1
44	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Server UAT > HCI Rack Servers > 7	Each Rack Server Controller Cards / Controller Drive should be provided in HA mode in RAID -1.		Request Change: Each HCI Server should be configured with two BOOT drives with hardware RAID Controller. For NVMe storage drives: Provides as per Certifed HCI Node with NVMe configuration	From the HCI Rack server or Pre configured HCI NODE - RAID Controller card is not required for NVMe drives. Also, is this ask for Boot drive with RAID Controller?	Yes, we need boot drive for HCI hypervisor provided in HA mode in RAID -1
45	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Server Prod > HCI Rack Servers > 6	Each Rack servers should have minimum usable Storage Capacity of 10 TB of all caching SSD and other HDD. 20% disk slot on each node should be free for future expansion		Clarification needed: In virtualized environment, the storage (usable) capacity is calcluated across the cluster. Need clarification on the total capacity required across the number of nodes in a cluster.	clarifiction will help arrive at the boq rightly	as mentioned in RFP 10TB usable storage per node * no of node = total usable capacity
46	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Server UAT > HCI Rack Servers > 6	Each Rack servers should have minimum usable Storage Capacity of 10 TB of all caching SSD and other HDD. 20% disk slot on each node should be free for future expansion		Clarification needed: In virtualized environment, the storage (usable) capacity is calcluated across the cluster. Need clarification on the total capacity required across the number of nodes in a cluster.	clarifiction will help arrive at the boq rightly	as mentioned in RFP 10TB usable storage per node * no of node = total usable capacity
47	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Server Prod > HCI Rack Servers > 13 >Server Security	Request New Point to be added		Request to add the below point for security and management features for HCI Nodes Day2 operations and management of HCI Nodes for updates on Hardware and Software. HCI Node management tool should integrate with Virtual platform and Network switches. Should be able to do Firmware updates, Manage Cluster and deployment, Full stack visibility of HCI Node, TAC/Case Support, Continuous Health checks on Networking, Server, VMs , Anomalies detection, Security advisories, patch management etc.	HCI Node should integrate with Virtual platform and Network switches, Should have management software for a Firmware update, Manage Cluster and deployment, Full stack visibility HCI Node, TAC/Case Support, Continuous Health checks on Networking, Server, VMs , Anomalies detection, Security advisories, patch management,	No Change, additional feature will be consider as value add

48	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Server UAT > HCI Rack Servers > 13> Server Security	Request New Point to be added		Request to add the below point for security and management features for HCI Nodes Day2 operations and management of HCI Nodes for updates on Hardware and Software. HCI Node management tool should integrate with Virtual platform and Network switches. Should be able to do Firmware updates, Manage Cluster and deployment, Full stack visibility of HCI Node, TAC/Case Support, Continuous Health checks on Networking, Server, VMs , Anomalies detection, Security advisories, patch management etc.	HCI Node should integrate with Virtual platform and Network switches, Should have management software for a Firmware update, Manage Cluster and deployment, Full stack visibility HCI Node, TAC/Case Support, Continuous Health checks on Networking, Server, VMs , Anomalies detection, Security advisories, patch management,	No Change, additional feature will be consider as value add
49	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Microsegmentation > 1	The Solution should be capable of supporting major hardware OEMs like Juniper, Arista, Cisco, HPE and Dell. The proposed solution should be a purely software-based solution and should not be dependent on any hardware make and model.		Request below modified clause be considered: The Solution should be capable of supporting major hardware OEMs like Juniper, Arista, Cisco, HPE and Dell. The proposed solution should be a purely software-based solution and should not be dependent on any hardware make and model by creating overlay tunnels between the hosts.	The key benefits of no dependecy on hardware is by using software defined networking i.e overlay. Overlay is mandatory for network & Security automation as part of software defined data center.	No Change
50	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Microsegmentation > 2	The solution should provide a distributed firewall such that the firewalling for Virtual Machines can be provided closest to the application within the server itself without traffic going to a Physical Firewall.		Request below modified clause be considered which includes additonal points The solution should provide a distributed firewall such that the application aware and identity based statefull firewalling for Virtual Machines can be provided closest to the application within the server itself without traffic going to a Physical Firewall or regardless of underlying L2 Netwrork topology. The solution should also provide an integrated networking solution (CNI implementations) as well as provide advance turnkey container networking & firewalling services. Solution should support for container networking plug-ins, support for pod to pod communication and support for ingress controllers. The micro-segmentation solution should have a capability for stateful firewalling and ALGs (Application Level Gateway) on a per-workload granularity regardless of the underlying L2 network topology (i.e. possible on either logical network overlays or underlying VLANs), embedded in the hypervisor kernel, distributed	*As per security framework its recommended not to use standard ports for your applications and hence to have effective security on per VM basis an application/L7 firewalling is must.* Containers & Kubernetes are now part of all modern applications hence networing and security for container shall also be considered for end to end application security. there is App ID requirement is mentioned in RFP as part of "Internal Firewall" spec point # 23 hence same should be considered for mirosegmenation as well otherwise it will create non standard architecture.	No Change

51	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmenation >5	The proposed solution should provide the ability to define firewall rules at VM level for east-west traffic in order to implement Zero Trust Security		Request below modified clause be considered: The proposed solution should provide the ability to define Layer 7 application firewall rules at VM level for east-west traffic in order to implement Zero Trust Security alongwith URL Filtering and TLS inspection for encrypted traffic	Zero trust Security framework mandates TLS inspection for encrypted traffic, URL Filtering and Layer 7 application firewalling.	No Change, additional feature will be consider as value add
52	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmenation >4	The Proposed Solution including Hypervisor, SDS and Micro segmentation must be from the same OEM.		Request below modified clause be consideredL The Proposed Solution including Hypervisor, SDS, SDN and Micro segmentation must be from the same OEM.	SDN is missing in the spec, SDN will be mandatory to create complete automated Software Defined data center by creating an abstraction of the network enabling programming of network behavior in a centrally controlled manner through software applications.	No Change, SDN will be consider as value add
53	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmenation >6	The proposed solution should allow users to define granular firewall rules based on IP Addresses, Tags/Categories and Subnets to segment User Applications		Request below modified clause be considered which includes additonal points The proposed solution should allow users to define granular firewall rules for both VM and conatiners based on IP Addresses, VM Names, Tags/Categories and Subnets to segment User Applications by creating dynamic security groups. The solution should have capability to provide stateful micro-segmentation for virtual machines and Kubernetes workloads from a single console. The solution should also support enforcement of stateful distributed firewall for IPv6 VM workloads. These firewall rules can use IPv6 addresses, IPv6 CIDR, IP Sets that include both IPv4 and IPv6 addresses and security groups that can include logical ports that have both IPv4 and IPv6 addresses. IPv6 capability should be available both at management and data plane	Its necessary to have dynamic security group capability to ensure complete automation. Mentioned in the RFP page 8 -> 2.0 --> Requirement Summary--> 2.1 Intent--> mentions requirement for IPv6 "The proposed solution should support both IPv4 and IPv6."	No Change
54	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmenation >7	Solution should provide capability to create network segments by defining them entirely in software and avoid the need to re-architect your network or deploy physical appliances		Request below modified clause be accmodated: Solution should provide capability to create network segments and L2 Streching between DC and DR by defining them entirely in software and avoid the need to re-architect your network or deploy physical appliances	L2 Streching is required for better application availability considering RFP asks for 99.99 % availability on monthly basis. RFP Page 17 -> "4. Service Levels "-->"SLA: The solution is expected to be available for 99.99% on 24x7 and up time availability will be calculated on monthly basis."	No Change, L2 stretching implementation will be discuss with elected bidder.

55	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Container >2	The solution must be able to manage Kubernetes clusters. Licenses for managing Kubernetes clusters should be implemented from Day-1		Request below modified clause be accmodated: The solution must be able to manage Kubernetes clusters. Licenses for managing Kubernetes clusters along with components such as backup, container registry and monitoring alongwith Windows Container support should be implemented from Day-1	Kubernetes Cluster doesn't work in isloation but require other components such as container registry and backup solution. If not included than Bob Card will have procure them separately. And Not aving Windows Container support will block any windows based apps to be deployed on Kubernetes Platform.	Yes, BOBCARD will take care such requirement
56	NA	Appendix02 Techno Functional Requirements- Network components > internal FW NG Firewall Features NEW POINT	Must have provisioning, operations and lifecycle management of Kubernetes, automated deployment, scaling, and operation of Kubernetes clusters		Request below modified clause be accmodated: Must have provisioning, operations and lifecycle management of Kubernetes, automated deployment, Auto scaling & Auto Healing, and operation of Kubernetes clusters	Complete Automation is not possible without Auto Scaling and Auto Healing of Kubernetes Clusters. One has to manually add nodes in case of failure or unprovisioned increase in load.	No Change
57	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Container >4	Container Platform should provide single pane of Glass for Lifecycle Management of all K8S clusters deployed on prem.		Request below modified clause be accmodated: Container Platform should provide single pane of Glass for Lifecycle Management of all K8S clusters alongwith ingress, backup and container registry deployed on prem.	Kubernetes Cluster doesn't work in isloation but require other components such as container registry and backup solution. These shall too be considered for life cycle management	Yes, BOBCARD will take care such requirement
58	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management >1	The solution should provide capability of generating reports for usage, performance, compliance, health, forecasting and capacity.		Request below modified clause be accmodated: The solution should provide capability of generating reports for health, Capacity Optmization - Right Sizing (Under sized, Oversized), Reclamation (Idle, Powered off , Snapshot, Orphaned Disk , Forecasting - Capacity Forecasting, Migration assessment, Migration Planning Usage - Process and service utlization Compliance - Regulatory Benchmark (PCIDSS and ISO) Security Guidelines for Infrastructure and Cloud Management	Bob Cards will need capacity optimization capabilities to identify over-provisioned & under-provisioned resources and provide recommendations, alerts and automated actions on right-sizing and resource consumption so they can be right-sized for adequate performance and avoid resource wastage. Should provide visibility of capacity and VMs which can be reclaimed and cost visibility of the reclaimed capacity and VMs.	No Change, additional feature will be consider as value add

59	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform >Cloud Management >11	The solution should have intelligent operations with anomaly detection which will allow monitoring seasonal trends and automatically send email alert		The solution should have AI/ML driven intelligent operations & troubleshooting workbench with anomaly detection,third party infra (Server, Storage , Network, database and Application) along with parent child relatiohship mapping, service and process monitoring which will allow monitoring seasonal trends and automatically send email alert. The solution should also have log management capability for infrastructure and applications . log management solution should delivers intuitive, actionable dashboards, sophisticated analytics, and broad third-party extensibility across physical, virtual, and cloud environments.	BoB Cards will not be able to manage the infrastructure without comprhesive log management capability. Its also mandatory for from regulation/compliance perspective to have log stored for given period of time for audit. BoB Card would need apps (database and Application) to infra (Server, Storage , Network) level visibility for toubleshooting and performance monitoring.	No Change, additional feature will be consider as value add
60	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform >Cloud Management >7	The solution must have an approval process to review, reject or approve the deployment requests from the marketplace.		Request below modified clause be considered: The Solution must support multiple levels of approval with E-mail notifications with ability to automate manual provisioning and de-provisioning of the tasks and policies embedded in each layer of their application including auto -approve and auto-reject capability based on application criticality	The solution must have an approval process to review, multi level & auto reject or approve the deployment requests from the marketplace.	No Change, additional feature will be consider as value add
61	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform >Hypervisor > 6	Hypervisor should support container and opensource integration for cloud native application from day-1. Must be a Kubernetes ready from day-1.		Request below modified clause be accmodated: Hypervisor should support container both Linux and Windows along with other kubernetes ecosystems such as container registry, backup, ingress & monitoring and opensource integration for cloud native application from day-1. Must be a Kubernetes ready from day-1.	Kubernetes doesn't work in isolation and requires multiple components for production setup.	Yes, BOBCARD will take care such requirement
62	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform >Hypervisor > 16	Virtualization Manager should provide feature which can perform quick, as-needed deployment of additional virtualized hosts. When the service is running, it can push out update images, eliminating patching and update without impacting production.		Please clarify the scenario and expected outcome out of the below point in this clause: "When the service is running, it can push out update images, eliminating patching and update without impacting production."		Virtualization manager should allow addition of new nodes and patching/upgrade of hypervisor running on the node without any VM downtime.
63	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform >Hypervisor > 22	Unlimited VM replication from DC to DR (No restriction on VM replication and DR orchestration) with the capability to define Recovery Plans		Request to provide the number of VMs to be orchestrated for automated recovery and not keep open as unlimited since this approach is OEM specific . The VMs to be protected/orchestrated are limited to what can be provisioned on these 14 servers of production. Furehr pls clarify the need for Recovery Plans		No Change, can not predict the exact number of VMs for next 5 Years which need to be replicated.

64	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 23	Proposed solution should have a self-service restore feature on a per-VM basis to allow trusted application administrators to recover their own files with the ability to mount snapshots as a drive in Windows VMs		Request this be modified as below or clarify the requriement: Proposed solution should have a self-service restore feature on a per-VM basis to allow trusted application administrators to recover their own VMs from the snapshot	Please clarify this requirement, this looks like back and restore requirements so the modified clause	This will help BOBCARD to recover file without losing current state of virtual machine.
65	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 24	Hypervisor should provide Visibility for Running VM and their connectivity co-relationship with Network Ports on attached Physical TOR / Core Direct which Include Network RX/TX Bytes.		Request below modified clause with additional inputs be considered : Hypervisor should provide Visibility for Running VM and their connectivity co-relationship with Network Ports on attached Physical TOR / Core Direct which Include Network RX/TX Bytes.Solution Should provide end to end visibility across physical firewall, switch and storage, Flow Analysis and Security Planning,Guided Troubleshooting, Microsegmentation planning, RCA (Connectivity Problem, Packet Loss, N/W latency), Application Discovery, Service Monitoring , Application Dependency Mapping and monitoring of non compliant ports	Monitoring is not considering all components of the stack. Unless end to end visibility is provided as part of this solution BoB Card has to spend separately on monitoring.	Yes, BOBCARD will take care such requirement. However Hypervisor should provide Visibility for Running VM and their connectivity co-relationship with Network Ports on attached Physical Port which Include Network RX/TX Bytes.
66	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 30	Virtualization software or the solution should provide Cluster level encryption protects unauthorized data access at-rest.		Request below modified clause be considered : Virtualization software or the solution should provide Cluster level, VM Level encryption protects unauthorized data access at-rest and in transit.	Having capability to do the enscryption at app VM level and in transit is required to complete solution.	No Change, additional feature will be consider as value add
67	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Software Defined Storage > 1	Maintain primary working set copy of active data on the Local Node as VM's are hosted to provide high IOPS and low latency. Proposed solution must be proposed for faster reads and write for Business-critical Apps.		Request below additional point be added in theis clause : Proposed solution must be proposed for faster reads and write for Business-critical Apps.	Architecture is specific to one vendor, request BoB Cards to consider on outcome than specific architecture. There is no specific latency requirements mentioned in the spec.	No Change.
68	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Software Defined Storage >2	The solution must have De-duplication and Compression features licensed and implemented from day one (Should not have dependency on any proprietary hardware device).		Request below modified clause be considered: The solution must have De-duplication/Compression features licensed and implemented from day one (Should not have dependency on any proprietary hardware device).	Solution should have flexibility to implement either compression and de-duplication. BoB Cards should conisder overhead while deciding on both.	No Change
69	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Software Defined Storage >24	The proposed solution should support 1 min RPO & 1 hour RTO for critical workload in case BOB Cards wants to have this capability replication for Future use. The proposed solution should have native Replication and DR Orchestration from Day-1		What is the use case for 1 min RPO and 1 Hour RTO? is this linked with some regulatory requirement?	Replication is best handled at application level as having additional solution for infrastructure will complexity and cost for BoB Cards Its best to use extends the existing DR orchestration solution for this environment as well.	This is required for BOBCARD mission critical application. The solution should capable to support 1min RPO. The propose replication solution should be same OEM as the virtualization solution to provide seamless integration.

70	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Software Defined Storage >25	The solution provided should function even after one node failure.		Request below modified clause be considered: The solution provided should function even after two node failure.	RFP asks for 99.99 % availability SLA for the proposed solution. It will require minimum N+2 configuration for required resiliency and uptime.	No Change, additional feature will be consider as value add
71	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Software Defined Storage >31	The solution should provide enterprise data services such as compression completely in software. Software Defined Storage solution must have de-duplication and compression features Licensed and implemented from day one. These functionalities should be part of the proposed solution. The solution must have functionality to support compression and or deduplication online on data container without any downtime and data loss as per business requirement.		Request below modified clause be considered: The solution should provide enterprise data services such as compression completely in software. Software Defined Storage solution must have de-duplication or compression features Licensed and implemented from day one. These functionalities should be part of the proposed solution. The solution must have functionality to support compression and or deduplication online on data container without any downtime and data loss as per business requirement.	Solution should have flexibility to implement either compression and de-duplication. BoB Cards should conisder overhead while deciding on both.	No Change
72	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmentation > new point	Additional Point for consideration		The solution must ensure that there is not alteration in the IP address of the Virtual machine, by blocking the traffic from or to the VM inherited as a feature in the Solution.	IP/MAC spoofing is major security concern for organizations like BoB Cards handing customers data.	No Change, additional feature will be consider as value add
73	NA				The solution should support multi-tenancy to isolate networking/security for different departments/function within BoB Cards upto a minimum of 4 tenants and 5 VPCs	VPC will enable Bob Cards to create isolation from access , resources, network and security.	ange, additional feature will be consider as valu
74	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Container > 6	Should support cluster scale out i.e addition of worker nodes as and when required.		Request below modified clause be considered: Should support Automated cluster scale out i.e addition of worker nodes as and when required.	Complete Automation is not possible without Auto Scaling and Auto Healing of Kubernetes Clusters. One has to manually add nodes in case of failure or unprovisioned increase in load.	No Change
75	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > 3	The solution shall provide a single pane of glass for automated provisioning with model-based orchestration of compute, network and storage through a unified multi-tenant self-service catalog.		Request below modified clause be consiered The solution shall provide a single pane of glass for automated provisioning with model-based orchestration of compute, network , storage and Kubernetes through a unified multi-tenant self-service catalog .	All modern applications are combination of both container and VM form factor.	No Change, additional feature will be consider as value add
76	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > 5	The solution must provide a self-service portal to allow user to consume the creation of infrastructure easily.		Request below modified clause be considered: The solution must provide a self-service portal to allow user to consume the creation of infrastructure easily for both VM and Kubernetes	All modern applications are combination of both container and VM form factor.	No Change, additional feature will be consider as value add

77	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Cloud Management > 8	The software must allow the designer to use shell script, PowerShell script to code the automation.		Request below modified clause be considered: The software must allow the designer to use shell script, PowerShell script, Python and node JS to code the automation.	Python and nodeJs are very popular language for scrpting in terms resource availability and community support	No Change, additional scripting will be value add
78	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Cloud Management > 9	The software must allow the designer to design VM blueprints.		Request below modified clause be considered: The software must allow the designer to design Multi VM & Kubernetes blueprints.	All modern applications are combination of both container and VM form factor.	No Change, additional feature will be consider as value add
79	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Cloud Management > 12	The solution should have simple low-code, no-code automation engine which allows automating day-to-day routine tasks		Request below modified clause and adidtoinal inpurs on the clause be considered: The solution should have simple low-code, no-code automation engine which allows automating day-to-day routine tasks such as Snapshot creation, Addition of Disk, Power Cycle (Suspend , Shutdown, Reboot, reset), Resize, Rebuild, Additional of Network, VM Unregister , Delete,connect remote console, Change Security Group with capability to create additional resource actions as out of the box capability.	All modern applications are combination of both container and VM form factor.	No Change, additional feature will be consider as value add
80	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Cloud Management > New Point	New Point		Solution should provide capability to define and showcase cost to create cloud like experience to the business unit with the overall cost spend on the infrastructure [server hardware, storage, licenses, application, maintenance, labor, network, facilities , etc.	Bob Cards will need Cost transparency (Showback and Chargeback capability) across private, hybrid to optimize planning and prioritization of VM/ Server/Application onboarding/provisioning	No Change, additional feature will be consider as value add
81	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF & IPS	New Point		We request BoB Card to allow for both software and hardware based solution for Load Balancer, WAF, IPS/IDS. As these components are dynamic as per application consumption requirements and considering bob card is directly managing customer data, its very critcal that these components are added as part of sofwate defined stack.	Modern applications increasingly require software-defined networking (SDN) and security solutions due to their need for greater flexibility, agility, and scalability. Traditional networking and security methods often lack the adaptability to support the dynamic nature of modern application environments, especially in cloud	No Change
82	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF C.Solution Capabilites Pont #5	The solution must support and integrate the web application vulnurability tools (Web application scanners) being proposed by bidder as part of this RFP at minimum to virtually patch web application vulnurabilies or else solution should have ready plug-ins to integrate banks VAPT tool.		Requesting you to modify the clause as below: The solution must support and integrate the web application vulnurability tools (Web application scanners) being proposed by bidder as part of this RFP, solution should have ready plug-ins to integrate banks VAPT tool.	Solution should be capable to protect against zero-day vulnerability using positive security model without being dependent on virtual patching. Virtual patch can even lead to false positive.	No Change

83	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #2	Appliance/Chassis based Hardware should support scalability with license upgrade. -18 vCPU from day 1 | Scalable to 32 vCPU -128 GB DDR RAM from day 1 -1 TB X 1 SSD M.2 SSD (in Raid) from Day 1		The clause represents single OEM offering for sizing		No Change
84	NA	7/B.Hardware & InAppendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #7	The proposed appliance shoulde provide minimum 1.2 Gbps of real world WAF throughput from day 1 and should be scalable to 2.2 Gbps with license upgrade on the same hardware or additional blades in case of a chassis based solution. The WAF throughput mentioned should be inclusive after enabling the below mentioned features: With all WAF functions enabled per intance in blocking mode SSL inspection.		The clause represents single OEM offering for sizing		No Change
85	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #8	The appliance should support the layer 7 throughput should be at least 58 Gbps scalable to 92 Gbps on same hardware with license upgrade. (Data rerernces for above should be verified from publicly available datasheet)		The clause represents single OEM offering for sizing		No Change
86	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #9	The proposed appliance must have minimum hardware compression of 34 Gbps for HTTP traffic form day 1 and scalable upto 48 Gbps with add on license on same hardware. (Data rerernces for above should be verified from publicly available datasheet)		The clause represents single OEM offering for sizing		No Change
87	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #10	The proposed appliance should support minimum hardware based SSL offloading from day 1 up to : 34 Gbps Scalable upto 48 Gbps on same hardware with license upgrade. (The SSL encryption & decryption process must be hardware-based proccessor for acceleration) (Data rerernces for above should be verified from publicly available datasheet)		The clause represents single OEM offering for sizing		No Change

88	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #11	The solution must support minimum SSL TPS/CPS: -29 K ECDSA P-256-bit keys from day 1 -58 K RSA 2048-bit keys from day 1 scalable to minimum SSL TPS/CPS -68 K ECDSA P-256-bit keys -98 K of RSA 2048-bit Keys (Data rerernces for above should be verified from publicly available datasheet with SSL)	The clause represents single OEM offering for sizing		No Change
89	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #12	The proposed appliance should support minimum 74 million L4 concurrent connections from day one and scalable upto 99 Million on same hardware with license upgrade.	The clause represents single OEM offering for sizing		No Change
90	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #13	The proposed appliance should support minimum 2.4 million L7 requests per seconds from day 1 and scalable upto 4.2 Million on same hardware with with license upgrade.	The clause represents single OEM offering for sizing		No Change
91	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF General Requirement Point #13	The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide traffic performance statistics for last 30 days including Active Connections, Active Sessions, CPU Usage By Core, HTTP Requests, Memory Used, RAM Cache Utilization, Rewrite Transaction, Data Rewrite Transactions, SSL Transactions, Throughput(bits), Throughput(packets), & Total New Connections	The clause should mention the functionality should be achieved without being dependent on tools.	The clause represents single OEM offering.	No Change
92	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #14	The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide a security event timeline dashboard where critical events like Audit logs, Pool status change, Failover status change, DOS attacks etc. must be shown for ease of troubleshooting with last 20 Failed logins details	The clause should mention the functionality should be achieved without being dependent on tools.	The clause represents single OEM offering.	No Change
93	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #15	The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide a Bug tracker option, where an admin can login and find any bugs affecting the devices	The clause should mention the functionality should be achieved without being dependent on tools.	The clause represents single OEM offering.	No Change

94	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF B.Hardware & Interfaces requirement Point #16	The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide an upgrade Options suggestions for next hotfix and stability release for ease of day-2 operations with single click access to release notes a nd EOS dates		The clause should mention the functionality should be achieved without being dependent on tools.	The clause represents single OEM offering.	No Change
95	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF B.Hardware & Interfaces requirement Point #17	The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide an ability to execute CLI commands which are essential for diagnostics which will show historic data or data at the time of file captured. E.g show history of all executed commands on the CLI		Request you to remove this clause	Database Load Balancer is provided as inbuilt feature from database solution provider and hence not needed from SLB solution	No Change
96	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF C.Solution Capabilities Point #23	Solution should have the capability to highlight (In red / any color code) only malicious payload from the entire attack payload on the event analysis dashboard for detailed fornsics analysis. This is extermly critical when our incident response teams are in combat with the attackers during wartime. This feature/functionality has to be live demonstrated by the bidder after the prebid query meeting, by setting up a lab in the cloud/on-premises		Forensics are not required for LB or WAF kind of solution. This is required for DDoS kind of solution and it is not recommended to have DDoS solution within WAF+LB as DDoS should be a stateless technology and it's placement should be at perimeter level above firewall to protect complete infrastruture		No Change
97	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF C.Solution Capabilities Point #36	The Proposed WAF Solution should provide built-in L7 layer DDoS detection and mitigation features based on machine learning and behavioral analytics and dynamic signatures. It should have CAPTCHA support or other mechanism to avoid distributed attack. This feature/functionality has to be live demonstrated by the bidder after the prebid query meeting, by setting up a lab in the cloud/on-premises		Request to remove this point	DDoS should be a stateless device and it's placement should be at perimeter level above firewall. This ensures protection to network from any advanced DDoS attacks. Hence, it should not be expected to be part of other security solutions within the network.	No Change

| 98 | NA | Appendix02 Techno Functional Requirements- Network components > LB+WAF C.Solution Capabilities Point #58 | The Solution should have IPSEC tunneling capabiltiies | | Request to remove this point | VPN is recommended to be a dedicated solution since it relies on TLS protocol. It is also recommended to terminate the traffic on Firewall or before Firewall as it will check for security parameters on the same.

If this is done on ADC, there won't be any security check and can possess threat or security flaw. | No Change |
|---|---|---|---|---|---|---|---|
| 99 | NA | Appendix02 Techno Functional Requirements- Network components > LB+WAF C.Solution Capabilities Point #59 | The proposed solution should support a comprehensive list of ways in which LB can monitor the backend services including Daimeter, DNS, FTP, Gateway ICMP, HTTP, HTTPS, TCP half open, TCP , LDAP, MSSQL, MYSQL, MQTT , POSTGRESQL, POP3 , IMAP, NNTP, Radius , SIP and custom external scripts | | Request to modify the clause as below:

The proposed solution should support a comprehensive list of ways in which LB can monitor the backend services including DNS, FTP, Gateway ICMP, HTTP, HTTPS, TCP half open, TCP , LDAP, MSSQL, MYSQL , POSTGRESQL, POP3 , IMAP, NNTP, Radius and custom external scripts | SIP, Diameter & MQTT Traffic are used in Service Provider environment and are not relevant and used in any Enterprise environment like BOB Cards. | No Change |
| 100 | NA | Appendix02 Techno Functional Requirements- Network components > LB+WAF C.Solution Capabilities Point #61 | The proposed solution should support various types of LB config for handling traffic, including standard reverse proxy, forwarding in L2 , Forwarding in IP, High performance mode, Stateless mode , Reject mode, DHCP relay, and Message routing for SIP, Daimeter and MQTT traffic | | Request this clause be modified as below:

The proposed solution should support various types of LB config for handling traffic, including standard reverse proxy, forwarding in L2 , Forwarding in IP, High performance mode, Stateless mode , Reject mode, DHCP relay | SIP, Diameter & MQTT Traffic are used in Service Provider environment and are not relevant and used in any Enterprise environment like BOB Cards. | No Change |
| 101 | NA | Appendix02 Techno Functional Requirements- Network components > LB+WAF C.Solution Capabilities Point #70 | The proposed solution should support native integration with kubernetes based platforms hosting microservices e.g. Openshift, TKG cluster etc. Solution should update the configuration of LB automatically by observing events within kubernetes clusters form day 1 without add on license. | | Solution should be able to support by means of same solution. | | No Change |
| 102 | NA | Appendix02 Techno Functional Requirements- Network components > LB+WAF C.Solution Capabilities Point #81 | The proposed LB solution should also support secure remote access to admin users (concurrency of not more than 10); where the solution can do endpoint checks for the admins and establist a secure tunnel with autentication against AD/OAUTH/Radius and MFA via Google authenticator. The system should allow per user basis a login schedule ?(e.g night shift employee cannot login during working hours) | | The clause represents single OEM offering. | | No Change |

103	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF D.Availability #2	The solution should support SQL-based querying for the following databases for the health checks: for Oracle, MSSQL, MySQL, PostgresSQL and other databases if required in future.		Request this clause be removed	Database Load Balancer is provided as inbuilt feature from database solution provider and this is proprietary load balancing feature of Database solution provider and hence not needed from ADC solution.	No Change
104	NA	Appendix02 Techno Functional Requirements-Network components > perimeter FW Specifications Point #7	The Firewall appliance should have certifications like ICSA /EAL4/CCNDPP		Request this be modified as below: The Firewall solution should have certifications like ICSA /EAL4/CCNDPP	Every OEM has its own solution offering and certification ask may align to the approach solution is provided rather than mandating it on the appliance inline to a particular OEM	No Change
105	NA	Appendix02 Techno Functional Requirements-Network components > perimeter FW Specifications Point #9	OEM/Bidder should provide below transceivers from Day-1. Firewall and SFP should be from same OEM. Below mentioned SFP quantity is required per appliance. 4 X 10GE SR SFP+ 4 X 1G SFP 4 x 25G SFP28		OEM/Bidder should provide below transceivers from Day-1. Firewall and SFP should be from same OEM. Below mentioned SFP quantity is required per appliance. 4 X 1G RJ 45 4 X 10G SFP+ 4 x 25G SFP28	Requesting if 1G can be considered using Copper Links and not SFP	No Change
106	NA	Appendix02 Techno Functional Requirements-Network components > perimeter FW Specifications Point #15	Solution should have minimum 450 GB SSD pair, system storage		Request to modify this as below Solution should have minimum 900 GB SSD pair, system storage	Perimeter Firewall needs high storage numbers as visible with mid/large scale deployments for storing logs considering 3/6 months retention in case the remote Management device is impacted , so good to ask for more	No Change, additional feature will consider as value add
107	NA	Appendix02 Techno Functional Requirements-Network components > perimeter FW Specifications Point #16	Solution should have minimum 32 GB		Request clause to be modifiedL Solution should have minimum 128 GB RAM	Perimeter Firewall has to have good RAM and such baselining will help with operations of critical banking infra	No Change, additional feature will consider as value add

108	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #19	"The proposed firewall must provide minimum 10 Gbps of Threat prevention throughput with Real world traffic. (Throughput must be derived from Appmix traffic and not Video/JPEG based traffic) (enterprise testing condition). The throughput must remain 10 Gbps even after enabling NGFW + IPS/IDS + Antivirus + Anti Spyware + Anti Bot + DoS/DDOS + All signature enabled + Logging enabled + Bidirectional inspection + File Blocking. OEM to provide publicly available The Test methodology and result should be compliant to the benchmark testing methodology for the above parameters provided in the Internet Engineering Task Force (IETF)- 'Benchmarking Methodology for		Request below modified clause be considered , instead of Appmix traffic , real world traffic should be mentioned for deriving throughput "The proposed firewall must provide minimum 10 Gbps of Threat prevention throughput with Real world traffic. (Throughput must be derived from real world traffic and not Video/JPEG based traffic) (enterprise testing condition). The throughput must remain 10 Gbps even after enabling NGFW + IPS/IDS + Antivirus + Anti Spyware + Anti Bot + DoS/DDOS + All signature enabled + Logging enabled + Bidirectional inspection + File Blocking. OEM to provide publicly available The Test methodology and result should be compliant to the benchmark testing methodology for the above parameters provided in the Internet Engineering Task Force (IETF)- 'Benchmarking Methodology for Network Security Device	instead of appmix traffic real world traffic will be rifht measure of throuhgput , so requesting the change	No Change
109	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #21	NGFW appliance must be capable of handling minimum 2 M concurrent sessions utilizing HTTP transactions with all Security feature Turned ON and not based on UDP / Lab environment / ideal testing environment, this claim has to be supported with declaration of concurrent connections claim from OEM		Request below modified clause to accomodate support for 5M concurrent sessions NGFW appliance must be capable of handling minimum 5 M concurrent sessions utilizing HTTP transactions with all Security feature Turned ON and not based on UDP / Lab environment / ideal testing environment, this claim has to be supported with declaration of concurrent connections claim from OEM	Mid/Large scale deployments need higher concurrent session support and baselining this to 50 Lakh concurrent sessions will be in the interest of the Bank , so the requested change	No Change, additional feature will consider as value add
110	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #49	Solution should support creation of minimum 1 virtual context / instance from Day-1 without any compromise on system performance and network bandwidth.		Solution should support creation of minimum 5 virtual context /instance from Day-1 without any compromise on system performance and network bandwidth.	Support for only 1 Virtual context may not be scalable for the DC design and min support for 5 instances is the need for any DC infra Perimeter Firewall understanding furture state architecure and growing needs.	No Change, additional feature will consider as value add

111	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #54	The proposed NGFW solution architecture should have Control Plane separated from the Data Plane in the Firewall appliance architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup, QoS, NAT etc). Control plane must have dedicated resources such as CPU, RAM etc. This is to ensure Bank always has management access to NGFW irrespective of Firewall load / Traffic Spike / Cyber Attack driving higher CPU utilization. Bank should able to login to the firewall and carry out reporting /		Request below modified clause be considered

The proposed NGFW solution architecture should have Control Plane separated from the Data Plane in the Firewall solution architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup, QoS, NAT etc). Control plane must have dedicated resources such as CPU, RAM etc. This is to ensure Bank always has management access to NGFW irrespective of Firewall load / Traffic Spike / Cyber Attack driving higher CPU utilization. Bank should able to login to the firewall and carry out reporting / management / packet capture etc to identify the root cause and accordingly take necessary action to remediate it. | OEMs have different approaches to achieving the use case and instead of the ask on the appliance itself , the Firewall Solution will be a generic term to use in requirements so this suggestion | No Change |
| 112 | NA | Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #72 | IPS should provide detailed information on each protection, including: Vulnerability and threat descriptions, Threat severity, Performance impact, Release date, Industry Reference, Confidence level etc. | | Request below changed clause :

IPS should provide detailed information on each protection, including: Vulnerability and threat descriptions, Threat severity, Release date, etc | Performance impact, industry reference and confidence level are subject to configuration and infrastructure in the bank. | No Change |
| 113 | NA | Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #76 | Should have more than 60+ predefined Categories based on Urls, Application types, Security Risk level etc. However solution should be able to create custom categories for URL and application. | | Request below modified clause with increased number of categories:

Should have more than 80+ predefined Categories based on Urls, Application types, Security Risk level etc. However solution should be able to create custom categories for URL and application. | Having more predefined categories support would help bank with improved threat detection and better granular policy control with less manual effort. | No Change, additional feature will consider as value add |
| 114 | NA | Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #89 | Solution should give information related to Performance impact and confidence level of protections while creating profiles. | | Request this clause be deleted | performance can be subject to policy configurations and existing infra at bank. | No Change |

115	NA	Appendix02 Techno Functional Requirements-Network components > perimeter FW Specifications Point #114	"Management server should support the following for rule optimization: • Unused Rules Calculation for specific time-period based on Firewall Traffic Logs. • Analysis on Covered/Shadow/Hidden Rules • Analysis on Rules Consolidation (Merging of similar kind of rules) • Analysis on Redundant Rules • Tightening of Overly Permissive Rules (Any-Any) • Analysis on Unattached/Unused Objects to simplify objects management • Analysis on Rule-Reordering to improve the performance of the Firewall • Analysis on Disabled/Expired Rules for enhanced visibility on the Firewall Rules sets"		"Management server should support the following for rule optimization: • Unused Rules Calculation for specific time-period based on Firewall Traffic Logs / HIt count • Analysis on Covered/Shadow/Hidden Rules • Analysis on Redundant Rules • Analysis on Unattached/Unused Objects to simplify objects management • Analysis on Disabled/Expired Rules for enhanced visibility on the Firewall Rules sets"	OEMs could be handling the use case suggested for removal differently or have no dependency on the performance of the Firewall , so requesting these be removed from the ask	No Change
116	NA	Appendix02 Techno Functional Requirements-Network components > IPS Features Point #15	Should support more than 3000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness		Should support more than 5000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness	Increasing number of signature support is beneficial for the Bank's operations and for Effective Security reasons	No Change
117	NA	Appendix02 Techno Functional Requirements-Network components > internal FW Point #11	The Firewall solution Should support more than 4000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness and should be able to create 40 or more application categories for operational efficiency. Dedicated IPS solution shall be in corporated by the bidder to achive this scale of IPS AVC signatures in this solution.		Request this clause be modfied as below: The Firewall solution Should support more than 6000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness and should be able to create 40 or more application categories for operational efficiency. Dedicated IPS solution shall be in corporated by the bidder to achive this scale of IPS AVC signatures in this solution.	Increasing number of signature support is Beneficial for the Bank's operations and for Effective Security reasons	No Change, additional feature will consider as value add
118	NA	Appendix02 Techno Functional Requirements-Network components > internal FW NG Firewall Features NEW POINT	New Point to be added		The solution should provide Change Management capability for the organizations needs to implement more formal processes for configuration changes, including audit tracking and official approval before changes are deployed.	By leveraging these features and integrating with external change management tools, organizations can implement a robust change management process that includes formal approval, audit tracking, and compliance reporting within Cisco FMC.	No Change

#							
		Features NEW POINT			The solution should provide traffic hit count, Rule Conflict Detection (Redundant & Shadowed) and policy warning for streamlining firewall policies.	These features are crucial for optimizing firewall policies, ensuring efficient traffic flow, and maintaining security posture.	No Change, additional feature will be consider as value add
119	NA						
120	NA	Appendix02 Techno Functional Requirements-Network components > internal FW Hardware Architecture Point #3	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 8x64 GB of RAM.		Request below modified clause be considered as correction on the ask which seems typo:\n\nThe 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.		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.
121	NA	Appendix02 Techno Functional Requirements-Network components > Mngmt Switch 6 Product Support Point #2	The OEM support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support		Request below modified clause be considered\n\nThe OEM/OEM certified partner support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support	OEM Certified partner has thorough experience of OS version upgrades and maintaining network operations troubleshooting issues and it will be cost effective to include this in the ask	The OEM/OEM certified partner support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support
122	NA	Appendix02 Techno Functional Requirements-Network components > Mngmt Switch 9 Miscellaneous Points Point #1	Console cable and power cable (As per Indian standards) as per customer requirement to be provided. All Cables shall be factory-terminated.		Since Console Cables are common for all devices per OEM , Request Bank to clarify the count of console cables to be provided , is it one each with each Switch or one per DC and DR Each ?.		No Change
123	NA	Appendix02 Techno Functional Requirements-Network components > Mngmt Switch 10 Product Support Point #2	The OEM support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support		Request below modified clause be considered\n\nThe OEM/OEM certified partner support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support	OEM Certified partner has thorough experience of OS version upgrades and maintaining network operations troubleshooting issues and it will be cost effective to include this in the ask	The OEM/OEM certified partner support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support
124	NA	Appendix02 Techno Functional Requirements-Network components > Core Swtich >9 Manageability > Appliance point 9.4	Switch Anomolies related with Advisories , PSIRT and Field Notices		Request this clause be removed from the telemetry asks	This feature is not requireed for the design at the BOB DataCenter and may be removed	No Change
125	NA	Appendix02 Techno Functional Requirements-Network components > Core Swtich >13 Fabric Management > Appliance point 13.1	Solution must provide Centralized Management Appliance – Single pane of glass for managing, monitoring and provisioning the entire Solution within Data Center & across all Data Centers		Request BOBCards to provide VM compute resources for spinning up the VMs to provide this functionality while we can provide the necessary sw and support.		Requested product functionality should be comply, BOBCards will provide VM compute resources for spinning up the VMs to provide this functionality however bidder should provide the necessary sw and support.
126	NA	Appendix02 Techno Functional Requirements-Network components > Core Swtich >5 Layer 2 Features > Appliance point 5.11	Switch Hardware should have capability to support BGP EVPN Route Type 1, Type 2, Type 3, Type 4, Route Type 5, Type 6/Type 7/Equivalent routes		Request this point be removed	BOBCards design doesn't have Fabric so this is not applicable	No Change

#	Page	Section	Clause		Query/Request	Justification	Response
127	NA	Appendix02 Techno Functional Requirements- Network components > Core Swtich >13 Fabric Management > Appliance point 13.36	Solution should provides reports using predefined templates, including inventory, use, and health reports.		Request below modified clause be considered: Solution should provides reports including inventory, use, and health reports.		No Change
128	NA	Annexure 02 Technical Evaluation Criteria Sr. No. 1	The bidder should have supplied and installed similar to proposed hardware in last three (3) financial years, i.e. 2021-2022, 2022-23, 2023-24 (Bidder to provide details in Annexure K and submit PO / Contract details)		Request you to remove "similar to Proposed hardware" from current Clause.	This change will allow more bidders to participate and bid will be more competitive.	The bidder should have supplied and installed proposed OEM hardware in last three (3) financial years, i.e. 2021-2022, 2022-23, 2023-24 (Bidder to provide details in Annexure K and submit PO / Contract details) yes we can consider separate PO.
129	NA	Annexure 02 Technical Evaluation Criteria Sr. No. 2	The bidder should have deployed and configured proposed software as per OEM standard on proposed hardware in last three (3) financial years, i.e. 2021-2022, 2022-23, 2023-24 (Bidder to provide details / submit PO / Contract details)		Request you to remove "Proposed hardware" from current Clause.	This change will allow more bidders to participate and bid will be more competitive.	The bidder should have deployed and configured proposed software as per OEM certified and standard hardware in last three (3) financial years, i.e. 2021-2022, 2022-23, 2023-24 (Bidder to provide details / submit PO / Contract details)
130	Pg.No-8	2. Requirements Summary 2.1 Intent	• The successful bidder will be expected to provide all the components mentioned in the RFP along with required necessary tools, hardware and software licenses to implement as complete cloud platform solution to run VMs on this setup. Provide training for all proposed Hardware and Software to BOBCARD IT Team and handover the solution.		Please change the clause to Bidder/OEM for providing components mentioned in the RFP along with required necessary tools, hardware and software licenses to implement as complete cloud platform solution to run VMs on this setup. Provide training for all proposed Hardware and Software to BOBCARD IT Team and handover the solution.	Please change the clause to Bidder/OEM for providing components mentioned in the RFP along with required necessary tools, hardware and software licenses to implement as complete cloud platform solution to run VMs on this setup. Provide training for all proposed Hardware and Software to BOBCARD IT Team and handover the solution.	• The successful bidder/OEM will be expected to provide all the components mentioned in the RFP along with required necessary tools, hardware and software licenses to implement as complete cloud platform solution to run VMs on this setup. Provide training for all proposed Hardware and Software to BOBCARD IT Team and handover the solution. How ever Bidder will be accountable & responsible for entire project and single point of contact for BOBCARD. PO will name of Bidder only.
131	11	3.1 Project Scope Point #1	The supplied Hardware and Software shall be of the latest versions and should not be end of life / end of support for the next 7 years.		Request the start Date for 7 Yrs mention in the clause be specified. Is it RFP Date or Date of PO Issuance/GoLive Date or something else?	Right tenure will help align the final BOM and any discrepent inpurs will impact pricing , so requesting clarification	The supplied Hardware and Software shall be of the latest versions and should not be end of life / end of support for the next 5 years from the date of delivery
132	12	3.1 Project Scope Point #4	All Software licenses effective date shall be effective as on Go-LIVE sign off or put in use for BOBCARD operations.		Contract Start period is mentioned as PO Issuance while the SW licenses effective date is mentioed as GoLive Sign off Dates as noticed. Request Bank to keep this synchronized if this is genuine or clarify the intent	Right tenure will help align the final BOM and any discrepent inpurs will impact pricing , so requesting clarification	License effectiveness should be start from the software is ready to use. License cost will not impact to BOBCARD due to implementation delay. No license activate without informing BOBCARD.
133	12	3.1 Project Scope Point #12	Hardware RMA (Return Merchandise Authorization) should be within 24 hours		Request this be modified as below Hardware RMA (Return Merchandise Authorization) should be within 24 hours on Next business Day Basis.	RMA for a request raised on Friday may be honored by Monday due to the wekend in between , so requesting to keep this clearly specified.	Hardware RMA (Return Merchandise Authorization) should be within 24 hours on Next business Day Basis.

#	No.	Clause Reference	Clause Text		Query / Clarification	Justification	Response
134	19	5.3 Price Comparisons Point #c iv	End of Sales/ End of support: The Vendor has to ensure that any application, related software supplied / put to use as part of this RFP should not have reached end of support. In the event if any equipment supplied / put to use by the vendor reaches end of support, within the contract period from the date of use, the vendor has to replace the equipment/ software at no additional cost to the Company before end of support.		End of Life/End of Sale Clause here should specifiy the start date as to if PO issuance, RFP Date or any other . Further the tenure within which EOS/EOL should not happen must be mentioned like 7 years in clause Project Scope point #1	Right tenure will help align the final BOM and any discrepent inpurs will impact pricing , so requesting clarification	The supplied Hardware and Software shall be of the latest versions and should not be end of life / end of support for the next 5 years from the date of delivery
135	9	2.2 Tenure	The tenure of the contract initially would be for 1 year from the date of the issuance of first purchase order. BOBCARD can further extend to 2 years at its at mutually agreed terms.		Contract Tenure mentioend as 1 Year from PO Issuance here while its 3 years in clause 3.1 Point 17/ Pls clarify the right tenure?	Right tenure will help align the final BOM and any discrepent inpurs will impact pricing , so requesting clarification	Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
136	13	3.1 Project Scope Point #17	The initial term of this contract shall be 3 years and may be extended to another 2 years subject to satisfactory performance by successful bidder and OEM(s).		Mentioned here is 3 years of initial contract and in 2.2 section the contract mentioned is 1 Year/ pls clarify the right tenure	Right tenure will help align the final BOM and any discrepent inpurs will impact pricing , so requesting clarification	Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
137	30	7.2 Evaluation Methodology for Eligible Bidder Commercial Bid Evaluation	The key considerations of the TCO would be the total payouts for entire project through the contract period of 5 years.		Mentioned here is 5 years contract but in 2.2 the tenure of contrat is 1 Year, pls clarify the number to consider	Right tenure will help align the final BOM and any discrepent inpurs will impact pricing , so requesting clarification	Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
138	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Server Prod > HCI Rack Servers > 1	Total QTY is 14		Clarifictaion Needed: 1. Please provide split of quantity of servers / Nodes per location. 2. Kindly specify the number of clusters and nodes per cluster also.	clarifiction will help arrive at the boq rightly	This will be shared with only elected bidder
139	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Server Prod > HCI Rack Servers > 7	Each Rack Server Controller Cards / Controller Drive should be provided in HA mode in RAID -1.		Request Change: Each HCI Server should be configured with two BOOT drives with hardware RAID Controller. For NVMe storage drives: Provides as per Certifed HCI Node with NVMe configuration	From the HCI Rack server or Pre configured HCI NODE - RAID Controller card is not required for NVMe drives. Also, is this ask for Boot drive with RAID Controller?	Yes, we need boot drive for HCI hypervisor provided in HA mode in RAID -1
140	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Server UAT > HCI Rack Servers > 7	Each Rack Server Controller Cards / Controller Drive should be provided in HA mode in RAID -1.		Request Change: Each HCI Server should be configured with two BOOT drives with hardware RAID Controller. For NVMe storage drives: Provides as per Certifed HCI Node with NVMe configuration	From the HCI Rack server or Pre configured HCI NODE - RAID Controller card is not required for NVMe drives. Also, is this ask for Boot drive with RAID Controller?	Yes, we need boot drive for HCI hypervisor provided in HA mode in RAID -1

141	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Server Prod > HCI Rack Servers > 6	Each Rack servers should have minimum usable Storage Capacity of 10 TB of all caching SSD and other HDD. 20% disk slot on each node should be free for future expansion		Clarification needed: In virtualized environment, the storage (usable) capacity is calcluated across the cluster. Need clarification on the total capacity required across the number of nodes in a cluster.	clarifiction will help arrive at the boq rightly	as mentioned in RFP 10TB usable storage per node * no of node = total usable capacity
142	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Server UAT > HCI Rack Servers > 6	Each Rack servers should have minimum usable Storage Capacity of 10 TB of all caching SSD and other HDD. 20% disk slot on each node should be free for future expansion		Clarification needed: In virtualized environment, the storage (usable) capacity is calcluated across the cluster. Need clarification on the total capacity required across the number of nodes in a cluster.	clarifiction will help arrive at the boq rightly	as mentioned in RFP 10TB usable storage per node * no of node = total usable capacity
143	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Server Prod > HCI Rack Servers > 13 >Server Security	Request New Point to be added		Request to add the below point for security and management features for HCI Nodes Day2 operations and management of HCI Nodes for updates on Hardware and Software. HCI Node management tool should integrate with Virtual platform and Network switches. Should be able to do Firmware updates, Manage Cluster and deployment, Full stack visibility of HCI Node, TAC/Case Support, Continuous Health checks on Networking, Server, VMs , Anomalies detection, Security advisories, patch management etc.	HCI Node should integrate with Virtual platform and Network switches, Should have management software for a Firmware update, Manage Cluster and deployment, Full stack visibility HCI Node, TAC/Case Support, Continuous Health checks on Networking, Server, VMs , Anomalies detection, Security advisories, patch management,	No Change, additional feature will be consider as value add
144	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Server UAT > HCI Rack Servers > 13> Server Security	Request New Point to be added		Request to add the below point for security and management features for HCI Nodes Day2 operations and management of HCI Nodes for updates on Hardware and Software. HCI Node management tool should integrate with Virtual platform and Network switches. Should be able to do Firmware updates, Manage Cluster and deployment, Full stack visibility of HCI Node, TAC/Case Support, Continuous Health checks on Networking, Server, VMs , Anomalies detection, Security advisories, patch management etc.	HCI Node should integrate with Virtual platform and Network switches, Should have management software for a Firmware update, Manage Cluster and deployment, Full stack visibility HCI Node, TAC/Case Support, Continuous Health checks on Networking, Server, VMs , Anomalies detection, Security advisories, patch management,	No Change, additional feature will be consider as value add
145	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmentation > 1	The Solution should be capable of supporting major hardware OEMs like Juniper, Arista, Cisco, HPE and Dell. The proposed solution should be a purely software-based solution and should not be dependent on any hardware make and model.		Request below modified clause be considered: The Solution should be capable of supporting major hardware OEMs like Juniper, Arista, Cisco, HPE and Dell. The proposed solution should be a purely software-based solution and should not be dependent on any hardware make and model by creating overlay tunnels between the hosts.	The key benefits of no dependecy on hardware is by using software defined networking i.e overlay. Overlay is mandatory for network & Security automation as part of software defined data center.	No Change

146	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmentation > 2	The solution should provide a distributed firewall such that the firewalling for Virtual Machines can be provided closest to the application within the server itself without traffic going to a Physical Firewall.		Request below modified clause be considered which includes additonal points The solution should provide a distributed firewall such that the application aware and identity based statefull firewalling for Virtual Machines can be provided closest to the application within the server itself without traffic going to a Physical Firewall or regardless of underlying L2 Netwrork topology. The solution should also provide an integrated networking solution (CNI implementations) as well as provide advance turnkey container networking & firewalling services. Solution should support for container networking plug-ins, support for pod to pod communication and support for ingress controllers. The micro-segmentation solution should have a capability for stateful firewalling and ALGs (Application Level Gateway) on a per-workload granularity regardless of the underlying L2 network topology (i.e. possible on either logical network overlays or underlying VLANs), embedded in the hypervisor kernel, distributed	*As per security framework its recommended not to use standard ports for your applications and hence to have effective security on per VM basis an application/L7 firewalling is must.* Containers & Kubernetes are now part of all modern applications hence networing and security for container shall also be considered for end to end application security. there is App ID requirement is mentioned in RFP as part of "Internal Firewall" spec point # 23 hence same should be considered for mirosegmenation as well otherwise it will create non standard architecture.	No Change
147	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmenation >5	The proposed solution should provide the ability to define firewall rules at VM level for east-west traffic in order to implement Zero Trust Security		Request below modified clause be considered: The proposed solution should provide the ability to define Layer 7 application firewall rules at VM level for east-west traffic in order to implement Zero Trust Security alongwith URL Filtering and TLS inspection for encrypted traffic	Zero trust Security framework mandates TLS inspection for encrypted traffic, URL Filtering and Layer 7 application firewalling.	No Change, additional feature will be consider as value add
148	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmenation >4	The Proposed Solution including Hypervisor, SDS and Micro segmentation must be from the same OEM.		Request below modified clause be consideredL The Proposed Solution including Hypervisor, SDS, SDN and Micro segmentation must be from the same OEM.	SDN is missing in the spec, SDN will be mandatory to create complete automated Software Defined data center by creating an abstraction of the network enabling programming of network behavior in a centrally controlled manner through software applications.	No Change, SDN will be consider as value add

149	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmenation >6	The proposed solution should allow users to define granular firewall rules based on IP Addresses, Tags/Categories and Subnets to segment User Applications		Request below modified clause be considered which includes additonal points

The proposed solution should allow users to define granular firewall rules for both VM and conatiners based on IP Addresses, VM Names, Tags/Categories and Subnets to segment User Applications by creating dynamic security groups. The solution should have capability to provide stateful micro-segmentation for virtual machines and Kubernetes workloads from a single console.
The solution should also support enforcement of stateful distributed firewall for IPv6 VM workloads. These firewall rules can use IPv6 addresses, IPv6 CIDR, IP Sets that include both IPv4 and IPv6 addresses and security groups that can include logical ports that have both IPv4 and IPv6 addresses. IPv6 capability should be available both at management and data plane | Its necessary to have dynamic security group capability to ensure complete automation. Mentioned in the RFP page 8 -> 2.0 --> Requirement Summary--> 2.1 Intent--> mentions requirement for IPv6 "The proposed solution should support both IPv4 and IPv6." | No Change |
| 150 | NA | Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmenation >7 | Solution should provide capability to create network segments by defining them entirely in software and avoid the need to re-architect your network or deploy physical appliances | | Request below modified clause be accmodated:

Solution should provide capability to create network segments and L2 Streching between DC and DR by defining them entirely in software and avoid the need to re-architect your network or deploy physical appliances | L2 Streching is required for better application availability considering RFP asks for 99.99 % availability on monthly basis.
RFP Page 17 -> "4. Service Levels "-->"SLA: The solution is expected to be available for 99.99% on 24x7 and up time availability will be calculated on monthly basis." | No Change, L2 stretching implementation will be discuss with elected bidder. |
| 151 | NA | Appendix01 Techno Functional Requirements- Server and Virtual platform > Container >2 | The solution must be able to manage Kubernetes clusters. Licenses for managing Kubernetes clusters should be implemented from Day-1 | | Request below modified clause be accmodated:

The solution must be able to manage Kubernetes clusters. Licenses for managing Kubernetes clusters along with components such as backup, container registry and monitoring alongwith Windows Container support should be implemented from Day-1 | Kubernetes Cluster doesn't work in isloation but require other components such as container registry and backup solution. If not included than Bob Card will have procure them separately. And Not aving Windows Container support will block any windows based apps to be deployed on Kubernetes Platform. | Yes, BOBCARD will take care such requirement |
| 152 | NA | Appendix02 Techno Functional Requirements- Network components > internal FW NG Firewall Features NEW POINT | Must have provisioning, operations and lifecycle management of Kubernetes, automated deployment, scaling, and operation of Kubernetes clusters | | Request below modified clause be accmodated:

Must have provisioning, operations and lifecycle management of Kubernetes, automated deployment, Auto scaling & Auto Healing, and operation of Kubernetes clusters | Complete Automation is not possible without Auto Scaling and Auto Healing of Kubernetes Clusters. One has to manually add nodes in case of failure or unprovisioned increase in load. | No Change |

153	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Container >4	Container Platform should provide single pane of Glass for Lifecycle Management of all K8S clusters deployed on prem.		Request below modified clause be accmodated: Container Platform should provide single pane of Glass for Lifecycle Management of all K8S clusters alongwith ingress, backup and container registry deployed on prem.	Kubernetes Cluster doesn't work in isloation but require other components such as container registry and backup solution. These shall too be considered for life cycle management	Yes, BOBCARD will take care such requirement
154	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Cloud Management >1	The solution should provide capability of generating reports for usage, performance, compliance, health, forecasting and capacity.		Request below modified clause be accmodated: The solution should provide capability of generating reports for health, Capacity Optmization - Right Sizing (Under sized, Oversized), Reclamation (Idle, Powered off , Snapshot, Orphaned Disk , Forecasting - Capacity Forecasting, Migration assessment, Migration Planning Usage - Process and service utlization Compliance - Regulatory Benchmark (PCIDSS and ISO) Security Guidelines for Infrastructure and Cloud Management	Bob Cards will need capacity optimization capabilities to identify over-provisioned & under-provisioned resources and provide recommendations, alerts and automated actions on right-sizing and resource consumption so they can be right-sized for adequate performance and avoid resource wastage. Should provide visibility of capacity and VMs which can be reclaimed and cost visibility of the reclaimed capacity and VMs.	No Change, additional feature will be consider as value add
155	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Cloud Management >11	The solution should have intelligent operations with anomaly detection which will allow monitoring seasonal trends and automatically send email alert		The solution should have AI/ML driven intelligent operations & troubleshooting workbench with anomaly detection,third party infra (Server, Storage , Network, database and Application) along with parent child relatiohship mapping, service and process monitoring which will allow monitoring seasonal trends and automatically send email alert. The solution should also have log management capability for infrastructure and applications . log management solution should delivers intuitive, actionable dashboards, sophisticated analytics, and broad third-party extensibility across physical, virtual, and cloud environments.	BoB Cards will not be able to manage the infrastructure without comprhesive log management capability. Its also mandatory for from regulation/compliance perspective to have log stored for given period of time for audit. BoB Card would need apps (database and Application) to infra (Server, Storage , Network) level visibility for toubleshooting and performance monitoring.	No Change, additional feature will be consider as value add
156	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Cloud Management >7	The solution must have an approval process to review, reject or approve the deployment requests from the marketplace.		Request below modified clause be considered: The Solution must support multiple levels of approval with E-mail notifications with ability to automate manual provisioning and de-provisioning of the tasks and policies embedded in each layer of their application including auto - approve and auto-reject capability based on application criticality	The solution must have an approval process to review, multi level & auto reject or approve the deployment requests from the marketplace.	No Change, additional feature will be consider as value add

157	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 6	Hypervisor should support container and opensource integration for cloud native application from day-1. Must be a Kubernetes ready from day-1.		Request below modified clause be accmodated: Hypervisor should support container both Linux and Windows along with other kubernetes ecosystems such as container registry, backup, ingress & monitoring and opensource integration for cloud native application from day-1. Must be a Kubernetes ready from day-1.	Kubernetes doesn't work in isolation and requires multiple components for production setup.	Yes, BOBCARD will take care such requirement
158	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 16	Virtualization Manager should provide feature which can perform quick, as-needed deployment of additional virtualized hosts. When the service is running, it can push out update images, eliminating patching and update without impacting production.		Please clarify the scenario and expected outcome out of the below point in this clause: "When the service is running, it can push out update images, eliminating patching and update without impacting production."		Virtualization manager should allow addition of new nodes and patching/upgrade of hypervisor running on the node without any VM downtime.
159	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 22	Unlimited VM replication from DC to DR (No restriction on VM replication and DR orchestration) with the capability to define Recovery Plans		Request to provide the number of VMs to be orchestrated for automated recovery and not keep open as unlimited since this approach is OEM specific . The VMs to be protected/orchestrated are limited to what can be provisioned on these 14 servers of production. Furehr pls clarify the need for Recovery Plans		No Change, can not predict the exact number of VMs for next 5 Years which need to be replicated.
160	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 23	Proposed solution should have a self-service restore feature on a per-VM basis to allow trusted application administrators to recover their own files with the ability to mount snapshots as a drive in Windows VMs		Request this be modified as below or clarify the requriement: Proposed solution should have a self-service restore feature on a per-VM basis to allow trusted application administrators to recover their own VMs from the snapshot	Please clarify this requirement, this looks like back and restore requirements so the modified clause	This will help BOBCARD to recover file without losing current state of virtual machine.
161	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 24	Hypervisor should provide Visibility for Running VM and their connectivity co-relationship with Network Ports on attached Physical TOR / Core Direct which Include Network RX/TX Bytes.		Request below modified clause with additional inputs be considered : Hypervisor should provide Visibility for Running VM and their connectivity co-relationship with Network Ports on attached Physical TOR / Core Direct which Include Network RX/TX Bytes.Solution Should provide end to end visibility across physical firewall, switch and storage, Flow Analysis and Security Planning,Guided Troubleshooting, Microsegmentation planning, RCA (Connectivity Problem, Packet Loss, N/W latency), Application Discovery, Service Monitoring , Application Dependency Mapping and monitoring of non compliant ports	Monitoring is not considering all components of the stack. Unless end to end visibility is provided as part of this solution BoB Card has to spend separately on monitoring.	Yes, BOBCARD will take care such requirement. However Hypervisor should provide Visibility for Running VM and their connectivity co-relationship with Network Ports on attached Physical Port which Include Network RX/TX Bytes.

162	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Hypervisor > 30	Virtualization software or the solution should provide Cluster level encryption protects unauthorized data access at-rest.		Request below modified clause be considered : Virtualization software or the solution should provide Cluster level, VM Level encryption protects unauthorized data access at-rest and in transit.	Having capability to do the enscryption at app VM level and in transit is required to complete solution.	No Change, additional feature will be consider as value add
163	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Software Defined Storage > 1	Maintain primary working set copy of active data on the Local Node as VM's are hosted to provide high IOPS and low latency. Proposed solution must be proposed for faster reads and write for Business-critical Apps.		Request below additional point be added in theis clause : Proposed solution must be proposed for faster reads and write for Business-critical Apps.	Architecture is specific to one vendor, request BoB Cards to consider on outcome than specific architecture. There is no specific latency requirements mentioned in the spec.	No Change.
164	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Software Defined Storage >2	The solution must have De-duplication and Compression features licensed and implemented from day one (Should not have dependency on any proprietary hardware device).		Request below modified clause be considered: The solution must have De-duplication/Compression features licensed and implemented from day one (Should not have dependency on any proprietary hardware device).	Solution should have flexibility to implement either compression and de-duplication. BoB Cards should conisder overhead while deciding on both.	No Change
165	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Software Defined Storage >24	The proposed solution should support 1 min RPO & 1 hour RTO for critical workload in case BOB Cards wants to have this capability replication for Future use. The proposed solution should have native Replication and DR Orchestration from Day-1		What is the use case for 1 min RPO and 1 Hour RTO? is this linked with some regulatory requirement?	Replication is best handled at application level as having additional solution for infrastructure will complexity and cost for BoB Cards Its best to use extends the existing DR orchestration solution for this environment as well.	This is required for BOBCARD mission critical application. The solution should capable to support 1min RPO. The propose replication solution should be same OEM as the virtualization solution to provide seamless integration.
166	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Software Defined Storage >25	The solution provided should function even after one node failure.		Request below modified clause be considered: The solution provided should function even after two node failure.	RFP asks for 99.99 % availability SLA for the proposed solution. It will require minimum N+2 configuration for required resiliency and uptime.	No Change, additional feature will be consider as value add
167	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Software Defined Storage >31	The solution should provide enterprise data services such as compression completely in software. Software Defined Storage solution must have de-duplication and compression features Licensed and implemented from day one. These functionalities should be part of the proposed solution. The solution must have functionality to support compression and or deduplication online on data container without any downtime and data loss as per business requirement.		Request below modified clause be considered: The solution should provide enterprise data services such as compression completely in software. Software Defined Storage solution must have de-duplication or compression features Licensed and implemented from day one. These functionalities should be part of the proposed solution. The solution must have functionality to support compression and or deduplication online on data container without any downtime and data loss as per business requirement.	Solution should have flexibility to implement either compression and de-duplication. BoB Cards should conisder overhead while deciding on both.	No Change

168	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmentation > new point	Additional Point for consideration		The solution must ensure that there is not alteration in the IP address of the Virtual machine, by blocking the traffic from or to the VM inherited as a feature in the Solution.	IP/MAC spoofing is major security concern for organizations like BoB Cards handing customers data.	No Change, additional feature will be consider as value add
169	NA				The solution should support multi-tenancy to isolate networking/security for different departments/function within BoB Cards upto a minimum of 4 tenants and 5 VPCs	VPC will enable Bob Cards to create isolation from access , resources, network and security.	ange, additional feature will be consider as valu
170	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Container > 6	Should support cluster scale out i.e addition of worker nodes as and when required.		Request below modified clause be considered: Should support Automated cluster scale out i.e addition of worker nodes as and when required.	Complete Automation is not possible without Auto Scaling and Auto Healing of Kubernetes Clusters. One has to manually add nodes in case of failure or unprovisioned increase in load.	No Change
171	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > 3	The solution shall provide a single pane of glass for automated provisioning with model-based orchestration of compute, network and storage through a unified multi-tenant self-service catalog.		Request below modified clause be consiered The solution shall provide a single pane of glass for automated provisioning with model-based orchestration of compute, network , storage and Kubernetes through a unified multi-tenant self-service catalog .	All modern applications are combination of both container and VM form factor.	No Change, additional feature will be consider as value add
172	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > 5	The solution must provide a self-service portal to allow user to consume the creation of infrastructure easily.		Request below modified clause be considered: The solution must provide a self-service portal to allow user to consume the creation of infrastructure easily for both VM and Kubernetes	All modern applications are combination of both container and VM form factor.	No Change, additional feature will be consider as value add
173	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > 8	The software must allow the designer to use shell script, PowerShell script to code the automation.		Request below modified clause be considered: The software must allow the designer to use shell script, PowerShell script, Python and node JS to code the automation.	Python and nodeJs are very popular language for scrpting in terms resource availability and community support	No Change, additional scripting will be value add
174	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > 9	The software must allow the designer to design VM blueprints.		Request below modified clause be considered: The software must allow the designer to design Multi VM & Kubernetes blueprints.	All modern applications are combination of both container and VM form factor.	No Change, additional feature will be consider as value add
175	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > 12	The solution should have simple low-code, no-code automation engine which allows automating day-to-day routine tasks		Request below modified clause and adidtoinal inpurs on the clause be considered: The solution should have simple low-code, no-code automation engine which allows automating day-to-day routine tasks such as Snapshot creation, Addition of Disk, Power Cycle (Suspend , Shutdown, Reboot, reset), Resize, Rebuild, Additional of Network, VM Unregister , Delete,connect remote console, Change Security Group with capability to create additional resource actions as out of the box capability.	All modern applications are combination of both container and VM form factor.	No Change, additional feature will be consider as value add

176	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Cloud Management > New Point	New Point		Solution should provide capability to define and showcase cost to create cloud like experience to the business unit with the overall cost spend on the infrastructure [server hardware, storage, licenses, application, maintenance, labor, network, facilities , etc.	Bob Cards will need Cost transparency (Showback and Chargeback capability) across private, hybrid to optimize planning and prioritization of VM/ Server/Application onboarding/provisioning	No Change, additional feature will be consider as value add
177	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF & IPS	New Point		We request BoB Card to allow for both software and hardware based solution for Load Balancer, WAF, IPS/IDS. As these components are dynamic as per application consumption requirements and considering bob card is directly managing customer data, its very critcal that these components are added as part of sofwate defined stack.	Modern applications increasingly require software-defined networking (SDN) and security solutions due to their need for greater flexibility, agility, and scalability. Traditional networking and security methods often lack the adaptability to support the dynamic nature of modern application environments, especially in cloud	No Change
178	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF C.Solution Capabilites Pont #5	The solution must support and integrate the web application vulnurability tools (Web application scanners) being proposed by bidder as part of this RFP at minimum to virtually patch web application vulnurabilies or else solution should have ready plug-ins to integrate banks VAPT tool.		Requesting you to modify the clause as below: The solution must support and integrate the web application vulnurability tools (Web application scanners) being proposed by bidder as part of this RFP, solution should have ready plug-ins to integrate banks VAPT tool.	Solution should be capable to protect against zero-day vulnerability using positive security model without being dependent on virtual patching. Virtual patch can even lead to false positive.	No Change
179	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF B.Hardware & Interfaces requirement Point #2	Appliance/Chassis based Hardware should support scalability with license upgrade. -18 vCPU from day 1	Scalable to 32 vCPU -128 GB DDR RAM from day 1 -1 TB X 1 SSD M.2 SSD (in Raid) from Day 1		The clause represents single OEM offering for sizing		No Change
180	NA	7/B.Hardware & InAppendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #7	The proposed appliance shoulde provide minimum 1.2 Gbps of real world WAF throughput from day 1 and should be scalable to 2.2 Gbps with license upgrade on the same hardware or additional blades in case of a chassis based solution. The WAF throughput mentioned should be inclusive after enabling the below mentioned features: With all WAF functions enabled per intance in blocking mode SSL inspection.		The clause represents single OEM offering for sizing		No Change
181	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF B.Hardware & Interfaces requirement Point #8	The appliance should support the layer 7 throughput should be at least 58 Gbps scalable to 92 Gbps on same hardware with license upgrade. (Data rerernces for above should be verified from publicly available datasheet)		The clause represents single OEM offering for sizing		No Change

182	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF B.Hardware & Interfaces requirement Point #9	The proposed appliance must have minimum hardware compression of 34 Gbps for HTTP traffic form day 1 and scalable upto 48 Gbps with add on license on same hardware. (Data rerernces for above should be verified from publicly available datasheet)		The clause represents single OEM offering for sizing		No Change
183	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF B.Hardware & Interfaces requirement Point #10	The proposed appliance should support minimum hardware based SSL offloading from day 1 up to : 34 Gbps Scalable upto 48 Gbps on same hardware with license upgrade. (The SSL encryption & decryption process must be hardware-based proccessor for acceleration) (Data rerernces for above should be verified from publicly available datasheet)		The clause represents single OEM offering for sizing		No Change
184	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF B.Hardware & Interfaces requirement Point #11	The solution must support minimum SSL TPS/CPS: -29 K ECDSA P-256-bit keys from day 1 -58 K RSA 2048-bit keys from day 1 scalable to minimum SSL TPS/CPS -68 K ECDSA P-256-bit keys -98 K of RSA 2048-bit Keys (Data rerernces for above should be verified from publicly available datasheet with SSL)		The clause represents single OEM offering for sizing		No Change
185	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF B.Hardware & Interfaces requirement Point #12	The proposed appliance should support minimum 74 million L4 concurrent connections from day one and scalable upto 99 Million on same hardware with license upgrade.		The clause represents single OEM offering for sizing		No Change
186	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF B.Hardware & Interfaces requirement Point #13	The proposed appliance should support minimum 2.4 million L7 requests per seconds from day 1 and scalable upto 4.2 Million on same hardware with with license upgrade.		The clause represents single OEM offering for sizing		No Change
187	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF General Requirement Point #13	The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide traffic performance statistics for last 30 days including Active Connections, Active Sessions, CPU Usage By Core, HTTP Requests, Memory Used, RAM Cache Utilization, Rewrite Transaction, Data Rewrite Transactions, SSL Transactions, Throughput(bits), Throughput(packets), & Total New Connections		The clause should mention the functionality should be achieved without being dependent on tools.	The clause represents single OEM offering.	No Change

188	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #14	The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide a security event timeline dashboard where critical events like Audit logs, Pool status change, Failover status change, DOS attacks etc. must be shown for ease of troubleshooting with last 20 Failed logins details		The clause should mention the functionality should be achieved without being dependent on tools.	The clause represents single OEM offering.	No Change
189	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #15	The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide a Bug tracker option, where an admin can login and find any bugs affecting the devices		The clause should mention the functionality should be achieved without being dependent on tools.	The clause represents single OEM offering.	No Change
190	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #16	The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide an upgrade Options suggestions for next hotfix and stability release for ease of day-2 operations with single click access to release notes a nd EOS dates		The clause should mention the functionality should be achieved without being dependent on tools.	The clause represents single OEM offering.	No Change
191	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #17	The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide an ability to execute CLI commands which are essential for diagnostics which will show historic data or data at the time of file captured. E.g show history of all executed commands on the CLI		Request you to remove this clause	Database Load Balancer is provided as inbuilt feature from database solution provider and hence not needed from SLB solution	No Change
192	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF C.Solution Capabilities Point #23	Solution should have the capability to highlight (In red / any color code) only malicious payload from the entire attack payload on the event analysis dashboard for detailed fornsics analysis. This is extermly critical when our incident response teams are in combat with the attackers during wartime. This feature/functionality has to be live demonstrated by the bidder after the prebid query meeting, by setting up a lab in the cloud/on-premises		Forensics are not required for LB or WAF kind of solution. This is required for DDoS kind of solution and it is not recommended to have DDoS solution within WAF+LB as DDoS should be a stateless technology and it's placement should be at perimeter level above firewall to protect complete infrastruture		No Change

| 193 | NA | Appendix02 Techno Functional Requirements- Network components > LB+WAF C.Solution Capabilities Point #36 | The Proposed WAF Solution should provide built-in L7 layer DDoS detection and mitigation features based on machine learning and behavioral analytics and dynamic signatures. It should have CAPTCHA support or other mechanism to avoid distributed attack.

This feature/functionality has to be live demonstrated by the bidder after the prebid query meeting, by setting up a lab in the cloud/on-premises | | Request to remove this point | DDoS should be a stateless device and it's placement should be at perimeter level above firewall. This ensures protection to network from any advanced DDoS attacks. Hence, it should not be expected to be part of other security solutions within the network. | No Change |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 194 | NA | Appendix02 Techno Functional Requirements- Network components > LB+WAF C.Solution Capabilities Point #58 | The Solution should have IPSEC tunneling capabiltiies | | Request to remove this point | VPN is recommended to be a dedicated solution since it relies on TLS protocol. It is also recommended to terminate the traffic on Firewall or before Firewall as it will check for security parameters on the same.

If this is done on ADC, there won't be any security check and can possess threat or security flaw. | No Change |
| 195 | NA | Appendix02 Techno Functional Requirements- Network components > LB+WAF C.Solution Capabilities Point #59 | The proposed solution should support a comprehensive list of ways in which LB can monitor the backend services including Daimeter, DNS, FTP, Gateway ICMP, HTTP, HTTPS, TCP half open, TCP , LDAP, MSSQL, MYSQL, MQTT , POSTGRESQL, POP3 , IMAP, NNTP, Radius , SIP and custom external scripts | | Request to modify the clause as below:

The proposed solution should support a comprehensive list of ways in which LB can monitor the backend services including DNS, FTP, Gateway ICMP, HTTP, HTTPS, TCP half open, TCP , LDAP, MSSQL, MYSQL , POSTGRESQL, POP3 , IMAP, NNTP, Radius and custom external scripts | SIP, Diameter & MQTT Traffic are used in Service Provider environment and are not relevant and used in any Enterprise environment like BOB Cards. | No Change |
| 196 | NA | Appendix02 Techno Functional Requirements- Network components > LB+WAF C.Solution Capabilities Point #61 | The proposed solution should support various types of LB config for handling traffic, including standard reverse proxy, forwarding in L2 , Forwarding in IP, High performance mode, Stateless mode , Reject mode, DHCP relay, and Message routing for SIP, Daimeter and MQTT traffic | | Request this clause be modified as below:

The proposed solution should support various types of LB config for handling traffic, including standard reverse proxy, forwarding in L2 , Forwarding in IP, High performance mode, Stateless mode , Reject mode, DHCP relay | SIP, Diameter & MQTT Traffic are used in Service Provider environment and are not relevant and used in any Enterprise environment like BOB Cards. | No Change |
| 197 | NA | Appendix02 Techno Functional Requirements- Network components > LB+WAF C.Solution Capabilities Point #70 | The proposed solution should support native integration with kubernetes based platforms hosting microservices e.g. Openshift, TKG cluster etc. Solution should update the configuration of LB automatically by observing events within kubernetes clusters form day 1 without add on license. | | Solution should be able to support by means of same solution. | | No Change |

198	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF C.Solution Capabilities Point #81	The proposed LB solution should also support secure remote access to admin users (concurrency of not more than 10); where the solution can do endpoint checks for the admins and establist a secure tunnel with autentication against AD/OAUTH/Radius and MFA via Google authenticator. The system should allow per user basis a login schedule ?(e.g night shift employee cannot login during working hours)	The clause represents single OEM offering.		No Change
199	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF D.Availability #2	The solution should support SQL-based querying for the following databases for the health checks: for Oracle, MSSQL, MySQL, PostgresSQL and other databases if required in future.	Request this clause be removed	Database Load Balancer is provided as inbuilt feature from database solution provider and this is proprietary load balancing feature of Database solution provider and hence not needed from ADC solution.	No Change
200	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #7	The Firewall appliance should have certifications like ICSA /EAL4/CCNDPP	Request this be modified as below: The Firewall solution should have certifications like ICSA /EAL4/CCNDPP	Every OEM has its own solution offering and certification ask may align to the approach solution is provided rather than mandating it on the appliance inline to a particular OEM	No Change
201	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #9	OEM/Bidder should provide below transceivers from Day-1. Firewall and SFP should be from same OEM. Below mentioned SFP quantity is required per appliance. 4 X 10GE SR SFP+ 4 X 1G SFP 4 x 25G SFP28	OEM/Bidder should provide below transceivers from Day-1. Firewall and SFP should be from same OEM. Below mentioned SFP quantity is required per appliance. 4 X 1G RJ 45 4 X 10G SFP+ 4 x 25G SFP28	Requesting if 1G can be considered using Copper Links and not SFP	No Change
202	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #15	Solution should have minimum 450 GB SSD pair, system storage	Request to modify this as below Solution should have minimum 900 GB SSD pair, system storage	Perimeter Firewall needs high storage numbers as visible with mid/large scale deployments for storing logs considering 3/6 months retention in case the remote Management device is impacted , so good to ask for more	No Change, additional feature will consider as value add
203	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #16	Solution should have minimum 32 GB	Request clause to be modifiedL Solution should have minimum 128 GB RAM	Perimeter Firewall has to have good RAM and such baselining will help with operations of critical banking infra	No Change, additional feature will consider as value add

204	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #19	"The proposed firewall must provide minimum 10 Gbps of Threat prevention throughput with Real world traffic. (Throughput must be derived from Appmix traffic and not Video/JPEG based traffic) (enterprise testing condition). The throughput must remain 10 Gbps even after enabling NGFW + IPS/IDS + Antivirus + Anti Spyware + Anti Bot + DoS/DDOS + All signature enabled + Logging enabled + Bidirectional inspection + File Blocking. OEM to provide publicly available The Test methodology and result should be compliant to the benchmark testing methodology for the above parameters provided in the Internet Engineering Task Force (IETF)- 'Benchmarking Methodology for		Request below modified clause be considered , instead of Appmix traffic , real world traffic should be mentioned for deriving throughput "The proposed firewall must provide minimum 10 Gbps of Threat prevention throughput with Real world traffic. (Throughput must be derived from real world traffic and not Video/JPEG based traffic) (enterprise testing condition). The throughput must remain 10 Gbps even after enabling NGFW + IPS/IDS + Antivirus + Anti Spyware + Anti Bot + DoS/DDOS + All signature enabled + Logging enabled + Bidirectional inspection + File Blocking. OEM to provide publicly available The Test methodology and result should be compliant to the benchmark testing methodology for the above parameters provided in the Internet Engineering Task Force (IETF)- 'Benchmarking Methodology for Network Security Device	instead of appmix traffic real world traffic will be rifht measure of throuhgput , so requesting the change	No Change
205	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #21	NGFW appliance must be capable of handling minimum 2 M concurrent sessions utilizing HTTP transactions with all Security feature Turned ON and not based on UDP / Lab environment / ideal testing environment, this claim has to be supported with declaration of concurrent connections claim from OEM		Request below modified clause to accomodate support for 5M concurrent sessions NGFW appliance must be capable of handling minimum 5 M concurrent sessions utilizing HTTP transactions with all Security feature Turned ON and not based on UDP / Lab environment / ideal testing environment, this claim has to be supported with declaration of concurrent connections claim from OEM	Mid/Large scale deployments need higher concurrent session support and baselining this to 50 Lakh concurrent sessions will be in the interest of the Bank , so the requested change	No Change, additional feature will consider as value add
206	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #49	Solution should support creation of minimum 1 virtual context / instance from Day-1 without any compromise on system performance and network bandwidth.		Solution should support creation of minimum 5 virtual context /instance from Day-1 without any compromise on system performance and network bandwidth.	Support for only 1 Virtual context may not be scalable for the DC design and min support for 5 instances is the need for any DC infra Perimeter Firewall understanding furture state architecure and growing needs.	No Change, additional feature will consider as value add

207	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #54	The proposed NGFW solution architecture should have Control Plane separated from the Data Plane in the Firewall appliance architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup, QoS, NAT etc). Control plane must have dedicated resources such as CPU, RAM etc. This is to ensure Bank always has management access to NGFW irrespective of Firewall load / Traffic Spike / Cyber Attack driving higher CPU utilization. Bank should able to login to the firewall and carry out reporting /		Request below modified clause be considered

The proposed NGFW solution architecture should have Control Plane separated from the Data Plane in the Firewall solution architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup, QoS, NAT etc). Control plane must have dedicated resources such as CPU, RAM etc. This is to ensure Bank always has management access to NGFW irrespective of Firewall load / Traffic Spike / Cyber Attack driving higher CPU utilization. Bank should able to login to the firewall and carry out reporting / management / packet capture etc to identify the root cause and accordingly take necessary action to remediate it. | OEMs have different approaches to achieving the use case and instead of the ask on the appliance itself , the Firewall Solution will be a generic term to use in requirements so this suggestion | No Change |
| 208 | NA | Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #72 | IPS should provide detailed information on each protection, including: Vulnerability and threat descriptions, Threat severity, Performance impact, Release date, Industry Reference, Confidence level etc. | | Request below changed clause :

IPS should provide detailed information on each protection, including: Vulnerability and threat descriptions, Threat severity, Release date, etc | Performance impact, industry reference and confidence level are subject to configuration and infrastructure in the bank. | No Change |
| 209 | NA | Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #76 | Should have more than 60+ predefined Categories based on Urls, Application types, Security Risk level etc. However solution should be able to create custom categories for URL and application. | | Request below modified clause with increased number of categories:

Should have more than 80+ predefined Categories based on Urls, Application types, Security Risk level etc. However solution should be able to create custom categories for URL and application. | Having more predefined categories support would help bank with improved threat detection and better granular policy control with less manual effort. | No Change, additional feature will consider as value add |
| 210 | NA | Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #89 | Solution should give information related to Performance impact and confidence level of protections while creating profiles. | | Request this clause be deleted | performance can be subject to policy configurations and existing infra at bank. | No Change |

211	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #114	"Management server should support the following for rule optimization: • Unused Rules Calculation for specific time-period based on Firewall Traffic Logs. • Analysis on Covered/Shadow/Hidden Rules • Analysis on Rules Consolidation (Merging of similar kind of rules) • Analysis on Redundant Rules • Tightening of Overly Permissive Rules (Any-Any) • Analysis on Unattached/Unused Objects to simplify objects management • Analysis on Rule-Reordering to improve the performance of the Firewall • Analysis on Disabled/Expired Rules for enhanced visibility on the Firewall Rules sets"		"Management server should support the following for rule optimization: • Unused Rules Calculation for specific time-period based on Firewall Traffic Logs / HIt count • Analysis on Covered/Shadow/Hidden Rules • Analysis on Redundant Rules • Analysis on Unattached/Unused Objects to simplify objects management • Analysis on Disabled/Expired Rules for enhanced visibility on the Firewall Rules sets"	OEMs could be handling the use case suggested for removal differently or have no dependency on the performance of the Firewall , so requesting these be removed from the ask	No Change
212	NA	Appendix02 Techno Functional Requirements- Network components > IPS Features Point #15	Should support more than 3000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness		Should support more than 5000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness	Increasing number of signature support is beneficial for the Bank's operations and for Effective Security reasons	No Change
213	NA	Appendix02 Techno Functional Requirements- Network components > internal FW Point #11	The Firewall solution Should support more than 4000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness and should be able to create 40 or more application categories for operational efficiency. Dedicated IPS solution shall be in corporated by the bidder to achive this scale of IPS AVC signatures in this solution.		Request this clause be modfied as below: The Firewall solution Should support more than 6000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness and should be able to create 40 or more application categories for operational efficiency. Dedicated IPS solution shall be in corporated by the bidder to achive this scale of IPS AVC signatures in this solution.	Increasing number of signature support is Beneficial for the Bank's operations and for Effective Security reasons	No Change, additional feature will consider as value add
214	NA	Appendix02 Techno Functional Requirements- Network components > internal FW NG Firewall Features NEW POINT	New Point to be added		The solution should provide Change Management capability for the organizations needs to implement more formal processes for configuration changes, including audit tracking and official approval before changes are deployed.	By leveraging these features and integrating with external change management tools, organizations can implement a robust change management process that includes formal approval, audit tracking, and compliance reporting within Cisco FMC.	No Change

				Features NEW POINT		
215	NA			The solution should provide traffic hit count, Rule Conflict Detection (Redundant & Shadowed) and policy warning for streamlining firewall policies.	These features are crucial for optimizing firewall policies, ensuring efficient traffic flow, and maintaining security posture.	No Change, additional feature will be consider as value add
216	NA	Appendix02 Techno Functional Requirements-Network components > internal FW Hardware Architecture Point #3	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 8x64 GB of RAM.	Request below modified clause be considered as correction on the ask which seems typo: 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.		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.
217	NA	Appendix02 Techno Functional Requirements-Network components > Mngmt Switch 6 Product Support Point #2	The OEM support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support	Request below modified clause be considered The OEM/OEM certified partner support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support	OEM Certified partner has thorough experience of OS version upgrades and maintaining network operations troubleshooting issues and it will be cost effective to include this in the ask	The OEM/OEM certified partner support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support
218	NA	Appendix02 Techno Functional Requirements-Network components > Mngmt Switch 9 Miscellaneous Points Point #1	Console cable and power cable (As per Indian standards) as per customer requirement to be provided. All Cables shall be factory-terminated.	Since Console Cables are common for all devices per OEM , Request Bank to clarify the count of console cables to be provided , is it one each with each Switch or one per DC and DR Each ?.		No Change
219	NA	Appendix02 Techno Functional Requirements-Network components > Mngmt Switch 10 Product Support Point #2	The OEM support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support	Request below modified clause be considered The OEM/OEM certified partner support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support	OEM Certified partner has thorough experience of OS version upgrades and maintaining network operations troubleshooting issues and it will be cost effective to include this in the ask	The OEM/OEM certified partner support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support
220	NA	Appendix02 Techno Functional Requirements-Network components > Core Swtich >9 Manageability > Appliance point 9.4	Switch Anomolies related with Advisories , PSIRT and Field Notices	Request this clause be removed from the telemetry asks	This feature is not requireed for the design at the BOB DataCenter and may be removed	No Change
221	NA	Appendix02 Techno Functional Requirements-Network components > Core Swtich >13 Fabric Management > Appliance point 13.1	Solution must provide Centralized Management Appliance – Single pane of glass for managing, monitoring and provisioning the entire Solution within Data Center & across all Data Centers	Request BOBCards to provide VM compute resources for spinning up the VMs to provide this functionality while we can provide the necessary sw and support.		Requested product functionality should be comply, BOBCards will provide VM compute resources for spinning up the VMs to provide this functionality however bidder should provide the necessary sw and support.
222	NA	Appendix02 Techno Functional Requirements-Network components > Core Swtich >5 Layer 2 Features > Appliance point 5.11	Switch Hardware should have capability to support BGP EVPN Route Type 1, Type 2, Type 3, Type 4, Route Type 5, Type 6/Type 7/Equivalent routes	Request this point be removed	BOBCards design doesn't have Fabric so this is not applicable	No Change

#							
223	NA	Appendix02 Techno Functional Requirements-Network components > Core Swtich >13 Fabric Management > Appliance point 13.36	Solution should provides reports using predefined templates, including inventory, use, and health reports.		Request below modified clause be considered: Solution should provides reports including inventory, use, and health reports.		No Change
224	19	5.4	Bid Security		Bidders are required to submit a Bid Security/ Earnest Money Deposit (EMD) for Rupees 5 Lac by way of RTGS/Online transfer (Appendix 06 – Bank Details for EMD & Tender Fees).	Dear Sir, Please confirm if MSME Bidders has 50% EMD relaxation in the said bid	It is exempted for MSME partner, with the submission of proper certification.
225			Eligibility Criteria		Bidder should have experience of minimum 3 years in providing the Proposed Products/Services mentioned in the RFP.	Please confirm if general Sever suppply & installation project will be considered	erver supply & installation project cannot be co
226			Evaluation Criteria		The bidder should have supplied and installed similar to proposed hardware in last three (3) financial years, i.e. 2021-2022, 2022-23, 2023-24 (Bidder to provide details in Annexure K and submit PO / Contract details)	Dear Sir, Please confirm if any specific value & project description needs to be fulfilled for complying the same.	The bidder should have supplied and installed proposed OEM hardware in last three (3) financial years, i.e. 2021-2022, 2022-23, 2023-24 (Bidder to provide details in Annexure K and submit PO / Contract details) yes we can consider separate PO.
227			Evaluation Criteria		The bidder should have deployed and configured proposed software as per OEM standard on proposed hardware in last three (3) financial years, i.e. 2021-2022, 2022-23, 2023-24 (Bidder to provide details / submit PO / Contract details)	Dear Sir, Please confirm if any specific value & project description needs to be fulfilled for complying the same.	The bidder should have deployed and configured proposed software as per OEM certified and standard hardware in last three (3) financial years, i.e. 2021-2022, 2022-23, 2023-24 (Bidder to provide details / submit PO / Contract details)
228	1	Annexure -I, Eligibility Criteria point 5	Bidder should have experience of minimum 3 years in providing the Proposed Products/Services mentioned in the RFP.		We request you to revise this clause as "Bidder should have experience of minimum 3 years in providing the similar Products/Services mentioned in the RFP."	We request you to revise this clause as "Bidder should have experience of minimum 3 years in providing the similar Products/Services mentioned in the RFP."	No Change
229	1	Annexure -II, Technical Evaluation point 1	The bidder should have supplied and installed similar to proposed hardware in last three (3) financial years, i.e. 2021-2022, 2022-23, 2023-24 1-3 deployment – 20 Marks 4-6 deployment – 30 Marks More than 6 deployment – 40 Marks		We request you to revise this clause as "The bidder should have supplied and installed similar to proposed hardware in last three (3) financial years, i.e. 2021-2022, 2022-23, 2023-24 1-2 deployment – 20 Marks 3-4 deployment – 30 Marks More than 4 deployment – 40 Marks."	We request you to revise this clause as "The bidder should have supplied and installed similar to proposed hardware in last three (3) financial years, i.e. 2021-2022, 2022-23, 2023-24 1-2 deployment – 20 Marks 3-4 deployment – 30 Marks More than 4 deployment – 40 Marks."	No Change
230	1	Annexure -II, Technical Evaluation point 2	The bidder should have deployed and configured proposed software as per OEM standard on proposed hardware in last three (3) financial years, i.e. 2021-2022, 2022-23, 2023-24 1-3 deployment – 10 Marks 4-6 deployment – 20 Marks More than 6 deployment – 30 Marks		We request you to revise this clause as "The bidder should have deployed and configured proposed software as per OEM standard on proposed hardware in last three (3) financial years, i.e. 2021-2022, 2022-23, 2023-24 1-2 deployment – 10 Marks 3-4 deployment – 20 Marks More than 4 deployment – 30 Marks."	We request you to revise this clause as "The bidder should have deployed and configured proposed software as per OEM standard on proposed hardware in last three (3) financial years, i.e. 2021-2022, 2022-23, 2023-24 1-2 deployment – 10 Marks 3-4 deployment – 20 Marks More than 4 deployment – 30 Marks."	No Change
231		Appendix 02-Perimeter Firewall, Point No.15	Solution should have minimum 450 GB SSD pair, system storage		Requesting change as "SSD's are by default high performance drives with inbuilt resiliencey"	Request you to change the Point to "Solution should have minimum 450 GB SSD , system storage"	No Change
232	1	Annexure -I, Eligibility Criteria point 5	Bidder should have experience of minimum 3 years in providing the Proposed Products/Services mentioned in the RFP.		We request you to revise this clause as "Bidder should have experience of minimum 3 years in providing the similar Products/Services mentioned in the RFP."	We request you to revise this clause as "Bidder should have experience of minimum 3 years in providing the similar Products/Services mentioned in the RFP."	No Change

233	1	Annexure -II, Technical Evaluation point 1	The bidder should have supplied and installed similar to proposed hardware in last three (3) financial years, i.e. 2021-2022, 2022-23, 2023-24 1-3 deployment – 20 Marks 4-6 deployment – 30 Marks More than 6 deployment – 40 Marks		We request you to revise this clause as "The bidder should have supplied and installed similar to proposed hardware in last three (3) financial years, i.e. 2021-2022, 2022-23, 2023-24 1-2 deployment – 20 Marks 3-4 deployment – 30 Marks More than 4 deployment – 40 Marks."	We request you to revise this clause as "The bidder should have supplied and installed similar to proposed hardware in last three (3) financial years, i.e. 2021-2022, 2022-23, 2023-24 1-2 deployment – 20 Marks 3-4 deployment – 30 Marks More than 4 deployment – 40 Marks."	No Change
234	1	Annexure -II, Technical Evaluation point 2	The bidder should have deployed and configured proposed software as per OEM standard on proposed hardware in last three (3) financial years, i.e. 2021-2022, 2022-23, 2023-24 1-3 deployment – 10 Marks 4-6 deployment – 20 Marks More than 6 deployment – 30 Marks		We request you to revise this clause as "The bidder should have deployed and configured proposed software as per OEM standard on proposed hardware in last three (3) financial years, i.e. 2021-2022, 2022-23, 2023-24 1-2 deployment – 10 Marks 3-4 deployment – 20 Marks More than 4 deployment – 30 Marks."	We request you to revise this clause as "The bidder should have deployed and configured proposed software as per OEM standard on proposed hardware in last three (3) financial years, i.e. 2021-2022, 2022-23, 2023-24 1-2 deployment – 10 Marks 3-4 deployment – 20 Marks More than 4 deployment – 30 Marks."	No Change
235		Appendix 02-Perimeter Firewall, Point No.15	Solution should have minimum 450 GB SSD pair, system storage		Requesting change as "SSD's are by default high performance drives with inbuilt resiliencey"	Request you to change the Point to "Solution should have minimum 450 GB SSD , system storage"	No Change
236	11	3.1 Project Scope Point #1	The supplied Hardware and Software shall be of the latest versions and should not be end of life / end of support for the next 7 years.		Request the start Date for 7 Yrs mention in the clause be specified. Is it RFP Date or Date of PO Issuance/GoLive Date or something else?	Right tenure will help align the final BOM and any discrepent inpurs will impact pricing , so requesting clarification	The supplied Hardware and Software shall be of the latest versions and should not be end of life / end of support for the next 5 years from the date of delivery
237	12	3.1 Project Scope Point #4	All Software licenses effective date shall be effective as on Go-LIVE sign off or put in use for BOBCARD operations.		Contract Start period is mentioned as PO Issuance while the SW licenses effective date is mentioed as GoLive Sign off Dates as noticed. Request Bank to keep this synchronized if this is genuine or clarify the intent	Right tenure will help align the final BOM and any discrepent inpurs will impact pricing , so requesting clarification	License effectiveness should be start from the software is ready to use. License cost will not impact to BOBCARD due to implementation delay. No license activate without informing BOBCARD.
238	12	3.1 Project Scope Point #12	Hardware RMA (Return Merchandise Authorization) should be within 24 hours		Request this be modified as below Hardware RMA (Return Merchandise Authorization) should be within 24 hours on Next business Day Basis.	RMA for a request raised on Friday may be honored by Monday due to the weekend in between , so requesting to keep this clearly specified.	Hardware RMA (Return Merchandise Authorization) should be within 24 hours on Next business Day Basis.

239	19	5.3 Price Comparisons Point #c iv	End of Sales/ End of support: The Vendor has to ensure that any application, related software supplied / put to use as part of this RFP should not have reached end of support. In the event if any equipment supplied / put to use by the vendor reaches end of support, within the contract period from the date of use, the vendor has to replace the equipment/ software at no additional cost to the Company before end of support.		End of Life/End of Sale Clause here should specifiy the start date as to if PO issuance, RFP Date or any other . Further the tenure within which EOS/EOL should not happen must be mentioned like 7 years in clause Project Scope point #1	Right tenure will help align the final BOM and any discrepent inpurs will impact pricing , so requesting clarification	The supplied Hardware and Software shall be of the latest versions and should not be end of life / end of support for the next 5 years from the date of delivery
240	9	2.2 Tenure	The tenure of the contract initially would be for 1 year from the date of the issuance of first purchase order. BOBCARD can further extend to 2 years at its at mutually agreed terms.		Contract Tenure mentioend as 1 Year from PO Issuance here while its 3 years in clause 3.1 Point 17/ Pls clarify the right tenure?	Right tenure will help align the final BOM and any discrepent inpurs will impact pricing , so requesting clarification	Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
241	13	3.1 Project Scope Point #17	The initial term of this contract shall be 3 years and may be extended to another 2 years subject to satisfactory performance by successful bidder and OEM(s).		Mentioned here is 3 years of initial contract and in 2.2 section the contract mentioned is 1 Year/ pls clarify the right tenure	Right tenure will help align the final BOM and any discrepent inpurs will impact pricing , so requesting clarification	Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
242	30	7.2 Evaluation Methodology for Eligible Bidder Commercial Bid Evaluation	The key considerations of the TCO would be the total payouts for entire project through the contract period of 5 years.		Mentioned here is 5 years contract but in 2.2 the tenure of contrat is 1 Year, pls clarify the number to consider	Right tenure will help align the final BOM and any discrepent inpurs will impact pricing , so requesting clarification	Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
243	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Server Prod > HCI Rack Servers > 1	Total QTY is 14		Clarifictaion Needed: 1. Please provide split of quantity of servers / Nodes per location. 2. Kindly specify the number of clusters and nodes per cluster also.	clarifiction will help arrive at the boq rightly	This will be shared with only elected bidder
244	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Server Prod > HCI Rack Servers > 7	Each Rack Server Controller Cards / Controller Drive should be provided in HA mode in RAID -1.		Request Change: Each HCI Server should be configured with two BOOT drives with hardware RAID Controller. For NVMe storage drives: Provides as per Certifed HCI Node with NVMe configuration	From the HCI Rack server or Pre configured HCI NODE - RAID Controller card is not required for NVMe drives. Also, is this ask for Boot drive with RAID Controller?	Yes, we need boot drive for HCI hypervisor provided in HA mode in RAID -1
245	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Server UAT > HCI Rack Servers > 7	Each Rack Server Controller Cards / Controller Drive should be provided in HA mode in RAID -1.		Request Change: Each HCI Server should be configured with two BOOT drives with hardware RAID Controller. For NVMe storage drives: Provides as per Certifed HCI Node with NVMe configuration	From the HCI Rack server or Pre configured HCI NODE - RAID Controller card is not required for NVMe drives. Also, is this ask for Boot drive with RAID Controller?	Yes, we need boot drive for HCI hypervisor provided in HA mode in RAID -1

246	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Server Prod > HCI Rack Servers > 6	Each Rack servers should have minimum usable Storage Capacity of 10 TB of all caching SSD and other HDD. 20% disk slot on each node should be free for future expansion		Clarification needed: In virtualized environment, the storage (usable) capacity is calcluated across the cluster. Need clarification on the total capacity required across the number of nodes in a cluster.	clarifiction will help arrive at the boq rightly	as mentioned in RFP 10TB usable storage per node * no of node = total usable capacity
247	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Server UAT > HCI Rack Servers > 6	Each Rack servers should have minimum usable Storage Capacity of 10 TB of all caching SSD and other HDD. 20% disk slot on each node should be free for future expansion		Clarification needed: In virtualized environment, the storage (usable) capacity is calcluated across the cluster. Need clarification on the total capacity required across the number of nodes in a cluster.	clarifiction will help arrive at the boq rightly	as mentioned in RFP 10TB usable storage per node * no of node = total usable capacity
248	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Server Prod > HCI Rack Servers > 13 >Server Security	Request New Point to be added		Request to add the below point for security and management features for HCI Nodes Day2 operations and management of HCI Nodes for updates on Hardware and Software. HCI Node management tool should integrate with Virtual platform and Network switches. Should be able to do Firmware updates, Manage Cluster and deployment, Full stack visibility of HCI Node, TAC/Case Support, Continuous Health checks on Networking, Server, VMs , Anomalies detection, Security advisories, patch management etc.	HCI Node should integrate with Virtual platform and Network switches, Should have management software for a Firmware update, Manage Cluster and deployment, Full stack visibility HCI Node, TAC/Case Support, Continuous Health checks on Networking, Server, VMs , Anomalies detection, Security advisories, patch management,	No Change, additional feature will be consider as value add
249	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Server UAT > HCI Rack Servers > 13> Server Security	Request New Point to be added		Request to add the below point for security and management features for HCI Nodes Day2 operations and management of HCI Nodes for updates on Hardware and Software. HCI Node management tool should integrate with Virtual platform and Network switches. Should be able to do Firmware updates, Manage Cluster and deployment, Full stack visibility of HCI Node, TAC/Case Support, Continuous Health checks on Networking, Server, VMs , Anomalies detection, Security advisories, patch management etc.	HCI Node should integrate with Virtual platform and Network switches, Should have management software for a Firmware update, Manage Cluster and deployment, Full stack visibility HCI Node, TAC/Case Support, Continuous Health checks on Networking, Server, VMs , Anomalies detection, Security advisories, patch management,	No Change, additional feature will be consider as value add
250	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Microsegmentation > 1	The Solution should be capable of supporting major hardware OEMs like Juniper, Arista, Cisco, HPE and Dell. The proposed solution should be a purely software-based solution and should not be dependent on any hardware make and model.		Request below modified clause be considered: The Solution should be capable of supporting major hardware OEMs like Juniper, Arista, Cisco, HPE and Dell. The proposed solution should be a purely software-based solution and should not be dependent on any hardware make and model by creating overlay tunnels between the hosts.	The key benefits of no dependecy on hardware is by using software defined networking i.e overlay. Overlay is mandatory for network & Security automation as part of software defined data center.	No Change

251	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Microsegmentation > 2	The solution should provide a distributed firewall such that the firewalling for Virtual Machines can be provided closest to the application within the server itself without traffic going to a Physical Firewall.		Request below modified clause be considered which includes additonal points The solution should provide a distributed firewall such that the application aware and identity based statefull firewalling for Virtual Machines can be provided closest to the application within the server itself without traffic going to a Physical Firewall or regardless of underlying L2 Netwrork topology. The solution should also provide an integrated networking solution (CNI implementations) as well as provide advance turnkey container networking & firewalling services. Solution should support for container networking plug-ins, support for pod to pod communication and support for ingress controllers. The micro-segmentation solution should have a capability for stateful firewalling and ALGs (Application Level Gateway) on a per-workload granularity regardless of the underlying L2 network topology (i.e. possible on either logical network overlays or underlying VLANs), embedded in the hypervisor kernel, distributed	As per security framework its recommended not to use standard ports for your applications and hence to have effective security on per VM basis an application/L7 firewalling is must. Containers & Kubernetes are now part of all modern applications hence networing and security for container shall also be considered for end to end application security. there is App ID requirement is mentioned in RFP as part of "Internal Firewall" spec point # 23 hence same should be considered for mirosegmenation as well otherwise it will create non standard architecture.	No Change
252	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Microsegmenation >5	The proposed solution should provide the ability to define firewall rules at VM level for east-west traffic in order to implement Zero Trust Security		Request below modified clause be considered: The proposed solution should provide the ability to define Layer 7 application firewall rules at VM level for east-west traffic in order to implement Zero Trust Security alongwith URL Filtering and TLS inspection for encrypted traffic	Zero trust Security framework mandates TLS inspection for encrypted traffic, URL Filtering and Layer 7 application firewalling.	No Change, additional feature will be consider as value add
253	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Microsegmenation >4	The Proposed Solution including Hypervisor, SDS and Micro segmentation must be from the same OEM.		Request below modified clause be consideredL The Proposed Solution including Hypervisor, SDS, SDN and Micro segmentation must be from the same OEM.	SDN is missing in the spec, SDN will be mandatory to create complete automated Software Defined data center by creating an abstraction of the network enabling programming of network behavior in a centrally controlled manner through software applications.	No Change, SDN will be consider as value add

254	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Microsegmenation >6	The proposed solution should allow users to define granular firewall rules based on IP Addresses, Tags/Categories and Subnets to segment User Applications		Request below modified clause be considered which includes additonal points The proposed solution should allow users to define granular firewall rules for both VM and conatiners based on IP Addresses, VM Names, Tags/Categories and Subnets to segment User Applications. The solution should have capability to provide stateful micro-segmentation for virtual machines and Kubernetes workloads from a single console. The solution should also support enforcement of stateful distributed firewall for IPv6 VM workloads. These firewall rules can use IPv6 addresses, IPv6 CIDR, IP Sets that include both IPv4 and IPv6 addresses and security groups that can include logical ports that have both IPv4 and IPv6 addresses. IPv6 capability should be available both at management and data plane	Its necessary to have dynamic security group capability to ensure complete automation. Mentioned in the RFP page 8 -> 2.0 --> Requirement Summary--> 2.1 Intent--> mentions requirement for IPv6 "The proposed solution should support both IPv4 and IPv6."
						No Change
255	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Microsegmenation >7	Solution should provide capability to create network segments by defining them entirely in software and avoid the need to re-architect your network or deploy physical appliances		Request below modified clause be accmodated: Solution should provide capability to create network segments and L2 Streching between DC and DR by defining them entirely in software and avoid the need to re-architect your network or deploy physical appliances	L2 Streching is required for better application availability considering RFP asks for 99.99 % availability on monthly basis. RFP Page 17 -> "4. Service Levels "-->"SLA: The solution is expected to be available for 99.99% on 24x7 and up time availability will be calculated on monthly basis."
						No Change, L2 stretching implementation will be discuss with elected bidder.
256	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Container >2	The solution must be able to manage Kubernetes clusters. Licenses for managing Kubernetes clusters should be implemented from Day-1		Request below modified clause be accmodated: The solution must be able to manage Kubernetes clusters. Licenses for managing Kubernetes clusters along with components such as backup, container registry and monitoring alongwith Windows Container support should be implemented from Day-1	Kubernetes Cluster doesn't work in isloation but require other components such as container registry and backup solution. If not included than Bob Card will have procure them separately. And Not aving Windows Container support will block any windows based apps to be deployed on Kubernetes Platform.
						Yes, BOBCARD will take care such requirement
257	NA	Appendix02 Techno Functional Requirements-Network components > internal FW NG Firewall Features NEW POINT	Must have provisioning, operations and lifecycle management of Kubernetes, automated deployment, scaling, and operation of Kubernetes clusters		Request below modified clause be accmodated: Must have provisioning, operations and lifecycle management of Kubernetes, automated deployment, Auto scaling & Auto Healing, and operation of Kubernetes clusters	Complete Automation is not possible without Auto Scaling and Auto Healing of Kubernetes Clusters. One has to manually add nodes in case of failure or unprovisioned increase in load.
						No Change

258	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Container >4	Container Platform should provide single pane of Glass for Lifecycle Management of all K8S clusters deployed on prem.		Request below modified clause be accmodated: Container Platform should provide single pane of Glass for Lifecycle Management of all K8S clusters alongwith ingress, backup and container registry deployed on prem.	Kubernetes Cluster doesn't work in isloation but require other components such as container registry and backup solution. These shall too be considered for life cycle management	Yes, BOBCARD will take care such requirement
259	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management >1	The solution should provide capability of generating reports for usage, performance, compliance, health, forecasting and capacity.		Request below modified clause be accmodated: The solution should provide capability of generating reports for health, Capacity Optmization - Right Sizing (Under sized, Oversized), Reclamation (Idle, Powered off , Snapshot, Orphaned Disk , Forecasting - Capacity Forecasting, Migration assessment, Migration Planning Usage - Process and service utlization Compliance - Regulatory Benchmark (PCIDSS and ISO) Security Guidelines for Infrastructure and Cloud Management	Bob Cards will need capacity optimization capabilities to identify over-provisioned & under-provisioned resources and provide recommendations, alerts and automated actions on right-sizing and resource consumption so they can be right-sized for adequate performance and avoid resource wastage. Should provide visibility of capacity and VMs which can be reclaimed and cost visibility of the reclaimed capacity and VMs.	No Change, additional feature will be consider as value add
260	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management >11	The solution should have intelligent operations with anomaly detection which will allow monitoring seasonal trends and automatically send email alert		The solution should have AI/ML driven intelligent operations & troubleshooting workbench with anomaly detection,third party infra (Server, Storage , Network, database and Application) along with parent child relatiohship mapping, service and process monitoring which will allow monitoring seasonal trends and automatically send email alert. The solution should also have log management capability for infrastructure and applications . log management solution should delivers intuitive, actionable dashboards, sophisticated analytics, and broad third-party extensibility across physical, virtual, and cloud environments.	BoB Cards will not be able to manage the infrastructure without comprhesive log management capability. Its also mandatory for from regulation/compliance perspective to have log stored for given period of time for audit. BoB Card would need apps (database and Application) to infra (Server, Storage , Network) level visibility for toubleshooting and performance monitoring.	No Change, additional feature will be consider as value add
261	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management >7	The solution must have an approval process to review, reject or approve the deployment requests from the marketplace.		Request below modified clause be considered: The Solution must support multiple levels of approval with E-mail notifications with ability to automate manual provisioning and de-provisioning of the tasks and policies embedded in each layer of their application including auto -approve and auto-reject capability based on application criticality	The solution must have an approval process to review, multi level & auto reject or approve the deployment requests from the marketplace.	No Change, additional feature will be consider as value add

262	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Hypervisor > 6	Hypervisor should support container and opensource integration for cloud native application from day-1. Must be a Kubernetes ready from day-1.		Request below modified clause be accmodated: Hypervisor should support container both Linux and Windows along with other kubernetes ecosystems such as container registry, backup, ingress & monitoring and opensource integration for cloud native application from day-1. Must be a Kubernetes ready from day-1.	Kubernetes does't work in isolation and requires multiple components for production setup.	Yes, BOBCARD will take care such requirement
263	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Hypervisor > 16	Virtualization Manager should provide feature which can perform quick, as-needed deployment of additional virtualized hosts. When the service is running, it can push out update images, eliminating patching and update without impacting production.		Please clarify the scenario and expected outcome out of the below point in this clause: "When the service is running, it can push out update images, eliminating patching and update without impacting production."		Virtualization manager should allow addition of new nodes and patching/upgrade of hypervisor running on the node without any VM downtime.
264	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Hypervisor > 22	Unlimited VM replication from DC to DR (No restriction on VM replication and DR orchestration) with the capability to define Recovery Plans		Request to provide the number of VMs to be orchestrated for automated recovery and not keep open as unlimited since this approach is OEM specific . The VMs to be protected/orchestrated are limited to what can be provisioned on these 14 servers of production. Furehr pls clarify the need for Recovery Plans		No Change, can not predict the exact number of VMs for next 5 Years which need to be replicated.
265	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Hypervisor > 23	Proposed solution should have a self-service restore feature on a per-VM basis to allow trusted application administrators to recover their own files with the ability to mount snapshots as a drive in Windows VMs		Request this be modified as below or clarify the requriement: Proposed solution should have a self-service restore feature on a per-VM basis to allow trusted application administrators to recover their own VMs from the snapshot	Please clarify this requirement, this looks like back and restore requirements so the modified clause	This will help BOBCARD to recover file without losing current state of virtual machine.
266	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Hypervisor > 24	Hypervisor should provide Visibility for Running VM and their connectivity co-relationship with Network Ports on attached Physical TOR / Core Direct which Include Network RX/TX Bytes.		Request below modified clause with additional inputs be considered : Hypervisor should provide Visibility for Running VM and their connectivity co-relationship with Network Ports on attached Physical TOR / Core Direct which Include Network RX/TX Bytes.Solution Should provide end to end visibility across physical firewall, switch and storage, Flow Analysis and Security Planning,Guided Troubleshooting, Microsegmentation planning, RCA (Connectivity Problem, Packet Loss, N/W latency), Application Discovery, Service Monitoring , Application Dependency Mapping and monitoring of non compliant ports	Monitoring is not considering all components of the stack. Unless end to end visibility is provided as part of this solution BoB Card has to spend separately on monitoring.	Yes, BOBCARD will take care such requirement. However Hypervisor should provide Visibility for Running VM and their connectivity co-relationship with Network Ports on attached Physical Port which Include Network RX/TX Bytes.

267	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Hypervisor > 30	Virtualization software or the solution should provide Cluster level encryption protects unauthorized data access at-rest.		Request below modified clause be considered : Virtualization software or the solution should provide Cluster level, VM Level encryption protects unauthorized data access at-rest and in transit.	Having capability to do the enscryption at app VM level and in transit is required to complete solution.	No Change, additional feature will be consider as value add
268	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Software Defined Storage > 1	Maintain primary working set copy of active data on the Local Node as VM's are hosted to provide high IOPS and low latency. Proposed solution must be proposed for faster reads and write for Business-critical Apps.		Request below additional point be added in theis clause : Proposed solution must be proposed for faster reads and write for Business-critical Apps.	Architecture is specific to one vendor, request BoB Cards to consider on outcome than specific architecture. There is no specific latency requirements mentioned in the spec.	No Change.
269	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Software Defined Storage >2	The solution must have De-duplication and Compression features licensed and implemented from day one (Should not have dependency on any proprietary hardware device).		Request below modified clause be considered: The solution must have De-duplication/Compression features licensed and implemented from day one (Should not have dependency on any proprietary hardware device).	Solution should have flexibility to implement either compression and de-duplication. BoB Cards should conisder overhead while deciding on both.	No Change
270	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Software Defined Storage >24	The proposed solution should support 1 min RPO & 1 hour RTO for critical workload in case BOB Cards wants to have this capability replication for Future use. The proposed solution should have native Replication and DR Orchestration from Day-1		What is the use case for 1 min RPO and 1 Hour RTO? is this linked with some regulatory requirement?	Replication is best handled at application level as having additional solution for infrastructure will complexity and cost for BoB Cards Its best to use extends the existing DR orchestration solution for this environment as well.	This is required for BOBCARD mission critical application. The solution should capable to support 1min RPO. The propose replication solution should be same OEM as the virtualization solution to provide seamless integration.
271	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Software Defined Storage >25	The solution provided should function even after one node failure.		Request below modified clause be considered: The solution provided should function even after two node failure.	RFP asks for 99.99 % availability SLA for the proposed solution. It will require minimum N+2 configuration for required resiliency and uptime.	No Change, additional feature will be consider as value add
272	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Software Defined Storage >31	The solution should provide enterprise data services such as compression completely in software. Software Defined Storage solution must have de-duplication and compression features Licensed and implemented from day one. These functionalities should be part of the proposed solution. The solution must have functionality to support compression and or deduplication online on data container without any downtime and data loss as per business requirement.		Request below modified clause be considered: The solution should provide enterprise data services such as compression completely in software. Software Defined Storage solution must have de-duplication or compression features Licensed and implemented from day one. These functionalities should be part of the proposed solution. The solution must have functionality to support compression and or deduplication online on data container without any downtime and data loss as per business requirement.	Solution should have flexibility to implement either compression and de-duplication. BoB Cards should conisder overhead while deciding on both.	No Change

273	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Microsegmentation > new point	Additional Point for consideration		The solution must ensure that there is not alteration in the IP address of the Virtual machine, by blocking the traffic from or to the VM inherited as a feature in the Solution.	IP/MAC spoofing is major security concern for organizations like BoB Cards handing customers data.	No Change, additional feature will be consider as value add
274	NA				The solution should support multi-tenancy to isolate networking/security for different departments/function within BoB Cards upto a minimum of 4 tenants and 5 VPCs	VPC will enable Bob Cards to create isolation from access , resources, network and security.	ange, additional feature will be consider as valu
275	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Container > 6	Should support cluster scale out i.e addition of worker nodes as and when required.		Request below modified clause be considered:

Should support Automated cluster scale out i.e addition of worker nodes as and when required. | Complete Automation is not possible without Auto Scaling and Auto Healing of Kubernetes Clusters. One has to manually add nodes in case of failure or unprovisioned increase in load. | No Change |
| 276 | NA | Appendix01 Techno Functional Requirements-Server and Virtual platform > Cloud Management > 3 | The solution shall provide a single pane of glass for automated provisioning with model-based orchestration of compute, network and storage through a unified multi-tenant self-service catalog. | | Request below modified clause be consiered

The solution shall provide a single pane of glass for automated provisioning with model-based orchestration of compute, network , storage and Kubernetes through a unified multi-tenant self-service catalog . | All modern applications are combination of both container and VM form factor. | No Change, additional feature will be consider as value add |
| 277 | NA | Appendix01 Techno Functional Requirements-Server and Virtual platform > Cloud Management > 5 | The solution must provide a self-service portal to allow user to consume the creation of infrastructure easily. | | Request below modified clause be considered:

The solution must provide a self-service portal to allow user to consume the creation of infrastructure easily for both VM and Kubernetes | All modern applications are combination of both container and VM form factor. | No Change, additional feature will be consider as value add |
| 278 | NA | Appendix01 Techno Functional Requirements-Server and Virtual platform > Cloud Management > 8 | The software must allow the designer to use shell script, PowerShell script to code the automation. | | Request below modified clause be considered:

The software must allow the designer to use shell script, PowerShell script, Python and node JS to code the automation. | Python and nodeJs are very popular language for scrpting in terms resource availability and community support | No Change, additional scripting will be value add |
| 279 | NA | Appendix01 Techno Functional Requirements-Server and Virtual platform > Cloud Management > 9 | The software must allow the designer to design VM blueprints. | | Request below modified clause be considered:

The software must allow the designer to design Multi VM & Kubernetes blueprints. | All modern applications are combination of both container and VM form factor. | No Change, additional feature will be consider as value add |
| 280 | NA | Appendix01 Techno Functional Requirements-Server and Virtual platform > Cloud Management > 12 | The solution should have simple low-code, no-code automation engine which allows automating day-to-day routine tasks | | Request below modified clause and adidtoinal inpurs on the clause be considered:

The solution should have simple low-code, no-code automation engine which allows automating day-to-day routine tasks such as Snapshot creation, Addition of Disk, Power Cycle (Suspend , Shutdown, Reboot, reset), Resize, Rebuild, Additional of Network, VM Unregister , Delete,connect remote console, Change Security Group with capability to create additional resource actions as out of the box capability. | All modern applications are combination of both container and VM form factor. | No Change, additional feature will be consider as value add |

281	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > New Point	New Point		Solution should provide capability to define and showcase cost to create cloud like experience to the business unit with the overall cost spend on the infrastructure [server hardware, storage, licenses, application, maintenance, labor, network, facilities , etc.	Bob Cards will need Cost transparency (Showback and Chargeback capability) across private, hybrid to optimize planning and prioritization of VM/ Server/Application onboarding/provisioning	No Change, additional feature will be consider as value add
282	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF & IPS	New Point		We request BoB Card to allow for both software and hardware based solution for Load Balancer, WAF, IPS/IDS. As these components are dynamic as per application consumption requirements and considering bob card is directly managing customer data, its very critcal that these components are added as part of sofwate defined stack.	Modern applications increasingly require software-defined networking (SDN) and security solutions due to their need for greater flexibility, agility, and scalability. Traditional networking and security methods often lack the adaptability to support the dynamic nature of modern application environments, especially in cloud	No Change
283	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF C.Solution Capabilites Pont #5	The solution must support and integrate the web application vulnurability tools (Web application scanners) being proposed by bidder as part of this RFP at minimum to virtually patch web application vulnurabilies or else solution should have ready plug-ins to integrate banks VAPT tool.		Requesting you to modify the clause as below: The solution must support and integrate the web application vulnurability tools (Web application scanners) being proposed by bidder as part of this RFP, solution should have ready plug-ins to integrate banks VAPT tool.	Solution should be capable to protect against zero-day vulnerability using positive security model without being dependent on virtual patching. Virtual patch can even lead to false positive.	No Change
284	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #2	Appliance/Chassis based Hardware should support scalability with license upgrade. -18 vCPU from day 1	Scalable to 32 vCPU -128 GB DDR RAM from day 1 -1 TB X 1 SSD M.2 SSD (in Raid) from Day 1		The clause represents single OEM offering for sizing		No Change
285	NA	7/B.Hardware & InAppendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #7	The proposed appliance shoulde provide minimum 1.2 Gbps of real world WAF throughput from day 1 and should be scalable to 2.2 Gbps with license upgrade on the same hardware or additional blades in case of a chassis based solution. The WAF throughput mentioned should be inclusive after enabling the below mentioned features: With all WAF functions enabled per intance in blocking mode SSL inspection.		The clause represents single OEM offering for sizing		No Change
286	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #8	The appliance should support the layer 7 throughput should be at least 58 Gbps scalable to 92 Gbps on same hardware with license upgrade. (Data rerernces for above should be verified from publicly available datasheet)		The clause represents single OEM offering for sizing		No Change

287	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF B.Hardware & Interfaces requirement Point #9	The proposed appliance must have minimum hardware compression of 34 Gbps for HTTP traffic form day 1 and scalable upto 48 Gbps with add on license on same hardware. (Data rerernces for above should be verified from publicly available datasheet)		The clause represents single OEM offering for sizing		No Change
288	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF B.Hardware & Interfaces requirement Point #10	The proposed appliance should support minimum hardware based SSL offloading from day 1 up to : 34 Gbps Scalable upto 48 Gbps on same hardware with license upgrade. (The SSL encryption & decryption process must be hardware-based proccessor for acceleration) (Data rerernces for above should be verified from publicly available datasheet)		The clause represents single OEM offering for sizing		No Change
289	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF B.Hardware & Interfaces requirement Point #11	The solution must support minimum SSL TPS/CPS: -29 K ECDSA P-256-bit keys from day 1 -58 K RSA 2048-bit keys from day 1 scalable to minimum SSL TPS/CPS -68 K ECDSA P-256-bit keys -98 K of RSA 2048-bit Keys (Data rerernces for above should be verified from publicly available datasheet with SSL)		The clause represents single OEM offering for sizing		No Change
290	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF B.Hardware & Interfaces requirement Point #12	The proposed appliance should support minimum 74 million L4 concurrent connections from day one and scalable upto 99 Million on same hardware with license upgrade.		The clause represents single OEM offering for sizing		No Change
291	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF B.Hardware & Interfaces requirement Point #13	The proposed appliance should support minimum 2.4 million L7 requests per seconds from day 1 and scalable upto 4.2 Million on same hardware with with license upgrade.		The clause represents single OEM offering for sizing		No Change
292	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF General Requirement Point #13	The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide traffic performance statistics for last 30 days including Active Connections, Active Sessions, CPU Usage By Core, HTTP Requests, Memory Used, RAM Cache Utilization, Rewrite Transaction, Data Rewrite Transactions, SSL Transactions, Throughput(bits), Throughput(packets), & Total New Connections		The clause should mention the functionality should be achieved without being dependent on tools.	The clause represents single OEM offering.	No Change

293	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF B.Hardware & Interfaces requirement Point #14	The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide a security event timeline dashboard where critical events like Audit logs, Pool status change, Failover status change, DOS attacks etc. must be shown for ease of troubleshooting with last 20 Failed logins details		The clause should mention the functionality should be achieved without being dependent on tools.	The clause represents single OEM offering.	No Change
294	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF B.Hardware & Interfaces requirement Point #15	The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide a Bug tracker option, where an admin can login and find any bugs affecting the devices		The clause should mention the functionality should be achieved without being dependent on tools.	The clause represents single OEM offering.	No Change
295	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF B.Hardware & Interfaces requirement Point #16	The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide an upgrade Options suggestions for next hotfix and stability release for ease of day-2 operations with single click access to release notes a nd EOS dates		The clause should mention the functionality should be achieved without being dependent on tools.	The clause represents single OEM offering.	No Change
296	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF B.Hardware & Interfaces requirement Point #17	The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide an ability to execute CLI commands which are essential for diagnostics which will show historic data or data at the time of file captured. E.g show history of all executed commands on the CLI		Request you to remove this clause	Database Load Balancer is provided as inbuilt feature from database solution provider and hence not needed from SLB solution	No Change
297	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF C.Solution Capabilities Point #23	Solution should have the capability to highlight (In red / any color code) only malicious payload from the entire attack payload on the event analysis dashboard for detailed fornsics analysis. This is extermly critical when our incident response teams are in combat with the attackers during wartime.

This feature/functionality has to be live demonstrated by the bidder after the prebid query meeting, by setting up a lab in the cloud/on-premises | | Forensics are not required for LB or WAF kind of solution. This is required for DDoS kind of solution and it is not recommended to have DDoS solution within WAF+LB as DDoS should be a stateless technology and it's placement should be at perimeter level above firewall to protect complete infrastruture | | No Change |

298	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF C.Solution Capabilities Point #36	The Proposed WAF Solution should provide built-in L7 layer DDoS detection and mitigation features based on machine learning and behavioral analytics and dynamic signatures. It should have CAPTCHA support or other mechanism to avoid distributed attack. This feature/functionality has to be live demonstrated by the bidder after the prebid query meeting, by setting up a lab in the cloud/on-premises		Request to remove this point	DDoS should be a stateless device and it's placement should be at perimeter level above firewall. This ensures protection to network from any advanced DDoS attacks. Hence, it should not be expected to be part of other security solutions within the network.	No Change
299	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF C.Solution Capabilities Point #58	The Solution should have IPSEC tunneling capabiltiies		Request to remove this point	VPN is recommended to be a dedicated solution since it relies on TLS protocol. It is also recommended to terminate the traffic on Firewall or before Firewall as it will check for security parameters on the same. If this is done on ADC, there won't be any security check and can possess threat or security flaw.	No Change
300	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF C.Solution Capabilities Point #59	The proposed solution should support a comprehensive list of ways in which LB can monitor the backend services including Daimeter, DNS, FTP, Gateway ICMP, HTTP, HTTPS, TCP half open, TCP , LDAP, MSSQL, MYSQL, MQTT , POSTGRESQL, POP3 , IMAP, NNTP, Radius , SIP and custom external scripts		Request to modify the clause as below: The proposed solution should support a comprehensive list of ways in which LB can monitor the backend services including DNS, FTP, Gateway ICMP, HTTP, HTTPS, TCP half open, TCP , LDAP, MSSQL, MYSQL , POSTGRESQL, POP3 , IMAP, NNTP, Radius and custom external scripts	SIP, Diameter & MQTT Traffic are used in Service Provider environment and are not relevant and used in any Enterprise environment like BOB Cards.	No Change
301	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF C.Solution Capabilities Point #61	The proposed solution should support various types of LB config for handling traffic, including standard reverse proxy, forwarding in L2 , Forwarding in IP, High performance mode, Stateless mode , Reject mode, DHCP relay, and Message routing for SIP, Daimeter and MQTT traffic		Request this clause be modified as below: The proposed solution should support various types of LB config for handling traffic, including standard reverse proxy, forwarding in L2 , Forwarding in IP, High performance mode, Stateless mode , Reject mode, DHCP relay	SIP, Diameter & MQTT Traffic are used in Service Provider environment and are not relevant and used in any Enterprise environment like BOB Cards.	No Change
302	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF C.Solution Capabilities Point #70	The proposed solution should support native integration with kubernetes based platforms hosting microservices e.g. Openshift, TKG cluster etc. Solution should update the configuration of LB automatically by observing events within kubernetes clusters form day 1 without add on license.		Solution should be able to support by means of same solution.		No Change

303	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF C.Solution Capabilities Point #81	The proposed LB solution should also support secure remote access to admin users (concurrency of not more than 10); where the solution can do endpoint checks for the admins and establist a secure tunnel with autentication against AD/OAUTH/Radius and MFA via Google authenticator. The system should allow per user basis a login schedule ?(e.g night shift employee cannot login during working hours)		The clause represents single OEM offering.	No Change
304	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF D.Availability #2	The solution should support SQL-based querying for the following databases for the health checks: for Oracle, MSSQL, MySQL, PostgresSQL and other databases if required in future.	Request this clause be removed	Database Load Balancer is provided as inbuilt feature from database solution provider and this is proprietary load balancing feature of Database solution provider and hence not needed from ADC solution.	No Change
305	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #7	The Firewall appliance should have certifications like ICSA /EAL4/CCNDPP	Request this be modified as below: The Firewall solution should have certifications like ICSA /EAL4/CCNDPP	Every OEM has its own solution offering and certification ask may align to the approach solution is provided rather than mandating it on the appliance inline to a particular OEM	No Change
306	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #9	OEM/Bidder should provide below transceivers from Day-1. Firewall and SFP should be from same OEM. Below mentioned SFP quantity is required per appliance. 4 X 10GE SR SFP+ 4 X 1G SFP 4 x 25G SFP28	OEM/Bidder should provide below transceivers from Day-1. Firewall and SFP should be from same OEM. Below mentioned SFP quantity is required per appliance. 4 X 1G RJ 45 4 X 10G SFP+ 4 x 25G SFP28	Requesting if 1G can be considered using Copper Links and not SFP	No Change
307	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #15	Solution should have minimum 450 GB SSD pair, system storage	Request to modify this as below Solution should have minimum 900 GB SSD pair, system storage	Perimeter Firewall needs high storage numbers as visible with mid/large scale deployments for storing logs considering 3/6 months retention in case the remote Management device is impacted , so good to ask for more	No Change, additional feature will consider as value add
308	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #16	Solution should have minimum 32 GB	Request clause to be modifiedL Solution should have minimum 128 GB RAM	Perimeter Firewall has to have good RAM and such baselining will help with operations of critical banking infra	No Change, additional feature will consider as value add

309	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #19	"The proposed firewall must provide minimum 10 Gbps of Threat prevention throughput with Real world traffic. (Throughput must be derived from Appmix traffic and not Video/JPEG based traffic) (enterprise testing condition). The throughput must remain 10 Gbps even after enabling NGFW + IPS/IDS + Antivirus + Anti Spyware + Anti Bot + DoS/DDOS + All signature enabled + Logging enabled + Bidirectional inspection + File Blocking. OEM to provide publicly available The Test methodology and result should be compliant to the benchmark testing methodology for the above parameters provided in the Internet Engineering Task Force (IETF)- 'Benchmarking Methodology for	Request below modified clause be considered , instead of Appmix traffic , real world traffic should be mentioned for deriving throughput "The proposed firewall must provide minimum 10 Gbps of Threat prevention throughput with Real world traffic. (Throughput must be derived from real world traffic and not Video/JPEG based traffic) (enterprise testing condition). The throughput must remain 10 Gbps even after enabling NGFW + IPS/IDS + Antivirus + Anti Spyware + Anti Bot + DoS/DDOS + All signature enabled + Logging enabled + Bidirectional inspection + File Blocking. OEM to provide publicly available The Test methodology and result should be compliant to the benchmark testing methodology for the above parameters provided in the Internet Engineering Task Force (IETF)- 'Benchmarking Methodology for Network Security Device	instead of appmix traffic real world traffic will be rifht measure of throuhgput , so requesting the change	No Change
310	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #21	NGFW appliance must be capable of handling minimum 2 M concurrent sessions utilizing HTTP transactions with all Security feature Turned ON and not based on UDP / Lab environment / ideal testing environment, this claim has to be supported with declaration of concurrent connections claim from OEM	Request below modified clause to accomodate support for 5M concurrent sessions NGFW appliance must be capable of handling minimum 5 M concurrent sessions utilizing HTTP transactions with all Security feature Turned ON and not based on UDP / Lab environment / ideal testing environment, this claim has to be supported with declaration of concurrent connections claim from OEM	Mid/Large scale deployments need higher concurrent session support and baselining this to 50 Lakh concurrent sessions will be in the interest of the Bank , so the requested change	No Change, additional feature will consider as value add
311	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #49	Solution should support creation of minimum 1 virtual context / instance from Day-1 without any compromise on system performance and network bandwidth.	Solution should support creation of minimum 5 virtual context /instance from Day-1 without any compromise on system performance and network bandwidth.	Support for only 1 Virtual context may not be scalable for the DC design and min support for 5 instances is the need for any DC infra Perimeter Firewall understanding furture state architecure and growing needs.	No Change, additional feature will consider as value add

| 312 | NA | Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #54 | The proposed NGFW solution architecture should have Control Plane separated from the Data Plane in the Firewall appliance architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup, QoS, NAT etc). Control plane must have dedicated resources such as CPU, RAM etc. This is to ensure Bank always has management access to NGFW irrespective of Firewall load / Traffic Spike / Cyber Attack driving higher CPU utilization. Bank should able to login to the firewall and carry out reporting / | | Request below modified clause be considered

The proposed NGFW solution architecture should have Control Plane separated from the Data Plane in the Firewall solution architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup, QoS, NAT etc). Control plane must have dedicated resources such as CPU, RAM etc. This is to ensure Bank always has management access to NGFW irrespective of Firewall load / Traffic Spike / Cyber Attack driving higher CPU utilization. Bank should able to login to the firewall and carry out reporting / management / packet capture etc to identify the root cause and accordingly take necessary action to remediate it. | OEMs have different approaches to achieving the use case and instead of the ask on the appliance itself , the Firewall Solution will be a generic term to use in requirements so this suggestion | No Change |
| 313 | NA | Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #72 | IPS should provide detailed information on each protection, including: Vulnerability and threat descriptions, Threat severity, Performance impact, Release date, Industry Reference, Confidence level etc. | | Request below changed clause :

IPS should provide detailed information on each protection, including: Vulnerability and threat descriptions, Threat severity, Release date, etc | Performance impact, industry reference and confidence level are subject to configuration and infrastructure in the bank. | No Change |
| 314 | NA | Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #76 | Should have more than 60+ predefined Categories based on Urls, Application types, Security Risk level etc. However solution should be able to create custom categories for URL and application. | | Request below modified clause with increased number of categories:

Should have more than 80+ predefined Categories based on Urls, Application types, Security Risk level etc. However solution should be able to create custom categories for URL and application. | Having more predefined categories support would help bank with improved threat detection and better granular policy control with less manual effort. | No Change, additional feature will consider as value add |
| 315 | NA | Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #89 | Solution should give information related to Performance impact and confidence level of protections while creating profiles. | | Request this clause be deleted | performance can be subject to policy configurations and existing infra at bank. | No Change |

316	NA	Appendix02 Techno Functional Requirements-Network components > perimeter FW Specifications Point #114	"Management server should support the following for rule optimization: • Unused Rules Calculation for specific time-period based on Firewall Traffic Logs. • Analysis on Covered/Shadow/Hidden Rules • Analysis on Rules Consolidation (Merging of similar kind of rules) • Analysis on Redundant Rules • Tightening of Overly Permissive Rules (Any-Any) • Analysis on Unattached/Unused Objects to simplify objects management • Analysis on Rule-Reordering to improve the performance of the Firewall • Analysis on Disabled/Expired Rules for enhanced visibility on the Firewall Rules sets"		"Management server should support the following for rule optimization: • Unused Rules Calculation for specific time-period based on Firewall Traffic Logs / HIt count • Analysis on Covered/Shadow/Hidden Rules • Analysis on Redundant Rules • Analysis on Unattached/Unused Objects to simplify objects management • Analysis on Disabled/Expired Rules for enhanced visibility on the Firewall Rules sets"	OEMs could be handling the use case suggested for removal differently or have no dependency on the performance of the Firewall , so requesting these be removed from the ask	No Change
317	NA	Appendix02 Techno Functional Requirements-Network components > IPS Features Point #15	Should support more than 3000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness		Should support more than 5000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness	Increasing number of signature support is beneficial for the Bank's operations and for Effective Security reasons	No Change
318	NA	Appendix02 Techno Functional Requirements-Network components > internal FW Point #11	The Firewall solution Should support more than 4000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness and should be able to create 40 or more application categories for operational efficiency. Dedicated IPS solution shall be in corporated by the bidder to achive this scale of IPS AVC signatures in this solution.		Request this clause be modfied as below:

The Firewall solution Should support more than 6000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness and should be able to create 40 or more application categories for operational efficiency. Dedicated IPS solution shall be in corporated by the bidder to achive this scale of IPS AVC signatures in this solution. | Increasing number of signature support is Beneficial for the Bank's operations and for Effective Security reasons | No Change, additional feature will consider as value add |
| 319 | NA | Appendix02 Techno Functional Requirements-Network components > internal FW NG Firewall Features NEW POINT | New Point to be added | | The solution should provide Change Management capability for the organizations needs to implement more formal processes for configuration changes, including audit tracking and official approval before changes are deployed. | By leveraging these features and integrating with external change management tools, organizations can implement a robust change management process that includes formal approval, audit tracking, and compliance reporting within Cisco FMC. | No Change |

320	NA				The solution should provide traffic hit count, Rule Conflict Detection (Redundant & Shadowed) and policy warning for streamlining firewall policies.	These features are crucial for optimizing firewall policies, ensuring efficient traffic flow, and maintaining security posture.	No Change, additional feature will be consider as value add
321	NA	Appendix02 Techno Functional Requirements-Network components > internal FW Hardware Architecture Point #3	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 8x64 GB of RAM.		Request below modified clause be considered as correction on the ask which seems typo: 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.		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.
322	NA	Appendix02 Techno Functional Requirements-Network components > Mngmt Switch 6 Product Support Point #2	The OEM support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support		Request below modified clause be considered The OEM/OEM certified partner support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support	OEM Certified partner has thorough experience of OS version upgrades and maintaining network operations troubleshooting issues and it will be cost effective to include this in the ask	The OEM/OEM certified partner support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support
323	NA	Appendix02 Techno Functional Requirements-Network components > Mngmt Switch 9 Miscellaneous Points Point #1	Console cable and power cable (As per Indian standards) as per customer requirement to be provided. All Cables shall be factory-terminated.		Since Console Cables are common for all devices per OEM , Request Bank to clarify the count of console cables to be provided , is it one each with each Switch or one per DC and DR Each ?.		No Change
324	NA	Appendix02 Techno Functional Requirements-Network components > Mngmt Switch 10 Product Support Point #2	The OEM support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support		Request below modified clause be considered The OEM/OEM certified partner support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support	OEM Certified partner has thorough experience of OS version upgrades and maintaining network operations troubleshooting issues and it will be cost effective to include this in the ask	The OEM/OEM certified partner support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support
325	NA	Appendix02 Techno Functional Requirements-Network components > Core Swtich >9 Manageability > Appliance point 9.4	Switch Anomolies related with Advisories , PSIRT and Field Notices		Request this clause be removed from the telemetry asks	This feature is not requireed for the design at the BOB DataCenter and may be removed	No Change
326	NA	Appendix02 Techno Functional Requirements-Network components > Core Swtich >13 Fabric Management > Appliance point 13.1	Solution must provide Centralized Management Appliance – Single pane of glass for managing, monitoring and provisioning the entire Solution within Data Center & across all Data Centers		Request BOBCards to provide VM compute resources for spinning up the VMs to provide this functionality while we can provide the necessary sw and support.		Requested product functionality should be comply, BOBCards will provide VM compute resources for spinning up the VMs to provide this functionality however bidder should provide the necessary sw and support.
327	NA	Appendix02 Techno Functional Requirements-Network components > Core Swtich >5 Layer 2 Features > Appliance point 5.11	Switch Hardware should have capability to support BGP EVPN Route Type 1, Type 2, Type 3, Type 4, Route Type 5, Type 6/Type 7/Equivalent routes		Request this point be removed	BOBCards design doesn't have Fabric so this is not applicable	No Change

328	NA	Appendix02 Techno Functional Requirements-Network components > Core Swtich >13 Fabric Management > Appliance point 13.36	Solution should provides reports using predefined templates, including inventory, use, and health reports.		Request below modified clause be considered: Solution should provides reports including inventory, use, and health reports.		No Change
329	IPS / Platform Requirement	3	The device should have functionality of in-built hardware based fail-open & software fail-open		As per our understanding, the device should support Layer 2 fallback functionality and not a bypass NIC card at hardware, which provides seamless traffic in case of appliance failure. "Is our understanding correct?		No Change
330	IPS / Performance & Scalability	3	The appliance should support 8x1G Copper ports and 8*10G SFP+ ports on board plus option of having another 1/10G port 8 numbers for expansion		The requirement is for 5 Gbps throughput and there are many ports asked in the RFP, So request to remove additional ports requirements.	Reuest for change "The appliance should support 8x1G Copper ports and 8*10G SFP+ ports on board".	another 1/10G port 8 numbers for expansion will be consider as value add
331	IPS / Features	15	Should support more than 3000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness		IPS solution provides IPS signatures including applications, vulnerabilities..ect.. IS there any specific reason to ask seperately 3000 sigantures for applications	Request for deletion	No Change
332	IPS / Features	16	Should support more than 50,000 (excluding custom signatures) IPS signatures or more		This is vendor specific, as there is only one OEM provides 50,000 + IPS signatures. So request to change it to at least 20,000+ IPS signatures	Request for change "Should support more than 20,000 (excluding custom signatures) IPS signatures or more".	No Change
333	IPS / Management	1	The management platform must be accessible via a web-based interface and ideally with no need for additional client software		The management platform provides ease of operational administrattion. It should not depend on the way to get access to the management platform, so request to remove "ideally with no need for additional client software".	Request for deletion	No Change
334	IPS / Management	3	The management appliance should have 2 x 1G and 2*10G port and integrated redundant power supply from day one		As per experience, most organizations have dedicated management zone and run with 1G port. Is there any specific reason to ask 10G port for the management appliance?	Request for deletion	10G is for uplink
335	IPS / Management	6	The management platform must domain multi-domain management		Please provide more clarity for multi domain management		IPS solution should manage multiple domains belongs to the BOBCARD
336	ernal Firewall Section 1 - NG Firew	8	Should have the capability of passively gathering information about virtual machine traffic, network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance.		Host information like IP address, OS, MAC etc can be detected by Firewall Also, applications being access by host will be visible in Web filter logs. However, Open ports and vulnerabilities are usually inspected by 3rd party assessment tools and not by Firewall. Firewall can inspect traffic and detect if vulnerabilities are getting exploited by applying IPS signatures, Web filters and find exploitation attempts like C&C connections etc.	Hence request you to modify this clause as following Should have the capability of passively gathering information about virtual machine traffic / network hosts and their activities, such as operating system, services & ports being accessed, applications being accessed to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance.	Should have the capability of passively gathering information about virtual machine traffic / network hosts and their activities, such as operating system, services & ports being accessed, applications being accessed to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance
337	Internal Firewall Section 6 - Performance & Scalability	1	Shall support minimum 5 Gbps of NGFW throughput (Firewall + Application Visibility Control)		As there are IPS and malware inspection features also asked in the RFP specs, throughput requirement should be considered along with IPS, App control and AV, Malware inspection services, hence request you to modify this clause as below	Hence request you to modify this clause as following Shall support minimum 5 Gbps of threat prevention throughput (Firewall + Application Visibility Control + IPS+ Antivirus+ AntiMalware)	No Change, additional feature will be consider as value add
338	Internal Firewall Section 6 - Performance & Scalability	2	Solution should support at least 1.5 million concurrent sessions with Application Visibility Control.		Considering the throughput asked in the RFP specs, concurrent sessions support should be on higher side. This will ensure that Firewall would not compromise during the DDOS attack as it will have enough state table (concurrent connections and sessions per sec) to accomodate DDOS attack	Hence request you to modify this clause as following Solution should support at least 5 million concurrent sessions	No Change

339	Internal Firewall Section 6 - Performance & Scalability	3	Solution should support at least 90,000 new connections per second with Application Visibility Control.		Considering the throughput asked in the RFP specs, concurrent sessions support should be on higher side. This will ensure that Firewall would not compromise during the DDOS attack as it will have enough state table (concurrent connections and sessions per sec) to accomodate DDOS attack	Hence request you to modify this clause as following Solution should support at least 400,000 new connections per second	No Change, additional new connection per second will be consider as value add
340	Internal Firewall Section 1 - NG Firewall	9	The Firewall solution Should support more than 4000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness and should be able to create 40 or more application categories for operational efficiency. Dedicated IPS solution shall be in corporated by the bidder to achive this scale of IPS AVC signatures in this solution.		Every OEM has their own methods of creating application signatures and seggregating them into different categories. Custom application signatures can be created on Fortigate, however categorization of signatures is done by threat intelligence engine i.e. Fortiguard.	Hence request you to modify this clause as following The Firewall solution Should support more than 4000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness. Dedicated IPS solution shall be in corporated by the bidder to achive this scale of IPS AVC signatures in this solution.	No Change, if required any additional component bidder can add it
341	Internal Firewall Section 1 - NG Firewall	10	Should be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention.		IPS signature tuning is typically done by threat intelligence engine as it requires large amount of resources like malware samples/IOCs etc.	Request you to modify this clause as below - Should be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) using threat intelligence engine with minimal human intervention.	No Change
342	Internal Firewall Section 1 - NG Firewall	11	The firewall solution should support at least 30,000 out of the box IPS signatures from Day 1. Should support capability to configure correlation rule where multiple rules/event can be combined together for better efficacy. Dedicated IPS solution shall be in corporated by the bidder to achive this scale of IPS signatures in this solution.		Every OEM has their own language for creating signatures and ways to optimize the number of signatures hence comparing number of signatures will not help to identify effectiveness of a Firewall. Instead, you can ask for 3rd party reports for testing Firewall effectiveness and performance. Also, dedicated IPS solution is asked in RFP, so please confirm whether IPS features needs to be considered for internal Firewall or not.	Request you to modify this clause as below- The firewall solution should support minimum 18,000 out of the box IPS signatures from Day 1. Should support capability to configure correlation rule where multiple rules/event can be combined together for better efficacy. Vendor should also ensure security effectiveness of the proposed solution to protect BOB's environment by providing 3rd party security testing reports like Cyber ratings / NSS labs	No Change
343	Internal Firewall Section 4 - Management platform and support	2	The management platform must be a dedicated OEM appliance and VM running on server will not be accepted.		It is recommended to use a Virtual machine as it provides ability to scale it in future when number of devices managed by management device increases. Hardware appliance will have a fix number of capacity in terms of devices being managed by it, which cannot be increased further.	Request you to modify this clause as below The management platform must be a dedicated OEM appliance or VM running on server. Required server hardware / resources should be provieded by the bidder.	No Change
344	Internal Firewall Section 4 - Management platform and support	4	The management appliance should have integrated redundant power supply from day one.		It is recommended to use a Virtual machine as it provides ability to scale it in future when number of devices managed by management device increases. Hardware appliance will have a fix number of capacity in terms of devices being managed by it, which cannot be increased further.	Request you to modify this clause as below In case OEM hardware appliance for management is proposed, it should have integrated redundant power supply from day one.	No Change
345	Internal Firewall Section 4 - Management platform and support	5	The management platform must be able to store record of at least 600,000 users or hosts.		Logging solution is sized based on the logs getting generated on Firewalls per day.	Request you to provide the expected log size getting generated on Firewall on per day bassis. (e.g 10 Gb, 50 Gb etc)	It is clearly call out in appendix 2, point no 23 of Management Platform and Support

346	Internal Firewall Section 5 - Hardware Architecture	2	The appliance should support 8x1G Copper ports and 8*10G SFP+ ports on board plus option of having another 1/10G port 8 numbers for expansion		Considering the throughput asked in the specifications, number of ports ask is on very higher side. These many number of 10G ports are typically supported on appliances more than 10 Gbps Threat prevention capacity.	Request you to modify this clause as below The appliance should support 8x1G Copper ports and 8*10G SFP+ ports on board plus option of having additional copper 1G port x 8 numbers for expansion or inbuilt additional 1G copper x 8 ports from day 1	another 1/10G port 8 numbers for expansion will be consider as value add
347	Internal Firewall Section 5 - Hardware Architecture	3	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 8x64 GB of RAM.		Every OEM has a different hardware architecture and different ways of utilizing hardware resources like RAM / Flash. RAM and CPU are not sizing parameters for any Firewall, it is usually considered for servers and storage.	Request you to modify this clause as below 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 16 GB of RAM.	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.
348	Internal Firewall Section 5 - Hardware Architecture	5	The appliance shall have redundant and hot swappable power supply and fan(s) module(s).		Redundant / Hotswappable fans are specific to one OEM It is typically supported in very higher series appliances, hence request you to modify this clause	Request you to modify this clause as below The appliance shall have redundant and hotswappable power supply	No Change
349	Internal Firewall Section 1 - NG Firewall	28	Solution should be able to detect HTTP/3 and SMB over QUIC. Should detect applications over QUIC without enabling decryption. Should be able to assign access control rules based on the service detected over QUIC protocol.		It is recommended practice to enable SSL inpsection for better security controls, because some of the applications might not be detected without SSL inspection, regardless of any OEM technology. Most of the today's applications runs over http and https, hence it will make more sense to run http / https traffic over QUIC protocol for better performance for roaming devices.	Hence request you to modify this clause as below - Solution should be able to inspect and detect HTTP/3 and QUIC traffic. Should detect applications over QUIC. Should be able to assign access control rules based on the service detected over QUIC protocol.	Solution should be able to inspect and detect HTTP/3 and QUIC traffic. Should detect applications over QUIC. Should be able to assign access control rules based on the service detected over QUIC protocol.
350	Internal Firewall Section 1 - NG Firewall	29	Solution should be able to generate indications of compromise (IoC) connection events based unsafe client applications detected by the system. IoC events should be triggered for encrypted sessions, without decryption, generated from a host using a malicious client. The system should capture the following information in the event viewer/dashboard "such as IP address, MAC address, and OS information of the malicious host, and the timestamp of the suspicious activity". The feature should work with all the TLS versions including TLS 1.3		It is recommended practice to enable SSL inpsection for better security controls, because not all the applications or threats can be detected without SSL inspection, regardless of any OEM technology. Also, information like MAC address, OS information can be available provided Firewall has reachability to users at layer 2	Hence request you to modify this clause as below - Solution should be able to generate indications of compromise (IoC) connection events based unsafe client applications detected by the system. IoC events should be triggered for sessions generated from a host using a malicious client. The system should capture the following information in the event viewer/dashboard "such as IP address, and OS information of the malicious host, and the timestamp of the suspicious activity". The feature should work with all the TLS versions including TLS 1.3	No Change
351	Internal Firewall Section 1 - NG Firewall	30	Solution should be able to block malicious communications in encrypted traffic based on threat score without decrypting the traffic. Solution should be able to reassemble fragmented Client Hello packets for detection purposes.		Without decryption, any Firewall has limited visibility into applications and threats and such limited visibility can also lead to false positives.	Hence request you to modify this clause as below - Solution should be able to block malicious communications in encrypted traffic based on threat score. Solution should be able to reassemble fragmented Client Hello packets for detection purposes.	No Change

352	Internal Firewall Section 1 - NG Firewall	31		Solution should be able to identify flows which are extremely large (in total bytes) flows measured over a network link. These flows are larger than 1 GB/10 seconds. Solution should be able to bypass and throttle these flows.	This clause is specific to the OEMs which do not support or has performance impact when processing large flows. This feature may be required in future to support high bandwidth sessions for east-west traffic	Hence Request you to either remove this clause or modify this clause as below Solution should be able to identify flows which are extremely large (in total bytes) flows measured over a network link. These flows are larger than 1 GB/10 seconds. Solution should be able to process these flows.	No Change
353	Internal Firewall Section 3 - Anti-APT Fearures	1		Should support the capability of providing network-based detection of malware by checking the disposition of unknown files using SHA-256 file-hash or signature (update to be provided in 300 seconds) as they transit the network and capability to do dynamic analysis.	If Sandboxing solution is required, it is recommended to enable inline sandboxing so that firewall can hold the file till the time Sandbox returns the verdict. This way Firewall will be able to avoid patient zero infection.	Hence request you to modify this clause as below - Should support the capability of providing network-based detection of malware by checking the disposition of unknown files using SHA-256 file-hash or signature (update to be provided in 300 seconds) as they transit the network and capability to do dynamic analysis using onprem hardware based sandbox. For dynamic analysis for files, Sandboxing solution is required. Please provide the sandbox sizing details - - Files needs to be scanned per hr - Number of Sandbox appliance in DC and DR We recommed to include below specification for sandboxing - 1) The solution should include onprem sandboxing appliance at DC and DR with required hardware, software and licenses included from Day-1.	No Change
354	Internal Firewall Section 4 - Management Platform and Support	9		The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows.	3rd party vulnerability exposures are managed by Fortiguard threat intelligence database on continuous bassis and required signatures are automatically pushed to Fortigate devices. Hence request you to modify this clause as following	The proposed solution must be capable of detecting third party vulnerability exposure and apply required signatures to Firewall policies to protect internal servers / apps from getting expoited	No Change
355	Internal Firewall Section 4 - Management Platform and Support	15		The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows.	Every OEM has different ways of sizing the solution. And for any logging appliance there would always be log capacity that it can handle. Logging solution is sized based on number of logs received on per day basis.	Hence request you to modify this clause as below - Solution should be able to provide insights of hosts/user on basis of indicators of compromise, any license required for this to be included from day one.	No Change
356	13	3.1 Project Scope	16. L2 and L3 onsite support post implementation a. Software upgradation b. Hardware Upgradation c. Mass Changes for compliance d. Major, minor changes in feature/functionality roll out on the same infrastructure.		Please help with detail scope of works, also please confirmed whether bidder need to deploy the deicated L2 & L3 resources at BOBCARD site or bidder need to provide the L2 / L3 resources as and when required by BOBCARD		Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
357	37	Data Migration	The selected Bidder will assist the company in migration exercise without any cost to the company.		Please help whether we need to provide the technical guidance (as our understanding if Correct - Tha Bank will migrate the data and bidder needs to support for the smooth migration) or bidder need to provide the technical resource in the migration activites		Data migration will be in scope on bidder

358	Eligibility criteria point no 5		Bidder should have experience of minimum 3 years in providing the Proposed Products/Services mentioned in the RFP.		Requested BOBCARD to consider the bidder should have experience of minimum 5 years on providing the Products / Services	No Change
359	Eligibility criteria point no 6		Client references and contact details (email/ landline/ mobile) of customers for whom the Bidder has executed similar projects in India. (Start and End Date of the Project to be mentioned) in the past (At least 3 client references are required)		Requested BOBCARD to please consider the Client references and contact details (email/ landline/ mobile) of customers for whom the Bidder has executed similar projects in India. (Start and End Date of the Project to be mentioned) in the past (At least 1 to 2 client references are required)	No Change
360	technical evaluation criteria point no 1		The bidder should have supplied and installed similar to proposed hardware in last three (3) financial years, i.e. 2021-2022, 2022-23, 2023-24 (Bidder to provide details in Annexure K and submit PO / Contract details)		Requested BOBCARD to consider the bidder should have supplied and installed similar to proposed hardware in last Five (5) financial years, i.e. from 2019-20 to 2023-24	No Change
361	technical evaluation criteria point no 2		The bidder should have deployed and configured proposed software as per OEM standard on proposed hardware in last three (3) financial years, i.e. 2021-2022, 2022-23, 2023-24 (Bidder to provide details / submit PO / Contract details)		Requested BOBCARD to consider the bidder should have deployed and configured software as per OEM standard on Infra (HArdware / Software) in last five (5) financial years, i.e. 2019-2020 to 2023-24	The bidder should have deployed and configured proposed software as per OEM certified and standard hardware in last three (3) financial years, i.e. 2021-2022, 2022-23, 2023-24 (Bidder to provide details / submit PO / Contract details)
362	Appendix01 Techno Functional Requirements- Server and Virtual		The proposed solution should be a Hyperconverged infrastructure (HCI) with 5 years comprehensive warranty	Not having the option to use extenal storage limits customer's ability from leveraging existing/external storage for specific application requirement which may come in future or on going setup. These application then will have to be hosted in seprate infrastructure adding to cost and will create seprate silo to manage along with migration effort of existing data	The proposed solution should be a Hyperconverged infrastructure (HCI) with option to use external storage with 5 years comprehensive warranty	The proposed solution should be a Hyperconverged infrastructure (HCI) with an option to use as external storage
363		Appendix01 Techno Functional Requirements- Server and Virtual platform > Software Defined Storage > 14	The proposed solution should support Replication factor RF-2 (1 Node failure). Proposed Solution must be planned with N+1 without considering Dedup, compression, erasure coding at both DC and DR location.	RFP asks for 99.99 % availability SLA for the proposed solution. It will require minimum N+2 configuration. 99.99 % SLA would also require BoB Cards to consider four site (DC, DR , NDC and NDR) architecture along with streched cluster (both Infrastructire & kubernetes) between DC and NDC . Request Bob Cards to clarify the business impact of missing 99.99 % availability SLA. Is current setup also has 99.99 % availability ?	The proposed solution should support Replication factor RF-3 (2 Node failure). Proposed Solution must be planned with N+2 without considering Dedup, compression at both DC and DR location.	No Change, additional feature will be consider as value add
364		Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmentation > 1	The Solution should be capable of supporting major hardware OEMs like Juniper, Arista, Cisco, HPE and Dell. The proposed solution should be a purely software-based solution and should not be dependent on any hardware make and model.	The key benefits of no dependecy on hardware is by using software defined networking i.e overlay. Overlay is mandatory for network & Security automation as part of software defined data center.	The Solution should be capable of supporting major hardware OEMs like Juniper, Arista, Cisco, HPE and Dell. The proposed solution should be a purely software-based solution and should not be dependent on any hardware make and model by creating overlay tunnels between the hosts.	No Change, additional feature will be consider as value add

365	Appendix01 Techno Functional Requirements- Server and Virtual pla	The solution should provide a distributed firewall such that the firewalling for Virtual Machines can be provided closest to the application within the server itself without traffic going to a Physical Firewall.		*As per security framework its recommended not to use standard ports for your applications and hence to have effective security on per VM basis an application/L7 firewalling is must.* Containers & Kubernetes are now part of all modern applications hence networing and security for container shall also be considered for end to end application security. there is App ID requirement is mentioned in RFP as part of "Internal Firewall" spec point # 23 hence same should be considered for mirosegmenation as well otherwise it will create non standard architecture.	The solution should provide a distributed firewall such that the application aware and identity based statefull firewalling for Virtual Machines can be provided closest to the application within the server itself without traffic going to a Physical Firewall or regardless of underlying L2 Netwrork topology. The solution should also provide an integrated networking solution (CNI implementations) as well as provide advance turnkey container networking & firewalling services. Solution should support for container networking plug-ins, support for pod to pod communication and support for ingress controllers. The micro-segmentation solution should have a capability for stateful firewalling and ALGs (Application Level Gateway) on a per-workload granularity regardless of the underlying L2 network topology (i.e. possible on either logical network overlays or underlying VLANs), embedded in the hypervisor kernel, distributed across entire environment with centralized policy and management	No Change
366	Appendix01 Techno Functional Requirements- Server and Virtual pl	The proposed solution should provide the ability to define firewall rules at VM level for east-west traffic in order to implement Zero Trust Security		Zero trust Security framework mandates TLS inspection for encrypted traffic, URL Filtering and Layer 7 application firewalling.	The proposed solution should provide the ability to define Layer 7 application firewall rules at VM level for east-west traffic in order to implement Zero Trust Security alongwith URL Filtering and TLS inspection for encrypted traffic	No Change, additional feature will be consider as value add
367	Appendix01 Techno Functional Requirements- Server and Virtual pl	The Proposed Solution including Hypervisor, SDS, SDN and Micro segmentation must be from the same OEM.		SDN is missing in the spec, SDN will be mandatory to create complete automated Software Defined data center by creating an abstraction of the network enabling programming of network behavior in a centrally controlled manner through software applications.	The Proposed Solution including Hypervisor, SDS, SDN and Micro segmentation must be from the same OEM.	No Change, additional feature will be consider as value add
368	Appendix01 Techno Functional Requirements- Server and Virtual pl	The proposed solution should allow users to define granular firewall rules based on IP Addresses, Tags/Categories and Subnets to segment User Applications		Its necessary to have dynamic security group capability to ensure complete automation. RFP page 8 -> 2.0 --> Requirement Summary--> 2.1 Intent--> mentions requirement for IPv6 "The proposed solution should support both IPv4 and IPv6."	The proposed solution should allow users to define granular firewall rules for both VM and conatiners based on IP Addresses, VM Names, Tags/Categories and Subnets to segment User Applications by creating dynamic security groups. The solution should have capability to provide stateful micro-segmentation for virtual machines and Kubernetes workloads from a single console. The solution should also support enforcement of stateful distributed firewall for IPv6 VM workloads. These firewall rules can use IPv6 addresses, IPv6 CIDR, IP Sets that include both IPv4 and IPv6 addresses and security groups that can include logical ports that have both IPv4 and IPv6 addresses. IPv6 capability should be available both at management and data plane	No Change
369	Appendix01 Techno Functional Requirements- Server and Virtual pl	Solution should provide capability to create network segments by defining them entirely in software and avoid the need to re-architect your network or deploy physical appliances		L2 Streching is required for better application availability considering RFP asks for 99.99 % availability on monthly basis. RFP Page 17 -> "4. Service Levels "-->"SLA: The solution is expected to be available for 99.99% on 24x7 and up time availability will be calculated on monthly basis."	Solution should provide capability to create network segments and L2 Streching between DC and DR by defining them entirely in software and avoid the need to re-architect your network or deploy physical appliances	No Change, L2 stretching implementation will be discuss with elected bidder.

370	Appendix01 Techno Functional Requirements- Server and Virtu	The solution must be able to manage Kubernetes clusters. Licenses for managing Kubernetes clusters should be implemented from Day-1		Kubernetes Cluster doesn't work in isloation but require other components such as container registry and backup solution. If not included than Bob Card will have procure them separately. And Not aving Windows Container support will block any windows based apps to be deployed on Kubernetes Platform.	The solution must be able to manage Kubernetes clusters. Licenses for managing Kubernetes clusters along with components such as backup, container registry aving monitoring alongwith Windows Container support should be implemented from Day-1	Yes, BOBCARD will take care such requirement
371	Appendix01 Techno Functional Requirements- Server and Virtu	Must have provisioning, operations and lifecycle management of Kubernetes, automated deployment, scaling, and operation of Kubernetes clusters		Complete Automation is not possible without Auto Scaling and Auto Healing of Kubernetes Clusters. One has to manually add nodes in case of failure or unprovisioned increase in load.	Must have provisioning, operations and lifecycle management of Kubernetes, automated deployment, Auto scaling & Auto Healing, and operation of Kubernetes clusters	Must have provisioning, operations and lifecycle management of Kubernetes, automated deployment, Auto scaling & Auto Healing, and operation of Kubernetes clusters
372	Appendix01 Techno Functional Requirements- Server and Virtu	Container Platform should provide single pane of Glass for Lifecycle Management of all K8S clusters deployed on prem.		Kubernetes Cluster doesn't work in isloation but require other components such as container registry and backup solution. These shall too be considered for life cycle management	Container Platform should provide single pane of Glass for Lifecycle Management of all K8S clusters alongwith ingress, backup and container registry deployed on prem.	No Change, additional feature will be consider as value add
373	Appendix01 Techno Functional Requirements- Server and Virtual pla	The solution should provide capability of generating reports for usage, performance, compliance, health, forecasting and capacity.		Bob Cards will need capacity optimization capabilities to identify over-provisioned & under-provisioned resources and provide recommendations, alerts and automated actions on right-sizing and resource consumption so they can be right-sized for adequate performance and avoid resource wastage. Should provide visibility of capacity and VMs which can be reclaimed and cost visibility of the reclaimed capacity and VMs.	The solution should provide capability of generating reports for health, Capacity Optmization - Right Sizing (Under sized, Oversized), Reclamation (Idle, Powered off , Snapshot, Orphaned Disk , Forecasting - Capacity Forecasting, Migration assessment, Migration Planning Usage - Process and service utlization Compliance - Regulatory Benchmark (PCIDSS and ISO) Security Guidelines for Infrastructure and Cloud Management	No Change, additional feature will be consider as value add
374	Appendix01 Techno Functional Requirements- Server and Virtual pla	The solution should have intelligent operations with anomaly detection which will allow monitoring seasonal trends and automatically send email alert		BoB Cards will not be able to manage the infrastructure without comprhesive log management capability. Its also mandatory for from regulation/compliance perspective to have log stored for given period of time for audit. BoB Card would need apps (database and Application) to infra (Server, Storage , Network) level visibility for toubleshooting and performance monitoring.	The solution should have AI/ML driven intelligent operations & troubleshooting workbench with anomaly detection,third party infra (Server, Storage , Network, database and Application) along with parent child relatiohship mapping, service and process monitoring which will allow monitoring seasonal trends and automatically send email alert. The solution should also have log management capability for infrastructure and applications . log management solution should delivers intuitive, actionable dashboards, sophisticated analytics, and broad third-party extensibility across physical, virtual, and cloud environments.	Compliance - Regulatory Benchmark (PCIDSS and ISO)
375	Appendix01 Techno Functional Requirements- Server and Virtual pla	The solution must have an approval process to review, reject or approve the deployment requests from the marketplace.		The solution must have an approval process to review, multi level & auto reject or approve the deployment requests from the marketplace.	Bob Cards would need multiple levels of approval with E-mail notifications with ability to automate manual provisioning and de-provisioning of the tasks and policies embedded in each layer of their application including auto -approve and auto-reject capability based on application criticality	No Change, additional feature will be consider as value add
376	Appendix01 Techno Functional Requirements- Server and Virtua	Hypervisor should support container and opensource integration for cloud native application from day-1. Must be a Kubernetes ready from day-1.		Kubernetes does't work in isolation and requires multiple components for production setup.	Hypervisor should support container both Linux and Windows along with other kubernetes ecosystems such as container registry, backup, ingress & monitoring and opensource integration for cloud native application from day-1. Must be a Kubernetes ready from day-1.	Yes, BOBCARD will take care such requirement

#					
377	Appendix01 Techno Functional Requirements- Server and Virtual	Virtualization Manager should provide feature which can perform quick, as-needed deployment of additional virtualized hosts. When the service is running, it can push out update images, eliminating patching and update without impacting production.		Please clarify the scenario "When the service is running, it can push out update images, eliminating patching and update without impacting production." Its not clear from the language as what is the expected outcome.	Virtualization Manager should provide feature which can perform quick, as-needed deployment of additional virtualized hosts. When the service is running, it can push out update images, eliminating patching and update without impacting production. Proposed solution should allow live patching of select critcal security patches.	Virtualization manager should allow addition of new nodes and patching/upgrade of hypervisor running on the node without any VM downtime.
378	Appendix01 Techno Functional Requirements- Server and Virtua	Unlimited VM replication from DC to DR (No restriction on VM replication and DR orchestration) with the capability to define Recovery Plans		Unlimted is open terms, request you to provide the number of VMs to orchestrated for automated recovery. As unlimited is relevant for one specific vendor . The VMs to be protected/orchestrated are limited to what can be provisioned on these 14 servers of production.	Request BoB cards to Clarify the need for Recovery Plans- We do provide unlimited Replication from DC to DR which is orchestrated. In Terms of Recovery Plans (which is automation) We request bank to consider defining specific number of Virtual Machines. Its however best to use extends the existing DR orchestration solution fot this environment as well.	No Change, can not predict the exact number of VMs for next 5 Years which need to be replicated.
379	Appendix01 Techno Functional Requirements- Server and Virtua	Proposed solution should have a self-service restore feature on a per-VM basis to allow trusted application administrators to recover their own files with the ability to mount snapshots as a drive in Windows VMs		Please clarify this requirement, this looks like back and restore requirements	Proposed solution should have a self-service restore feature on a per-VM basis to allow trusted application administrators to recover their own VMs from the snapshot	This will help BOBCARD to recover file without losing current state of virtual machine.
380	Appendix01 Techno Functional Requirements- Server and Virtua	Hypervisor should provide Visibility for Running VM and their connectivity co-relationship with Network Ports on attached Physical TOR / Core Direct which Include Network RX/TX Bytes.		Monitoring is not considering all components of the stack. Unless end to end visibility is provided as part of this solution BoB Card has to spend separately on monitoring.	Hypervisor should provide Visibility for Running VM and their connectivity co-relationship with Network Ports on attached Physical TOR / Core Direct which Include Network RX/TX Bytes.Solution Should provide end to end visibility across physical firewall, switch and storage, Flow Analysis and Security Planning,Guided Troubleshooting, Microsegmentation planning, RCA (Connectivity Problem, Packet Loss, N/W latency), Application Discovery, Service Monitoring , Application Dependency Mapping and monitoring of non compliant ports	Yes, BOBCARD will take care such requirement. However Hypervisor should provide Visibility for Running VM and their connectivity co-relationship with Network Ports on attached Physical Port which Include Network RX/TX Bytes.
381	Appendix01 Techno Functional Requirements- Server and Virtua	Virtualization software or the solution should provide Cluster level encryption protects unauthorized data access at-rest.		Having capability to do the enscryption at app VM level and in transit is required to complete solution.	Virtualization software or the solution should provide Cluster level, VM Level encryption protects unauthorized data access at-rest and in transit.	No Change, additional feature will be consider as value add
382	Appendix01 Techno Functional Requirements- Server and Virtual platfo	Maintain primary working set copy of active data on the Local Node as VM's are hosted to provide high IOPS and low latency. Proposed solution must be proposed for faster reads and write for Business-critical Apps.		Architecture is specific to one vendor, request BoB Cards to consider on outcome than specific architecture. There is no specific latency requirements mentioned in the spec.	Proposed solution must be proposed for faster reads and write for Business-critical Apps.	No Change
383	Appendix01 Techno Functional Requirements- Server and Virtual platfo	The solution must have De-duplication and Compression features licensed and implemented from day one (Should not have dependency on any proprietary hardware device).		Solution should have flexibility to implement either compression and de-duplication. BoB Cards should conisder overhead while deciding on both.	The solution must have De-duplication/Compression features licensed and implemented from day one (Should not have dependency on any proprietary hardware device).	No Change
384	Appendix01 Techno Functional Requirements- Server and Virtual platfo	The proposed solution should support 1 min RPO & 1 hour RTO for critical workload in case BOB Cards wants to have this capability replication for Future use. The proposed solution should have native Replication and DR Orchestration from Day-1		What is the use case for 1 min RPO and 1 Hour RTO? is this linked with some regulatory requirement? Replication is best handled at application level as having additional solution for infrastructure will complexity and cost for BoB Cards Its best to use extends the existing DR orchestration solution for this environment as well.	What is the use case for 1 min RPO and 1 Hour RTO? is this linked with some regulatory requirement? Replication is best handled at application level as having additional solution for infrastructure will complexity and cost for BoB Cards Its best to use extends the existing DR orchestration solution for this environment as well.	This is required for BOBCARD mission critical application. The solution should capable to support 1min RPO. The propose replication solution should be same OEM as the virtualization solution to provide seamless integration.
385	Appendix01 Techno Functional Requirements- Server and Virtual platfo	The solution provided should function even after one node failure.		RFP asks for 99.99 % availability SLA for the proposed solution. It will require minimum N+2 configuration for required resiliency and uptime.	The solution provided should function even after two node failure.	No Change, additional feature will be consider as value add

#			Requirement		Comment	Revised	Response
386			Appendix01 Techno Functional Requirements- Server and Virtual platfor	The solution should provide enterprise data services such as compression completely in software. Software Defined Storage solution must have de-duplication and compression features Licensed and implemented from day one. These functionalities should be part of the proposed solution. The solution must have functionality to support compression and or deduplication online on data container without any downtime and data loss as per business requirement.	Solution should have flexibility to implement either compression and de-duplication. BoB Cards should conisder overhead while deciding on both.	The solution should provide enterprise data services such as compression completely in software. Software Defined Storage solution must have de-duplication or compression features Licensed and implemented from day one. These functionalities should be part of the proposed solution. The solution must have functionality to support compression and or deduplication online on data container without any downtime and data loss as per business requirement.	No Change
387			Appendix01 Techno Functional Requirements- Server and Virtual platfor	New Point	IP/MAC spoofing is major security concern for organizations like BoB Cards handing customers data.	The solution must ensure that there is not alteration in the IP address of the Virtual machine, by blocking the traffic from or to the VM inherited as a feature in the Solution.	No Change
388			Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmentation > new point		VPC will enable Bob Cards to create isolation from access , resources, network and security.	The solution should support multi-tenancy to isolate networking/security for different departments/function within BoB Cards upto a minimum of 4 tenants and 5 VPCs	No Change, additional feature will be consider as value add
389			Appendix01 Techno Functional Requirements- Server and Virtua	Should support cluster scale out i.e addition of worker nodes as and when required.	Complete Automation is not possible without Auto Scaling and Auto Healing of Kubernetes Clusters. One has to manually add nodes in case of failure or unprovisioned increase in load.	Should support Automated cluster scale out i.e addition of worker nodes as and when required.	No Change
390			Appendix01 Techno Functional Requirements- Server and Virtual pla	The solution shall provide a single pane of glass for automated provisioning with model-based orchestration of compute, network and storage through a unified multi-tenant self-service catalog.	All modern applications are combination of both container and VM form factor.	The solution shall provide a single pane of glass for automated provisioning with model-based orchestration of compute, network , storage and Kubernetes through a unified multi-tenant self-service catalog .	No Change, additional feature will be consider as value add
391			Appendix01 Techno Functional Requirements- Server and Virtual pla	The solution must provide a self-service portal to allow user to consume the creation of infrastructure easily.	All modern applications are combination of both container and VM form factor.	The solution must provide a self-service portal to allow user to consume the creation of infrastructure easily for both VM and Kubernetes.	No Change, additional feature will be consider as value add
392			Appendix01 Techno Functional Requirements- Server and Virtual pla	The software must allow the designer to use shell script, PowerShell script to code the automation.	Python and nodeJs are very popular language for scrpting in terms resource availability and community support	The software must allow the designer to use shell script, PowerShell script, Python and node JS to code the automation.	No Change, additional scripting will be value add
393			Appendix01 Techno Functional Requirements- Server and Virtual pla	The software must allow the designer to design VM blueprints.	All modern applications are combination of both container and VM form factor.	The software must allow the designer to design Multi VM & Kubernetes blueprints.	No Change, additional feature will be consider as value add
394			Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > 12	The solution should have simple low-code, no-code automation engine which allows automating day-to-day routine tasks	All modern applications are combination of both container and VM form factor.	The solution should have simple low-code, no-code automation engine which allows automating day-to-day routine tasks such as Snapshot creation, Addition of Disk, Power Cycle (Suspend , Shutdown, Reboot, reset), Resize, Rebuild, Additional of Network, VM Unregister , Delete,connect remote console, Change Security Group with capability to create additional resource actions as out of the box capability.	No Change, additional feature will be consider as value add
395			Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > New Point	New Point	Cost transparency (Showback and Chargeback capability) across private, hybrid to optimize planning an	Solution should provide capability to define and showcase cost to create cloud like experience to the business unit with the overall cost spend on the infrastructure [server hardware, storage, licenses, application, maintenance, labor, network, facilities , etc.	No Change, additional feature will be consider as value add
396	12	7	The successful bidder should also integrate existing infrastructure setup (like existing LAN, proxy, MFA, SIEM) with the new devices to be supplied.	Clarification required: Please share the existing setup details to intigrate and also check compatiblity for intigration?		This will be market leading product only. Basis on compatibility Bidder has to integrate the existing infra setup with new setup. All the product will be share only with the final bidder

397	12	8	All required configuration to integrate with existing setup should be taken care of by bidder.		Clarification required: Please share the existing setup details to intigrate and also check compatiblity for intigration?		This will be market leading product only. Basis on compatibility Bidder has to integrate the existing infra setup with new setup. All the product will be share only with the final bidder
398	12	9	The successful bidder should suggest the appropriate IOS for all the supplied devices; the IOS should be of N-1 version.		Clarification required: Please sugest which IOS version mentioned here?		IOS latest stable available version at the time of deployment
399	37	Data Migration	The selected Bidder will assist the company in migration exercise without any cost to the company.		Clarification required: Please share if anydata migration to be done? If yes thennshare the details e.g what data migration and size of the data?		As mentioned in this corrigendum
400	13	16	L2 and L3 onsite support post implementation a. Software upgradation b. Hardware Upgradation c. Mass Changes for compliance d. Major, minor changes in feature/functionality roll out on the same infrastructure.		Clarification required: Please provide clarity on resource requirment? How many onsite resource required? Which technology and timing for the resource?		Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
401	Appendix02-Perimeter Firewall	15	Solution should have minimum 450 GB SSD pair, system storage		Requesting change as "SSD's are by default high performance drives with inbuilt resiliencey"	Request you to change the Point to "Solution should have minimum 450 GB SSD , system storage"	No Change
402	31	8. Payment Term	Activity: Supply of Servers & Network component as prescribed under hardware requirement. Timlines: Within 5-6 weeks from date of PO		Please change the delivery timelines to 8 to 10 weeks	Please change the delivery timelines to 8 to 10 weeks	Supply of Servers & Network component as prescribed under hardware requirement Within 6-8 weeks from date of PO. Rest all clause remain same
403	31	8. Payment Term	Activity: Completion of rack mounting of Servers & Network component and Configuration. Implementation of Software Timlines: Within 4-6 weeks post-delivery of servers & Network Component		Please change the delivery timelines to 8 to 10 weeks	Please change the delivery timelines to 8 to 10 weeks	Supply of Servers & Network component as prescribed under hardware requirement Within 6-8 weeks from date of PO. Rest all clause remain same
404	8	Requirements Summary	Acceptance: A one-month test period will be used by BOBCARD to evaluate the implemented Solution. After the implemented solution has been successfully tested, BOBCARD and the Bidder shall agree on the Go-LIVE date.		Requesting change testing period from 1 month to 1 week	Requesting change testing period from 1 month to 1 week	No Change
405	15	Appendix02-Perimeter Firewall	Solution should have minimum 450 GB SSD pair, system storage		Requesting change as "SSD's are by default high performance drives with inbuilt resiliencey"	Request you to change the Point to "Solution should have minimum 450 GB SSD , system storage"	No Change
406			The proposed solution should be capable of adding additional combined server and storage components, seamlessly, with node owntime, to scale performance and capacity on demand.		There seems to be a typo in this point:		The proposed solution should be capable of adding additional combined server and storage components, seamlessly, with no downtime, to scale performance and capacity on demand.
407	NA	Virtual Platform / Pt 30			Please confirm if the solution is expected to be capable of adding additional combined server compute and storage capacity with adding new nodes without any cluster downtime to scale the performance and capacity on demand	Revised point: "The proposed solution should be capable of adding additional combined server and storage components, seamlessly, with no downtime, to scale performance and capacity on demand."	The proposed solution should be capable of adding additional combined server and storage components, seamlessly, with no downtime, to scale performance and capacity on demand.

408	NA	Virtual Platform / Pt 2	The Bidder should provide 1 Technical Resource from Software OEM for a period of 1 Year to provide timely health check, suggest OEM best practice, conduct timely health check of the deployed solution and submit a report indicating OEM best practices.		Please confirm if the Onsite resource which has been asked for needs to be a HCI Software OEM resource		Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
409	NA	Appendix 03 Bill of Material / Optional commercial / Sr.no. 5	One year support cost of on site L3 resource (1 server & Virtual platform)				Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
410	12	8	All required configuration to integrate with existing setup should be taken care of by bidder		Need details for existing setup		This will be market leading product only. Basis on compatibility Bidder has to integrate the existing infra setup with new setup. All the product will be share only with the final bidder
411	12	9	The successful bidder should suggest the appropriate IOS for all the supplied devices; the IOS should be of N-1 version		Need details for existing setup. -- It seems to be (OS) but need clarification on IOS.		IOS latest stable available version at the time of deployment
412	13	16	L2 and L3 onsite support post implementation a. Software upgradation b. Hardware Upgradation c. Mass Changes for compliance d. Major, minor changes in feature/functionality roll out on the same infrastructure.		Required resource count		Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
413	10	2.5 Training	The Bidder is required to provide training to the BOBCARD team on the proposed solution in RFP for *Procurement of Servers, Network & Software components* , provide a training schedule and furnish training details as per the RFP requirements for all major components		Please clarify if this training is to be conducted by the bidder or the OEM.		One time Training need to be provided in BOBCARD Office inperson for implemented solution. Training can be given by OEM/Bidder, trainer must be certified resource.
414	14	29	BOBCARD shall accept the application software only after the critical or major Bugs are fixed.		Please specify which application		BOBCARD shall accept the Proposed Application, software's and Hardware only after the critical or major Bugs are fixed if any identified.
415	14		Application upgradation and patches management document		Bidder will only be responsible install and manage applications installed by the bidder as a part of the solution		Propose Software and Application upgradation and patches management document
416	11	3.1 Project Scope Point #1	The supplied Hardware and Software shall be of the latest versions and should not be end of life / end of support for the next 7 years.		Request the start Date for 7 Yrs mention in the clause be specified. Is it RFP Date or Date of PO Issuance/GoLive Date or something else?	Right tenure will help align the final BOM and any discrepent inpurs will impact pricing , so requesting clarification	The supplied Hardware and Software shall be of the latest versions and should not be end of life / end of support for the next 5 years from the date of delivery
417	12	3.1 Project Scope Point #4	All Software licenses effective date shall be effective as on Go-LIVE sign off or put in use for BOBCARD operations.		Contract Start period is mentioned as PO Issuance while the SW licenses effective date is mentioed as GoLive Sign off Dates as noticed. Request Bank to keep this synchronized if this is genuine or clarify the intent	Right tenure will help align the final BOM and any discrepent inpurs will impact pricing , so requesting clarification	License effectiveness should be start from the software is ready to use. License cost will not impact to BOBCARD due to implementation delay. No license activate without informing BOBCARD.

418	12	3.1 Project Scope Point #12	Hardware RMA (Return Merchandise Authorization) should be within 24 hours		Request this be modified as below Hardware RMA (Return Merchandise Authorization) should be within 24 hours on Next business Day Basis.	RMA for a request raised on Friday may be honored by Monday due to the weekend in between , so requesting to keep this clearly specified.	Hardware RMA (Return Merchandise Authorization) should be within 24 hours on Next business Day Basis.
419	19	5.3 Price Comparisons Point #c iv	End of Sales/ End of support: The Vendor has to ensure that any application, related software supplied / put to use as part of this RFP should not have reached end of support. In the event if any equipment supplied / put to use by the vendor reaches end of support, within the contract period from the date of use, the vendor has to replace the equipment/ software at no additional cost to the Company before end of support.		End of Life/End of Sale Clause here should specifiy the start date as to if PO issuance, RFP Date or any other . Further the tenure within which EOS/EOL should not happen must be mentioned like 7 years in clause Project Scope point #1	Right tenure will help align the final BOM and any discrepent inpurs will impact pricing , so requesting clarification	The supplied Hardware and Software shall be of the latest versions and should not be end of life / end of support for the next 5 years from the date of delivery
420	9	2.2 Tenure	The tenure of the contract initially would be for 1 year from the date of the issuance of first purchase order. BOBCARD can further extend to 2 years at its at mutually agreed terms.		Contract Tenure mentioend as 1 Year from PO Issuance here while its 3 years in clause 3.1 Point 17/ Pls clarify the right tenure?	Right tenure will help align the final BOM and any discrepent inpurs will impact pricing , so requesting clarification	Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
421	13	3.1 Project Scope Point #17	The initial term of this contract shall be 3 years and may be extended to another 2 years subject to satisfactory performance by successful bidder and OEM(s).		Mentioned here is 3 years of initial contract and in 2.2 section the contract mentioned is 1 Year/ pls clarify the right tenure	Right tenure will help align the final BOM and any discrepent inpurs will impact pricing , so requesting clarification	Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
422	30	7.2 Evaluation Methodology for Eligible Bidder Commercial Bid Evaluation	The key considerations of the TCO would be the total payouts for entire project through the contract period of 5 years.		Mentioned here is 5 years contract but in 2.2 the tenure of contrat is 1 Year, pls clarify the number to consider	Right tenure will help align the final BOM and any discrepent inpurs will impact pricing , so requesting clarification	Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
423	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Server Prod > HCI Rack Servers > 1	Total QTY is 14		Clarifictaion Needed: 1. Please provide split of quantity of servers / Nodes per location. 2. Kindly specify the number of clusters and nodes per cluster also.	clarifiction will help arrive at the boq rightly	This will be shared with only elected bidder
424	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Server Prod > HCI Rack Servers > 7	Each Rack Server Controller Cards / Controller Drive should be provided in HA mode in RAID -1.		Request Change: Each HCI Server should be configured with two BOOT drives with hardware RAID Controller. For NVMe storage drives: Provides as per Certifed HCI Node with NVMe configuration	From the HCI Rack server or Pre configured HCI NODE - RAID Controller card is not required for NVMe drives. Also, is this ask for Boot drive with RAID Controller?	Yes, we need boot drive for HCI hypervisor provided in HA mode in RAID -1

425	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Server UAT > HCI Rack Servers > 7	Each Rack Server Controller Cards / Controller Drive should be provided in HA mode in RAID -1.		Request Change: Each HCI Server should be configured with two BOOT drives with hardware RAID Controller. For NVMe storage drives: Provides as per Certifed HCI Node with NVMe configuration	From the HCI Rack server or Pre configured HCI NODE - RAID Controller card is not required for NVMe drives. Also, is this ask for Boot drive with RAID Controller?	Yes, we need boot drive for HCI hypervisor provided in HA mode in RAID -1
426	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Server Prod > HCI Rack Servers > 6	Each Rack servers should have minimum usable Storage Capacity of 10 TB of all caching SSD and other HDD. 20% disk slot on each node should be free for future expansion		Clarification needed: In virtualized environment, the storage (usable) capacity is calcluated across the cluster. Need clarification on the total capacity required across the number of nodes in a cluster.	clarifiction will help arrive at the boq rightly	as mentioned in RFP 10TB usable storage per node * no of node = total usable capacity
427	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Server UAT > HCI Rack Servers > 6	Each Rack servers should have minimum usable Storage Capacity of 10 TB of all caching SSD and other HDD. 20% disk slot on each node should be free for future expansion		Clarification needed: In virtualized environment, the storage (usable) capacity is calcluated across the cluster. Need clarification on the total capacity required across the number of nodes in a cluster.	clarifiction will help arrive at the boq rightly	as mentioned in RFP 10TB usable storage per node * no of node = total usable capacity
428	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Server Prod > HCI Rack Servers > 13 >Server Security	Request New Point to be added		Request to add the below point for security and management features for HCI Nodes Day2 operations and management of HCI Nodes for updates on Hardware and Software. HCI Node management tool should integrate with Virtual platform and Network switches. Should be able to do Firmware updates, Manage Cluster and deployment, Full stack visibility of HCI Node, TAC/Case Support, Continuous Health checks on Networking, Server, VMs , Anomalies detection, Security advisories, patch management etc.	HCI Node should integrate with Virtual platform and Network switches, Should have management software for a Firmware update, Manage Cluster and deployment, Full stack visibility HCI Node, TAC/Case Support, Continuous Health checks on Networking, Server, VMs , Anomalies detection, Security advisories, patch management,	No Change, additional feature will be consider as value add
429	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Server UAT > HCI Rack Servers > 13> Server Security	Request New Point to be added		Request to add the below point for security and management features for HCI Nodes Day2 operations and management of HCI Nodes for updates on Hardware and Software. HCI Node management tool should integrate with Virtual platform and Network switches. Should be able to do Firmware updates, Manage Cluster and deployment, Full stack visibility of HCI Node, TAC/Case Support, Continuous Health checks on Networking, Server, VMs , Anomalies detection, Security advisories, patch management etc.	HCI Node should integrate with Virtual platform and Network switches, Should have management software for a Firmware update, Manage Cluster and deployment, Full stack visibility HCI Node, TAC/Case Support, Continuous Health checks on Networking, Server, VMs , Anomalies detection, Security advisories, patch management,	No Change, additional feature will be consider as value add

| 430 | NA | Appendix01 Techno Functional Requirements-Server and Virtual platform > Microsegmentation > 1 | The Solution should be capable of supporting major hardware OEMs like Juniper, Arista, Cisco, HPE and Dell. The proposed solution should be a purely software-based solution and should not be dependent on any hardware make and model. | | Request below modified clause be considered:

 The Solution should be capable of supporting major hardware OEMs like Juniper, Arista, Cisco, HPE and Dell. The proposed solution should be a purely software-based solution and should not be dependent on any hardware make and model by creating overlay tunnels between the hosts. | The key benefits of no dependecy on hardware is by using software defined networking i.e overlay. Overlay is mandatory for network & Security automation as part of software defined data center. | No Change |
|---|---|---|---|---|---|---|---|
| 431 | NA | Appendix01 Techno Functional Requirements-Server and Virtual platform > Microsegmentation > 2 | The solution should provide a distributed firewall such that the firewalling for Virtual Machines can be provided closest to the application within the server itself without traffic going to a Physical Firewall. | | Request below modified clause be considered which includes additonal points

The solution should provide a distributed firewall such that the application aware and identity based statefull firewalling for Virtual Machines can be provided closest to the application within the server itself without traffic going to a Physical Firewall or regardless of underlying L2 Netwrork topology.

The solution should also provide an integrated networking solution (CNI implementations) as well as provide advance turnkey container networking & firewalling services. Solution should support for container networking plug-ins, support for pod to pod communication and support for ingress controllers.

The micro-segmentation solution should have a capability for stateful firewalling and ALGs (Application Level Gateway) on a per-workload granularity regardless of the underlying L2 network topology (i.e. possible on either logical network overlays or underlying VLANs), embedded in the hypervisor kernel, distributed | *As per security framework its recommended not to use standard ports for your applications and hence to have effective security on per VM basis an application/L7 firewalling is must.* Containers & Kubernetes are now part of all modern applications hence networing and security for container shall also be considered for end to end application security. there is App ID requirement is mentioned in RFP as part of "Internal Firewall" spec point # 23 hence same should be considered for mirosegmenation as well otherwise it will create non standard architecture. | No Change |
| 432 | NA | Appendix01 Techno Functional Requirements-Server and Virtual platform > Microsegmenation >5 | The proposed solution should provide the ability to define firewall rules at VM level for east-west traffic in order to implement Zero Trust Security | | Request below modified clause be considered:

The proposed solution should provide the ability to define Layer 7 application firewall rules at VM level for east-west traffic in order to implement Zero Trust Security alongwith URL Filtering and TLS inspection for encrypted traffic | Zero trust Security framework mandates TLS inspection for encrypted traffic, URL Filtering and Layer 7 application firewalling. | No Change, additional feature will be consider as value add |
| 433 | NA | Appendix01 Techno Functional Requirements-Server and Virtual platform > Microsegmenation >4 | The Proposed Solution including Hypervisor, SDS and Micro segmentation must be from the same OEM. | | Request below modified clause be consideredL

The Proposed Solution including Hypervisor, SDS, SDN and Micro segmentation must be from the same OEM. | SDN is missing in the spec, SDN will be mandatory to create complete automated Software Defined data center by creating an abstraction of the network enabling programming of network behavior in a centrally controlled manner through software applications. | No Change, SDN will be consider as value add |

434	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Microsegmenation >6	The proposed solution should allow users to define granular firewall rules based on IP Addresses, Tags/Categories and Subnets to segment User Applications		Request below modified clause be considered which includes additonal points The proposed solution should allow users to define granular firewall rules for both VM and conatiners based on IP Addresses, VM Names, Tags/Categories and Subnets to segment User Applications by creating dynamic security groups. The solution should have capability to provide stateful micro-segmentation for virtual machines and Kubernetes workloads from a single console. The solution should also support enforcement of stateful distributed firewall for IPv6 VM workloads. These firewall rules can use IPv6 addresses, IPv6 CIDR, IP Sets that include both IPv4 and IPv6 addresses and security groups that can include logical ports that have both IPv4 and IPv6 addresses. IPv6 capability should be available both at management and data plane	Its necessary to have dynamic security group capability to ensure complete automation. Mentioned in the RFP page 8 -> 2.0 --> Requirement Summary--> 2.1 Intent--> mentions requirement for IPv6 "The proposed solution should support both IPv4 and IPv6."	No Change
435	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Microsegmenation >7	Solution should provide capability to create network segments by defining them entirely in software and avoid the need to re-architect your network or deploy physical appliances		Request below modified clause be accmodated: Solution should provide capability to create network segments and L2 Streching between DC and DR by defining them entirely in software and avoid the need to re-architect your network or deploy physical appliances	L2 Streching is required for better application availability considering RFP asks for 99.99 % availability on monthly basis. RFP Page 17 -> "4. Service Levels "-->"SLA: The solution is expected to be available for 99.99% on 24x7 and up time availability will be calculated on monthly basis."	No Change, L2 stretching implementation will be discuss with elected bidder.
436	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Container >2	The solution must be able to manage Kubernetes clusters. Licenses for managing Kubernetes clusters should be implemented from Day-1		Request below modified clause be accmodated: The solution must be able to manage Kubernetes clusters. Licenses for managing Kubernetes clusters along with components such as backup, container registry and monitoring alongwith Windows Container support should be implemented from Day-1	Kubernetes Cluster doesn't work in isloation but require other components such as container registry and backup solution. If not included than Bob Card will have procure them separately. And Not aving Windows Container support will block any windows based apps to be deployed on Kubernetes Platform.	Yes, BOBCARD will take care such requirement
437	NA	Appendix02 Techno Functional Requirements-Network components > internal FW NG Firewall Features NEW POINT	Must have provisioning, operations and lifecycle management of Kubernetes, automated deployment, scaling, and operation of Kubernetes clusters		Request below modified clause be accmodated: Must have provisioning, operations and lifecycle management of Kubernetes, automated deployment, Auto scaling & Auto Healing, and operation of Kubernetes clusters	Complete Automation is not possible without Auto Scaling and Auto Healing of Kubernetes Clusters. One has to manually add nodes in case of failure or unprovisioned increase in load.	No Change

438	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Container >4	Container Platform should provide single pane of Glass for Lifecycle Management of all K8S clusters deployed on prem.		Request below modified clause be accmodated: Container Platform should provide single pane of Glass for Lifecycle Management of all K8S clusters alongwith ingress, backup and container registry deployed on prem.	Kubernetes Cluster doesn't work in isloation but require other components such as container registry and backup solution. These shall too be considered for life cycle management	Yes, BOBCARD will take care such requirement
439	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Cloud Management >1	The solution should provide capability of generating reports for usage, performance, compliance, health, forecasting and capacity.		Request below modified clause be accmodated: The solution should provide capability of generating reports for health, Capacity Optmization - Right Sizing (Under sized, Oversized), Reclamation (Idle, Powered off , Snapshot, Orphaned Disk , Forecasting - Capacity Forecasting, Migration assessment, Migration Planning Usage - Process and service utlization Compliance - Regulatory Benchmark (PCIDSS and ISO) Security Guidelines for Infrastructure and Cloud Management	Bob Cards will need capacity optimization capabilities to identify over-provisioned & under-provisioned resources and provide recommendations, alerts and automated actions on right-sizing and resource consumption so they can be right-sized for adequate performance and avoid resource wastage. Should provide visibility of capacity and VMs which can be reclaimed and cost visibility of the reclaimed capacity and VMs.	No Change, additional feature will be consider as value add
440	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Cloud Management >11	The solution should have intelligent operations with anomaly detection which will allow monitoring seasonal trends and automatically send email alert		The solution should have AI/ML driven intelligent operations & troubleshooting workbench with anomaly detection,third party infra (Server, Storage , Network, database and Application) along with parent child relatiohship mapping, service and process monitoring which will allow monitoring seasonal trends and automatically send email alert. The solution should also have log management capability for infrastructure and applications . log management solution should delivers intuitive, actionable dashboards, sophisticated analytics, and broad third-party extensibility across physical, virtual, and cloud environments.	BoB Cards will not be able to manage the infrastructure without comprhesive log management capability. Its also mandatory for from regulation/compliance perspective to have log stored for given period of time for audit. BoB Card would need apps (database and Application) to infra (Server, Storage , Network) level visibility for toubleshooting and performance monitoring.	No Change, additional feature will be consider as value add
441	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Cloud Management >7	The solution must have an approval process to review, reject or approve the deployment requests from the marketplace.		Request below modified clause be considered: The Solution must support multiple levels of approval with E-mail notifications with ability to automate manual provisioning and de-provisioning of the tasks and policies embedded in each layer of their application including auto - approve and auto-reject capability based on application criticality	The solution must have an approval process to review, multi level & auto reject or approve the deployment requests from the marketplace.	No Change, additional feature will be consider as value add

442	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 6	Hypervisor should support container and opensource integration for cloud native application from day-1. Must be a Kubernetes ready from day-1.		Request below modified clause be accmodated: Hypervisor should support container both Linux and Windows along with other kubernetes ecosystems such as container registry, backup, ingress & monitoring and opensource integration for cloud native application from day-1. Must be a Kubernetes ready from day-1.	Kubernetes doesn't work in isolation and requires multiple components for production setup.	Yes, BOBCARD will take care such requirement
443	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 16	Virtualization Manager should provide feature which can perform quick, as-needed deployment of additional virtualized hosts. When the service is running, it can push out update images, eliminating patching and update without impacting production.		Please clarify the scenario and expected outcome out of the below point in this clause: "When the service is running, it can push out update images, eliminating patching and update without impacting production."		Virtualization manager should allow addition of new nodes and patching/upgrade of hypervisor running on the node without any VM downtime.
444	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 22	Unlimited VM replication from DC to DR (No restriction on VM replication and DR orchestration) with the capability to define Recovery Plans		Request to provide the number of VMs to be orchestrated for automated recovery and not keep open as unlimited since this approach is OEM specific . The VMs to be protected/orchestrated are limited to what can be provisioned on these 14 servers of production. Furehr pls clarify the need for Recovery Plans		No Change, can not predict the exact number of VMs for next 5 Years which need to be replicated.
445	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 23	Proposed solution should have a self-service restore feature on a per-VM basis to allow trusted application administrators to recover their own files with the ability to mount snapshots as a drive in Windows VMs		Request this be modified as below or clarify the requriement: Proposed solution should have a self-service restore feature on a per-VM basis to allow trusted application administrators to recover their own VMs from the snapshot	Please clarify this requirement, this looks like back and restore requirements so the modified clause	This will help BOBCARD to recover file without losing current state of virtual machine.
446	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 24	Hypervisor should provide Visibility for Running VM and their connectivity co-relationship with Network Ports on attached Physical TOR / Core Direct which Include Network RX/TX Bytes.		Request below modified clause with additional inputs be considered : Hypervisor should provide Visibility for Running VM and their connectivity co-relationship with Network Ports on attached Physical TOR / Core Direct which Include Network RX/TX Bytes.Solution Should provide end to end visibility across physical firewall, switch and storage, Flow Analysis and Security Planning,Guided Troubleshooting, Microsegmentation planning, RCA (Connectivity Problem, Packet Loss, N/W latency), Application Discovery, Service Monitoring , Application Dependency Mapping and monitoring of non compliant ports	Monitoring is not considering all components of the stack. Unless end to end visibility is provided as part of this solution BoB Card has to spend separately on monitoring.	Yes, BOBCARD will take care such requirement. However Hypervisor should provide Visibility for Running VM and their connectivity co-relationship with Network Ports on attached Physical Port which Include Network RX/TX Bytes.

447	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Hypervisor > 30	Virtualization software or the solution should provide Cluster level encryption protects unauthorized data access at-rest.		Request below modified clause be considered : Virtualization software or the solution should provide Cluster level, VM Level encryption protects unauthorized data access at-rest and in transit.	Having capability to do the enscryption at app VM level and in transit is required to complete solution.	No Change, additional feature will be consider as value add
448	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Software Defined Storage > 1	Maintain primary working set copy of active data on the Local Node as VM's are hosted to provide high IOPS and low latency. Proposed solution must be proposed for faster reads and write for Business-critical Apps.		Request below additional point be added in theis clause : Proposed solution must be proposed for faster reads and write for Business-critical Apps.	Architecture is specific to one vendor, request BoB Cards to consider on outcome than specific architecture. There is no specific latency requirements mentioned in the spec.	No Change.
449	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Software Defined Storage >2	The solution must have De-duplication and Compression features licensed and implemented from day one (Should not have dependency on any proprietary hardware device).		Request below modified clause be considered: The solution must have De-duplication/Compression features licensed and implemented from day one (Should not have dependency on any proprietary hardware device).	Solution should have flexibility to implement either compression and de-duplication. BoB Cards should conisder overhead while deciding on both.	No Change
450	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Software Defined Storage >24	The proposed solution should support 1 min RPO & 1 hour RTO for critical workload in case BOB Cards wants to have this capability replication for Future use. The proposed solution should have native Replication and DR Orchestration from Day-1		What is the use case for 1 min RPO and 1 Hour RTO? is this linked with some regulatory requirement?	Replication is best handled at application level as having additional solution for infrastructure will complexity and cost for BoB Cards Its best to use extends the existing DR orchestration solution for this environment as well.	This is required for BOBCARD mission critical application. The solution should capable to support 1min RPO. The propose replication solution should be same OEM as the virtualization solution to provide seamless integration.
451	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Software Defined Storage >25	The solution provided should function even after one node failure.		Request below modified clause be considered: The solution provided should function even after two node failure.	RFP asks for 99.99 % availability SLA for the proposed solution. It will require minimum N+2 configuration for required resiliency and uptime.	No Change, additional feature will be consider as value add
452	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Software Defined Storage >31	The solution should provide enterprise data services such as compression completely in software. Software Defined Storage solution must have de-duplication and compression features Licensed and implemented from day one. These functionalities should be part of the proposed solution. The solution must have functionality to support compression and or deduplication online on data container without any downtime and data loss as per business requirement.		Request below modified clause be considered: The solution should provide enterprise data services such as compression completely in software. Software Defined Storage solution must have de-duplication or compression features Licensed and implemented from day one. These functionalities should be part of the proposed solution. The solution must have functionality to support compression and or deduplication online on data container without any downtime and data loss as per business requirement.	Solution should have flexibility to implement either compression and de-duplication. BoB Cards should conisder overhead while deciding on both.	No Change

453	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmentation > new point	Additional Point for consideration		The solution must ensure that there is not alteration in the IP address of the Virtual machine, by blocking the traffic from or to the VM inherited as a feature in the Solution.	IP/MAC spoofing is major security concern for organizations like BoB Cards handing customers data.	No Change, additional feature will be consider as value add
454	NA				The solution should support multi-tenancy to isolate networking/security for different departments/function within BoB Cards upto a minimum of 4 tenants and 5 VPCs	VPC will enable Bob Cards to create isolation from access , resources, network and security.	ange, additional feature will be consider as valu
455	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Container > 6	Should support cluster scale out i.e addition of worker nodes as and when required.		Request below modified clause be considered: Should support Automated cluster scale out i.e addition of worker nodes as and when required.	Complete Automation is not possible without Auto Scaling and Auto Healing of Kubernetes Clusters. One has to manually add nodes in case of failure or unprovisioned increase in load.	No Change
456	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > 3	The solution shall provide a single pane of glass for automated provisioning with model-based orchestration of compute, network and storage through a unified multi-tenant self-service catalog.		Request below modified clause be consiered The solution shall provide a single pane of glass for automated provisioning with model-based orchestration of compute, network , storage and Kubernetes through a unified multi-tenant self-service catalog .	All modern applications are combination of both container and VM form factor.	No Change, additional feature will be consider as value add
457	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > 5	The solution must provide a self-service portal to allow user to consume the creation of infrastructure easily.		Request below modified clause be considered: The solution must provide a self-service portal to allow user to consume the creation of infrastructure easily for both VM and Kubernetes	All modern applications are combination of both container and VM form factor.	No Change, additional feature will be consider as value add
458	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > 8	The software must allow the designer to use shell script, PowerShell script to code the automation.		Request below modified clause be considered: The software must allow the designer to use shell script, PowerShell script, Python and node JS to code the automation.	Python and nodeJs are very popular language for scrpting in terms resource availability and community support	No Change, additional scripting will be value add
459	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > 9	The software must allow the designer to design VM blueprints.		Request below modified clause be considered: The software must allow the designer to design Multi VM & Kubernetes blueprints.	All modern applications are combination of both container and VM form factor.	No Change, additional feature will be consider as value add
460	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > 12	The solution should have simple low-code, no-code automation engine which allows automating day-to-day routine tasks		Request below modified clause and adidtoinal inpurs on the clause be considered: The solution should have simple low-code, no-code automation engine which allows automating day-to-day routine tasks such as Snapshot creation, Addition of Disk, Power Cycle (Suspend , Shutdown, Reboot, reset), Resize, Rebuild, Additional of Network, VM Unregister , Delete,connect remote console, Change Security Group with capability to create additional resource actions as out of the box capability.	All modern applications are combination of both container and VM form factor.	No Change, additional feature will be consider as value add

461	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > New Point	New Point		Solution should provide capability to define and showcase cost to create cloud like experience to the business unit with the overall cost spend on the infrastructure [server hardware, storage, licenses, application, maintenance, labor, network, facilities , etc.	Bob Cards will need Cost transparency (Showback and Chargeback capability) across private, hybrid to optimize planning and prioritization of VM/ Server/Application onboarding/provisioning	No Change, additional feature will be consider as value add
462	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF & IPS	New Point		We request BoB Card to allow for both software and hardware based solution for Load Balancer, WAF, IPS/IDS. As these components are dynamic as per application consumption requirements and considering bob card is directly managing customer data, its very critcal that these components are added as part of sofwate defined stack.	Modern applications increasingly require software-defined networking (SDN) and security solutions due to their need for greater flexibility, agility, and scalability. Traditional networking and security methods often lack the adaptability to support the dynamic nature of modern application environments, especially in cloud	No Change
463	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF C.Solution Capabilites Pont #5	The solution must support and integrate the web application vulnurability tools (Web application scanners) being proposed by bidder as part of this RFP at minimum to virtually patch web application vulnurabilies or else solution should have ready plug-ins to integrate banks VAPT tool.		Requesting you to modify the clause as below:

The solution must support and integrate the web application vulnurability tools (Web application scanners) being proposed by bidder as part of this RFP, solution should have ready plug-ins to integrate banks VAPT tool. | Solution should be capable to protect against zero-day vulnerability using positive security model without being dependent on virtual patching. Virtual patch can even lead to false positive. | No Change |
464	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #2	Appliance/Chassis based Hardware should support scalability with license upgrade. -18 vCPU from day 1	Scalable to 32 vCPU -128 GB DDR RAM from day 1 -1 TB X 1 SSD M.2 SSD (in Raid) from Day 1		The clause represents single OEM offering for sizing		No Change
465	NA	7/B.Hardware & InAppendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #7	The proposed appliance shoulde provide minimum 1.2 Gbps of real world WAF throughput from day 1 and should be scalable to 2.2 Gbps with license upgrade on the same hardware or additional blades in case of a chassis based solution. The WAF throughput mentioned should be inclusive after enabling the below mentioned features: With all WAF functions enabled per intance in blocking mode SSL inspection.		The clause represents single OEM offering for sizing		No Change
466	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #8	The appliance should support the layer 7 throughput should be at least 58 Gbps scalable to 92 Gbps on same hardware with license upgrade. (Data rerernces for above should be verified from publicly available datasheet)		The clause represents single OEM offering for sizing		No Change

467	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF B.Hardware & Interfaces requirement Point #9	The proposed appliance must have minimum hardware compression of 34 Gbps for HTTP traffic form day 1 and scalable upto 48 Gbps with add on license on same hardware. (Data rerernces for above should be verified from publicly available datasheet)		The clause represents single OEM offering for sizing		No Change
468	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF B.Hardware & Interfaces requirement Point #10	The proposed appliance should support minimum hardware based SSL offloading from day 1 up to : 34 Gbps Scalable upto 48 Gbps on same hardware with license upgrade. (The SSL encryption & decryption process must be hardware-based proccessor for acceleration) (Data rerernces for above should be verified from publicly available datasheet)		The clause represents single OEM offering for sizing		No Change
469	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF B.Hardware & Interfaces requirement Point #11	The solution must support minimum SSL TPS/CPS: -29 K ECDSA P-256-bit keys from day 1 -58 K RSA 2048-bit keys from day 1 scalable to minimum SSL TPS/CPS -68 K ECDSA P-256-bit keys -98 K of RSA 2048-bit Keys (Data rerernces for above should be verified from publicly available datasheet with SSL)		The clause represents single OEM offering for sizing		No Change
470	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF B.Hardware & Interfaces requirement Point #12	The proposed appliance should support minimum 74 million L4 concurrent connections from day one and scalable upto 99 Million on same hardware with license upgrade.		The clause represents single OEM offering for sizing		No Change
471	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF B.Hardware & Interfaces requirement Point #13	The proposed appliance should support minimum 2.4 million L7 requests per seconds from day 1 and scalable upto 4.2 Million on same hardware with with license upgrade.		The clause represents single OEM offering for sizing		No Change
472	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF General Requirement Point #13	The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide traffic performance statistics for last 30 days including Active Connections, Active Sessions, CPU Usage By Core, HTTP Requests, Memory Used, RAM Cache Utilization, Rewrite Transaction, Data Rewrite Transactions, SSL Transactions, Throughput(bits), Throughput(packets), & Total New Connections		The clause should mention the functionality should be achieved without being dependent on tools.	The clause represents single OEM offering.	No Change

473	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF B.Hardware & Interfaces requirement Point #14	The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide a security event timeline dashboard where critical events like Audit logs, Pool status change, Failover status change, DOS attacks etc. must be shown for ease of troubleshooting with last 20 Failed logins details		The clause should mention the functionality should be achieved without being dependent on tools.	The clause represents single OEM offering.	No Change
474	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF B.Hardware & Interfaces requirement Point #15	The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide a Bug tracker option, where an admin can login and find any bugs affecting the devices		The clause should mention the functionality should be achieved without being dependent on tools.	The clause represents single OEM offering.	No Change
475	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF B.Hardware & Interfaces requirement Point #16	The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide an upgrade Options suggestions for next hotfix and stability release for ease of day-2 operations with single click access to release notes a nd EOS dates		The clause should mention the functionality should be achieved without being dependent on tools.	The clause represents single OEM offering.	No Change
476	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF B.Hardware & Interfaces requirement Point #17	The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide an ability to execute CLI commands which are essential for diagnostics which will show historic data or data at the time of file captured. E.g show history of all executed commands on the CLI		Request you to remove this clause	Database Load Balancer is provided as inbuilt feature from database solution provider and hence not needed from SLB solution	No Change
477	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF C.Solution Capabilities Point #23	Solution should have the capability to highlight (In red / any color code) only malicious payload from the entire attack payload on the event analysis dashboard for detailed fornsics analysis. This is extermly critical when our incident response teams are in combat with the attackers during wartime.

This feature/functionality has to be live demonstrated by the bidder after the prebid query meeting, by setting up a lab in the cloud/on-premises | | Forensics are not required for LB or WAF kind of solution. This is required for DDoS kind of solution and it is not recommended to have DDoS solution within WAF+LB as DDoS should be a stateless technology and it's placement should be at perimeter level above firewall to protect complete infrastruture | | No Change |

478	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF C.Solution Capabilities Point #36	The Proposed WAF Solution should provide built-in L7 layer DDoS detection and mitigation features based on machine learning and behavioral analytics and dynamic signatures. It should have CAPTCHA support or other mechanism to avoid distributed attack. This feature/functionality has to be live demonstrated by the bidder after the prebid query meeting, by setting up a lab in the cloud/on-premises		Request to remove this point	DDoS should be a stateless device and it's placement should be at perimeter level above firewall. This ensures protection to network from any advanced DDoS attacks. Hence, it should not be expected to be part of other security solutions within the network.	No Change
479	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF C.Solution Capabilities Point #58	The Solution should have IPSEC tunneling capabiltiies		Request to remove this point	VPN is recommended to be a dedicated solution since it relies on TLS protocol. It is also recommended to terminate the traffic on Firewall or before Firewall as it will check for security parameters on the same. If this is done on ADC, there won't be any security check and can possess threat or security flaw.	No Change
480	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF C.Solution Capabilities Point #59	The proposed solution should support a comprehensive list of ways in which LB can monitor the backend services including Daimeter, DNS, FTP, Gateway ICMP, HTTP, HTTPS, TCP half open, TCP , LDAP, MSSQL, MYSQL, MQTT , POSTGRESQL, POP3 , IMAP, NNTP, Radius , SIP and custom external scripts		Request to modify the clause as below: The proposed solution should support a comprehensive list of ways in which LB can monitor the backend services including DNS, FTP, Gateway ICMP, HTTP, HTTPS, TCP half open, TCP , LDAP, MSSQL, MYSQL , POSTGRESQL, POP3 , IMAP, NNTP, Radius and custom external scripts	SIP, Diameter & MQTT Traffic are used in Service Provider environment and are not relevant and used in any Enterprise environment like BOB Cards.	No Change
481	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF C.Solution Capabilities Point #61	The proposed solution should support various types of LB config for handling traffic, including standard reverse proxy, forwarding in L2 , Forwarding in IP, High performance mode, Stateless mode , Reject mode, DHCP relay, and Message routing for SIP, Daimeter and MQTT traffic		Request this clause be modified as below: The proposed solution should support various types of LB config for handling traffic, including standard reverse proxy, forwarding in L2 , Forwarding in IP, High performance mode, Stateless mode , Reject mode, DHCP relay	SIP, Diameter & MQTT Traffic are used in Service Provider environment and are not relevant and used in any Enterprise environment like BOB Cards.	No Change
482	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF C.Solution Capabilities Point #70	The proposed solution should support native integration with kubernetes based platforms hosting microservices e.g. Openshift, TKG cluster etc. Solution should update the configuration of LB automatically by observing events within kubernetes clusters form day 1 without add on license.		Solution should be able to support by means of same solution.		No Change

483	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF C.Solution Capabilities Point #81	The proposed LB solution should also support secure remote access to admin users (concurrency of not more than 10); where the solution can do endpoint checks for the admins and establist a secure tunnel with autentication against AD/OAUTH/Radius and MFA via Google authenticator. The system should allow per user basis a login schedule ?(e.g night shift employee cannot login during working hours)		The clause represents single OEM offering.	No Change
484	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF D.Availability #2	The solution should support SQL-based querying for the following databases for the health checks: for Oracle, MSSQL, MySQL, PostgresSQL and other databases if required in future.		Request this clause be removed	Database Load Balancer is provided as inbuilt feature from database solution provider and this is proprietary load balancing feature of Database solution provider and hence not needed from ADC solution.	No Change
485	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #7	The Firewall appliance should have certifications like ICSA /EAL4/CCNDPP		Request this be modified as below: The Firewall solution should have certifications like ICSA /EAL4/CCNDPP	Every OEM has its own solution offering and certification ask may align to the approach solution is provided rather than mandating it on the appliance inline to a particular OEM	No Change
486	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #9	OEM/Bidder should provide below transceivers from Day-1. Firewall and SFP should be from same OEM. Below mentioned SFP quantity is required per appliance. 4 X 10GE SR SFP+ 4 X 1G SFP 4 x 25G SFP28		OEM/Bidder should provide below transceivers from Day-1. Firewall and SFP should be from same OEM. Below mentioned SFP quantity is required per appliance. 4 X 1G RJ 45 4 X 10G SFP+ 4 x 25G SFP28	Requesting if 1G can be considered using Copper Links and not SFP	No Change
487	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #15	Solution should have minimum 450 GB SSD pair, system storage		Request to modify this as below Solution should have minimum 900 GB SSD pair, system storage	Perimeter Firewall needs high storage numbers as visible with mid/large scale deployments for storing logs considering 3/6 months retention in case the remote Management device is impacted , so good to ask for more	No Change, additional feature will consider as value add
488	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #16	Solution should have minimum 32 GB		Request clause to be modifiedL Solution should have minimum 128 GB RAM	Perimeter Firewall has to have good RAM and such baselining will help with operations of critical banking infra	No Change, additional feature will consider as value add

489	NA	Appendix02 Techno Functional Requirements-Network components > perimeter FW Specifications Point #19	"The proposed firewall must provide minimum 10 Gbps of Threat prevention throughput with Real world traffic. (Throughput must be derived from Appmix traffic and not Video/JPEG based traffic) (enterprise testing condition). The throughput must remain 10 Gbps even after enabling NGFW + IPS/IDS + Antivirus + Anti Spyware + Anti Bot + DoS/DDOS + All signature enabled + Logging enabled + Bidirectional inspection + File Blocking. OEM to provide publicly available The Test methodology and result should be compliant to the benchmark testing methodology for the above parameters provided in the Internet Engineering Task Force (IETF)- 'Benchmarking Methodology for		Request below modified clause be considered , instead of Appmix traffic , real world traffic should be mentioned for deriving throughput "The proposed firewall must provide minimum 10 Gbps of Threat prevention throughput with Real world traffic. (Throughput must be derived from real world traffic and not Video/JPEG based traffic) (enterprise testing condition). The throughput must remain 10 Gbps even after enabling NGFW + IPS/IDS + Antivirus + Anti Spyware + Anti Bot + DoS/DDOS + All signature enabled + Logging enabled + Bidirectional inspection + File Blocking. OEM to provide publicly available The Test methodology and result should be compliant to the benchmark testing methodology for the above parameters provided in the Internet Engineering Task Force (IETF)- 'Benchmarking Methodology for Network Security Device	instead of appmix traffic real world traffic will be rifht measure of throuhgput , so requesting the change	No Change
490	NA	Appendix02 Techno Functional Requirements-Network components > perimeter FW Specifications Point #21	NGFW appliance must be capable of handling minimum 2 M concurrent sessions utilizing HTTP transactions with all Security feature Turned ON and not based on UDP / Lab environment / ideal testing environment, this claim has to be supported with declaration of concurrent connections claim from OEM		Request below modified clause to accomodate support for 5M concurrent sessions NGFW appliance must be capable of handling minimum 5 M concurrent sessions utilizing HTTP transactions with all Security feature Turned ON and not based on UDP / Lab environment / ideal testing environment, this claim has to be supported with declaration of concurrent connections claim from OEM	Mid/Large scale deployments need higher concurrent session support and baselining this to 50 Lakh concurrent sessions will be in the interest of the Bank , so the requested change	No Change, additional feature will consider as value add
491	NA	Appendix02 Techno Functional Requirements-Network components > perimeter FW Specifications Point #49	Solution should support creation of minimum 1 virtual context / instance from Day-1 without any compromise on system performance and network bandwidth.		Solution should support creation of minimum 5 virtual context /instance from Day-1 without any compromise on system performance and network bandwidth.	Support for only 1 Virtual context may not be scalable for the DC design and min support for 5 instances is the need for any DC infra Perimeter Firewall understanding furture state architecure and growing needs.	No Change, additional feature will consider as value add

492	NA	Appendix02 Techno Functional Requirements-Network components > perimeter FW Specifications Point #54	The proposed NGFW solution architecture should have Control Plane separated from the Data Plane in the Firewall appliance architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup, QoS, NAT etc). Control plane must have dedicated resources such as CPU, RAM etc. This is to ensure Bank always has management access to NGFW irrespective of Firewall load / Traffic Spike / Cyber Attack driving higher CPU utilization. Bank should able to login to the firewall and carry out reporting /		Request below modified clause be considered The proposed NGFW solution architecture should have Control Plane separated from the Data Plane in the Firewall solution architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup, QoS, NAT etc). Control plane must have dedicated resources such as CPU, RAM etc. This is to ensure Bank always has management access to NGFW irrespective of Firewall load / Traffic Spike / Cyber Attack driving higher CPU utilization. Bank should able to login to the firewall and carry out reporting / management / packet capture etc to identify the root cause and accordingly take necessary action to remediate it.	OEMs have different approaches to achieving the use case and instead of the ask on the appliance itself , the Firewall Solution will be a generic term to use in requirements so this suggestion	No Change
493	NA	Appendix02 Techno Functional Requirements-Network components > perimeter FW Specifications Point #72	IPS should provide detailed information on each protection, including: Vulnerability and threat descriptions, Threat severity, Performance impact, Release date, Industry Reference, Confidence level etc.		Request below changed clause : IPS should provide detailed information on each protection, including: Vulnerability and threat descriptions, Threat severity, Release date, etc	Performance impact, industry reference and confidence level are subject to configuration and infrastructure in the bank.	No Change
494	NA	Appendix02 Techno Functional Requirements-Network components > perimeter FW Specifications Point #76	Should have more than 60+ predefined Categories based on Urls, Application types, Security Risk level etc. However solution should be able to create custom categories for URL and application.		Request below modified clause with increased number of categories: Should have more than 80+ predefined Categories based on Urls, Application types, Security Risk level etc. However solution should be able to create custom categories for URL and application.	Having more predefined categories support would help bank with improved threat detection and better granular policy control with less manual effort.	No Change, additional feature will consider as value add
495	NA	Appendix02 Techno Functional Requirements-Network components > perimeter FW Specifications Point #89	Solution should give information related to Performance impact and confidence level of protections while creating profiles.		Request this clause be deleted	performance can be subject to policy configurations and existing infra at bank.	No Change

496	NA	Appendix02 Techno Functional Requirements-Network components > perimeter FW Specifications Point #114	"Management server should support the following for rule optimization: • Unused Rules Calculation for specific time-period based on Firewall Traffic Logs. • Analysis on Covered/Shadow/Hidden Rules • Analysis on Rules Consolidation (Merging of similar kind of rules) • Analysis on Redundant Rules • Tightening of Overly Permissive Rules (Any-Any) • Analysis on Unattached/Unused Objects to simplify objects management • Analysis on Rule-Reordering to improve the performance of the Firewall • Analysis on Disabled/Expired Rules for enhanced visibility on the Firewall Rules sets"		"Management server should support the following for rule optimization: • Unused Rules Calculation for specific time-period based on Firewall Traffic Logs / HIt count • Analysis on Covered/Shadow/Hidden Rules • Analysis on Redundant Rules • Analysis on Unattached/Unused Objects to simplify objects management • Analysis on Disabled/Expired Rules for enhanced visibility on the Firewall Rules sets"	OEMs could be handling the use case suggested for removal differently or have no dependency on the performance of the Firewall , so requesting these be removed from the ask	No Change
497	NA	Appendix02 Techno Functional Requirements-Network components > IPS Features Point #15	Should support more than 3000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness		Should support more than 5000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness	Increasing number of signature support is beneficial for the Bank's operations and for Effective Security reasons	No Change
498	NA	Appendix02 Techno Functional Requirements-Network components > internal FW Point #11	The Firewall solution Should support more than 4000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness and should be able to create 40 or more application categories for operational efficiency. Dedicated IPS solution shall be in corporated by the bidder to achive this scale of IPS AVC signatures in this solution.		Request this clause be modfied as below: The Firewall solution Should support more than 6000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness and should be able to create 40 or more application categories for operational efficiency. Dedicated IPS solution shall be in corporated by the bidder to achive this scale of IPS AVC signatures in this solution.	Increasing number of signature support is Beneficial for the Bank's operations and for Effective Security reasons	No Change, additional feature will consider as value add
499	NA	Appendix02 Techno Functional Requirements-Network components > internal FW NG Firewall Features NEW POINT	New Point to be added		The solution should provide Change Management capability for the organizations needs to implement more formal processes for configuration changes, including audit tracking and official approval before changes are deployed.	By leveraging these features and integrating with external change management tools, organizations can implement a robust change management process that includes formal approval, audit tracking, and compliance reporting within Cisco FMC.	No Change

		Features NEW POINT				
500	NA			The solution should provide traffic hit count, Rule Conflict Detection (Redundant & Shadowed) and policy warning for streamlining firewall policies.	These features are crucial for optimizing firewall policies, ensuring efficient traffic flow, and maintaining security posture.	No Change, additional feature will be consider as value add
501	NA	Appendix02 Techno Functional Requirements- Network components > internal FW Hardware Architecture Point #3	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 8x64 GB of RAM.	Request below modified clause be considered as correction on the ask which seems typo:

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. | | 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. |
| 502 | NA | Appendix02 Techno Functional Requirements- Network components > Mngmt Switch 6 Product Support Point #2 | The OEM support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support | Request below modified clause be considered

The OEM/OEM certified partner support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support | OEM Certified partner has thorough experience of OS version upgrades and maintaining network operations troubleshooting issues and it will be cost effective to include this in the ask | The OEM/OEM certified partner support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support |
| 503 | NA | Appendix02 Techno Functional Requirements- Network components > Mngmt Switch 9 Miscellaneous Points Point #1 | Console cable and power cable (As per Indian standards) as per customer requirement to be provided. All Cables shall be factory-terminated. | Since Console Cables are common for all devices per OEM , Request Bank to clarify the count of console cables to be provided , is it one each with each Switch or one per DC and DR Each ?. | | No Change |
| 504 | NA | Appendix02 Techno Functional Requirements- Network components > Mngmt Switch 10 Product Support Point #2 | The OEM support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support | Request below modified clause be considered

The OEM/OEM certified partner support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support | OEM Certified partner has thorough experience of OS version upgrades and maintaining network operations troubleshooting issues and it will be cost effective to include this in the ask | The OEM/OEM certified partner support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support |
505	NA	Appendix02 Techno Functional Requirements- Network components > Core Swtich >9 Manageability > Appliance point 9.4	Switch Anomolies related with Advisories , PSIRT and Field Notices	Request this clause be removed from the telemetry asks	This feature is not requireed for the design at the BOB DataCenter and may be removed	No Change
506	NA	Appendix02 Techno Functional Requirements- Network components > Core Swtich >13 Fabric Management > Appliance point 13.1	Solution must provide Centralized Management Appliance – Single pane of glass for managing, monitoring and provisioning the entire Solution within Data Center & across all Data Centers	Request BOBCards to provide VM compute resources for spinning up the VMs to provide this functionality while we can provide the necessary sw and support.		Requested product functionality should be comply, BOBCards will provide VM compute resources for spinning up the VMs to provide this functionality however bidder should provide the necessary sw and support.
507	NA	Appendix02 Techno Functional Requirements- Network components > Core Swtich >5 Layer 2 Features > Appliance point 5.11	Switch Hardware should have capability to support BGP EVPN Route Type 1, Type 2, Type 3, Type 4, Route Type 5, Type 6/Type 7/Equivalent routes	Request this point be removed	BOBCards design doesn't have Fabric so this is not applicable	No Change

508	NA	Appendix02 Techno Functional Requirements- Network components > Core Swtich >13 Fabric Management > Appliance point 13.36	Solution should provides reports using predefined templates, including inventory, use, and health reports.		Request below modified clause be considered: Solution should provides reports including inventory, use, and health reports.		No Change
509	N/A	Annexure 02 Technical Evaluation Criteria	Presentation: Project plan, Deliverables, Timelines, Experience on proposed solution, value add			Request for Change: Request BOB Cards to Change clause as per below, Project plan, Deliverables, Timelines, Experience on similar to proposed solution, value add	Project plan, Deliverables, Timelines, Experience on proposed OEM solution, value add
510	N/A	Appendix02 Techno Functional Requirements- Network components	WAF - Administration, Manageability & Reporting 2.The solution should support integration with banks SIEM, SOAR and management solutions.		Request for clarification: Request BOB Cards to provide information on existing SIEM and SOAR solution and any other Management solution for integration, so bidder can check for compatibility.		This will be share only with elected Bidder.
511	N/A	General	Log Retention requirement		Request for Clarification: Request BOB Cards to clarify if there any requirement for log retention in same hardware appliance / solution, if yes please specify number of days log retention requirement.		Any device should store minimum 24hrs logs
512	12	3.1 Project Scope	11. The resolution time for the hardware/software related issues should be 4 hours, there should be 24*7*365 support from the OEM for all the supplied products through this RFP.			Request For Change: Request BOB Cards to change clause as per below, The response time for the hardware/software related issues should be 4 hours, there should be 24*7*365 support from the OEM for all the supplied products through this RFP. Or Request bank to remove Resolution clause as resolution may depend on various scenario.	No Change.
513	12	3.1 Project Scope	12. Hardware RMA (Return Merchandise Authorization) should be within 24 hours.			Request for Change: Request BOB Cards to change clause as per below, Hardware RMA (Return Merchandise Authorization) should be within 48 hours.	Hardware RMA (Return Merchandise Authorization) should be within 24 hours on Next business Day Basis.
514	13	3.1 Project Scope	16. L2 and L3 onsite support post implementation a. Software upgradation b. Hardware Upgradation c. Mass Changes for compliance d. Major, minor changes in feature/functionality roll out on the same infrastructure.		Request for clarification: request BOB Cards to clarify, total number of L2 & L3 resource requirement along with Shift details. Or clarify is it L2 & L3 level onsite support on incident basis requirement?		Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
515	NA	Annexure 02 - Technical Evaluation	The bidder should have supplied and installed similar to proposed hardware in last three (3) financial years, i.e. 2021-2022, 2022-23, 2023-24 (Bidder to provide details in Annexure K and submit PO / Contract details)		Pls. clarify that refrences required for hardwae as per RFP should be required in single PO or multiple PO copies for solution asked in RFP from the same customer will work.		Multiple copies of PO will be considered

#	Page	Section	Clause		Query	Request to Change	Response
516	NA	Annexure 02 - Technical Evaluation	The bidder should have deployed and configured proposed software as per OEM standard on proposed hardware in last three (3) financial years, i.e. 2021-2022, 2022-23, 2023-24 (Bidder to provide details / submit PO / Contract details)			Request to change clause as The bidder should have deployed and configured proposed software as per OEM standard on similar hardware in last three (3) financial years, i.e. 2021-2022, 2022-23, 2023-24 (Bidder to provide details / submit PO / Contract details)	The bidder should have deployed and configured proposed software as per OEM certified and standard hardware in last three (3) financial years, i.e. 2021-2022, 2022-23, 2023-24 (Bidder to provide details / submit PO / Contract details)
517	9	2.2 Tenure	The tenure of the contract initially would be for 1 year from the date of the issuance of first purchase order. BOBCARD can further extend to 2 years at its at mutually agreed terms.		Need Clarity on Contract tenure as on page no 13, it is written 3 years.		Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
518	17	3.1 Project Scope - Point 17	The initial term of this contract shall be 3 years and may be extended to another 2 years subject to satisfactory performance by successful bidder and OEM(s).		Need Clarity as on page no 9, it is written 1 year.		Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
519	34	9.4 Extension of Contract Post Expiry	The Company desires to appoint the vendor for a total period specified in the RFP, considering the effort and investments required in the arrangement. However, understanding the complexities of the entire arrangement, Company would like to safe guard the interests of all the entities involved in the arrangement. Therefore, the Company would like to have options to revisit the arrangements and terms of contract as well as to re-price the same (rates similar or less than existing arrangement) after the contract expiry, if necessary		Need clarity on the terms. The Extension of contract post expiry of contract period will be done as per mutual understanding.		No Change
520			The Company expects the benefits from any unanticipated decrease in technology infrastructure costs, over the term of the contract due to reduction of prices, efficient use of IT infrastructure/reduction of statutory charges, etc. and operations management methods that yield more efficient operations, to be passed on through re-negotiation. No conflict between the Selected Bidder and the Company will cause cessation of services				The extension of contract post expiry i.e. after 5 years for TCO mentioned in BOM can be extend further to next 2 years as per mutual understanding.
521			Supply of Servers & Network component as prescribed under hardware requirement.			Supply of Servers & Network component as prescribed under hardware requirement.	Supply of Servers & Network component as prescribed under hardware requirement Within 6-8 weeks from date of PO. Rest all clause remain same
522			20% of Total Cost of Equipment outlined in BOM.			Request to change the clause as : 70% of Total Cost of Equipment outlined in BOM	No Change
523	31		Supply of Software as prescribed under software requirement			Supply of Software as prescribed under software requirement	No Change
524			20% of Total Cost of Equipment outlined in BOM.			Request to change the clause as: 70% of Total Cost of Equipment outlined in BOM.	No Change
525			Completion of rack mounting of Servers & Network component and Configuration. Implementation of Software			Completion of rack mounting of Servers & Network component and Configuration. Implementation of Software	No Change

526			30% of Hardware and software licenses amount within 45 days from the date of acceptance of Tax Invoice by BOBCARD.			Request to change the clause as: 20% of Hardware and software licenses amount within 45 days from the date of acceptance of Tax Invoice by BOBCARD.	No Change
527		8. Payment Terms	30% of one time implementation cost.			30% of one time implementation cost.	No Change
528			Acceptance / Go-live by BOBCARD			Acceptance / Go-live by BOBCARD	No Change
529			Balance 50% of Hardware and software licenses amount and 70% of installation within 45 days from the date of acceptance of Tax Invoice by BOBCARD.			Request to change the clause as Balance 10% of Hardware and software licenses amount and 70% of installation within 30 days from the date of acceptance of Tax Invoice by BOBCARD.	No Change
530			Annual Maintenance, Support / Subscription Renewal of Licenses and Hardware			Annual Maintenance, Support / Subscription Renewal of Licenses and Hardware	No Change
531	32		100% payment on renewal of licenses support / subscription within 45 days from the date of acceptance of Tax Invoice by BOBCARD.		Help to confirm it is 100%advance payment i.e. start of the year.	Request to amend the clause as 100% yearly advance payment on renewal of licenses support / subscription within 45 days from the date of acceptance of Tax Invoice by BOBCARD.	No Change
532			Support for the day-to-day operations			Support for the day-to-day operations	No Change
533			Payment shall be released on half yearly basis; i.e., 50% of invoice Cost shall be paid on completion 06 month & balance 50% on completion of 12 months of the respective year subjected to acceptance of Tax Invoice by BOBCARD			Request to change the payment as : Payment shall be released on Quaterly subjected to acceptance of Tax Invoice by BOBCARD	No Change
534	1	Annexure 1 - Eligibility Criteria	Bidder should have experience of minimum 3 years in providing the Proposed Products/Services mentioned in the RFP.		Bidder request to consider folloiwng : Bidder should have experience of minimum 3 years in providing the Proposed / Similar Products/Services mentioned in the RFP. PO should have atlest one similar solutions required in the current RFP.		Need to check
535	1	Annexure 02 Technical Evaluation Criteria	The bidder should have supplied and installed similar to proposed hardware in last three (3) financial years, i.e. 2021-2022, 2022-23, 2023-24 (Bidder to provide details in Annexure K and submit PO / Contract details)		Bidder requests to consider the following : The bidder should have supplied and installed similar to the proposed/ similar hardware in the last Five (5) financial years, i.e. 2019-2020,2020-2021,2021- 2022, 2022-23, 2023-24 (Bidder to provide details in Annexure K and submit PO / Contract details). The purchase order can have any of the similar solutions required in the current RFP. 2 deployments – 10 Marks More than 2 deployments– 15 Marks In case of OEMs part code bidder request to consider reference from its authorised partner		No Change
536	1	Annexure 02 Technical Evaluation Criteria	The bidder should have deployed and configured proposed software as per OEM standard on proposed hardware in last three (3) financial years, i.e. 2021-2022, 2022-23, 2023-24 (Bidder to provide details / submit PO / Contract details)		Bidder requests to consider following : The bidder should have deployed and configured proposed / Simialr software as per OEM standard on proposed / similar hardware in last Five (5) financial years, i.e. 2019-2020,2020-2021, 2021-2022, 2022-23, 2023-24 (Bidder to provide details / submit PO / Contract details) The purchase order can have any of the similar solutions required in the current RFP. 2 deployments – 10 Marks More than 2 deployments– 15 Marks		No Change
537	1	Annexure 02 Technical Evaluation Criteria	Presentation		Bidder request to cosnider 40 marks for presentation and technical capabilites		No Change

538		New	Project manager with total experience more than 10 years A. Educational Qualification: BE / B. Tech / MCA with MBA/M. Tech /PGDM/ or equivalent with Certification on PMP/ Prince Certification mark and Work experience in the capacity of Project/Program Manager in ICT implementation Projects (with more than 10 years of relevant experience) 5 Project Managers - 15 marks 4 Project Managers - 10 marks 3 Project Managers - 5 Marks		Bidder request to add this marking criteria		Bidder to decide the project manager criteria.
539		New	The bidder must have IT Security permanent professionals with experience in-scope solutions on their payroll with certifications such as CISSP / OSCP / CEH / CCNP / CISA / CISM / OEM Level Certification. 15 IT Security Professionals: 15 marks 10 IT Security Professionals: 10 marks 5 IT Security Professionals: 5 marks		Bidder request to add this marking criteria		Bidder to decide the project manager criteria.
540	7	7, Integrity Pact	Fall Clause- The BIDDER undertakes that it has not offered/is not offering similar product/systems or subsystems at a price lower than that offered in the present bid in respect of any other Ministry/Department of the Government of India or PSU or any other Bank and if it is found at any stage that similar product/systems or sub systems was supplied by the BIDDER to any other Ministry/Department of the Government of India or a PSU or a Bank at a lower price, then that very price, with due allowance for elapsed time, will be applicable to the present case and the difference in the cost would be refunded by the BIDDER to the COMPANY, if the contract has already been concluded.		Request to delete this clause from the Integrity Pact		No Change
541	17	4. Service Levels	SLA Penalty Calculation: Deployment: In case of the Rollout delays by the Bidder the financial Penalty as per the BOBCARD discretion will be imposed on the Bidder at 0.5% of the total contract value per month of delay, to the maximum of 5% of the total contract value.		Request to limit this to 5% of the undelivered or delayed deliverables only.		SLA Penalty Calculation: Deployment: In case of the Rollout delays by the Bidder the financial Penalty as per the BOBCARD discretion will be imposed on the Bidder at 0.5% of the total contract value per month of delay, to the maximum of 5% of the total First year value.
542	31	8 Payment terms	Absent		Request that all payments be made within 30 days of submission of the invoice		Supply of Servers & Network component as prescribed under hardware requirement Within 6-8 weeks from date of PO. Rest all clause remain same

543	32	9.2 Indemnity	Entire clause		We submit replacing the current language with the following: "The Indemnifying Party ("Bidder") shall defend (settle and/or pay damages awarded by the court) the Indemnified Party against any third party claims arising from the following: a. Claims for loss or damage to third party tangible property; b. claim by any person in respect of bodily injury or death; c. claims by any third party in respect of any IP infringement; brought against or recovered from Indemnified Party by reasons of any act or omission of the Indemnifying Party, his agents or employees in the performance of the contractual obligation." We request removal of indemnity clause from NDA.		No Change
544	33	9.3 No liability	Exclusion of indirect damages		Request this to be made mutual - ie "Under no circumstances will either party shall be liable to the other for direct, indirect, incidental, consequential, special or exemplary damages arising from termination of this project, even if either party has been advised of the possibility of such damages, such as, but not limited to, loss of revenue or anticipated profits or lost business"		No Change
545	Absent	Limitation of Liability	Absent		Request to include indemnities under Section 9.2 within the LOL cap. We suggest the following instead: HPE suggests the following: "NOTWITHSTANDING ANYTHING TO THE CONTRARY ELSEWHERE CONTAINED IN THIS AGREEMENT, NEITHER PARTY SHALL, IN ANY EVENT, REGARDLESS OF THE FORM OF CLAIM, BE LIABLE FOR (1) ANY INDIRECT, SPECIAL, PUNITIVE, EXEMPLARY, SPECULATIVE OR CONSEQUENTIAL DAMAGES, INCLUDING, BUT NOT LIMITED TO, ANY LOSS OF USE, LOSS OF DATA, BUSINESS INTERRUPTION, AND LOSS OF INCOME OR PROFITS, IRRESPECTIVE OF WHETHER IT HAD AN ADVANCE NOTICE OF THE POSSIBILITY OF ANY SUCH DAMAGES; OR (2) DAMAGES RELATING TO ANY CLAIM THAT ACCRUED MORE THAN TWO (2) YEARS BEFORE THE INSTITUTION OF ADVERSARIAL PROCEEDINGS THEREON. The maximum liability, REGARDLESS OF THE FORM OF CLAIM, shall be limited to 100% of contract value except in case of fraud and/or wilful negligence. HPE shall not be liable for consequential losses on account of production revenue or profit.		No Change
546	34	9.5 Termination of Contract	Termination of contract		Request to insert termination for convenience for both parties of 90 days. We also request termination right for Bidder for non-payments by customer.		No Change
547	34	9.4 Extension of Contract Post Expiry	The Company desires to appoint the vendor for a total period specified in the RFP, considering the effort and investments required in the arrangement. However, understanding the complexities of the entire arrangement, Company would like to safe guard the interests of all the entities involved in the arrangement. Therefore, the Company would like to have options to revisit the arrangements and terms of contract as well as to re-price the same (rates similar or less than existing arrangement) after the contract expiry, if necessary.		Request to clarify that the rates / prices should be finalised after consultation and mutual agreement by both the parties.		No Change
548	36	9.5 Termination of Contract	The company shall recover all the cost of replacing vendor and or the company shall impose the liquidated damages.		Request to limit any cost of replacement of vendor up to 10% of the undelivered deliverables and request to delete the imposition of LD.		No Change

549	36	9.5 Termination of Contract	Reverse Transtion		Request payments for termination assistance and reverse transition services at mutually agreed rates / prices. Further all knowledge transfer and reverse transition services to be completed upon full payment for all deliverables.		No Change
550	37	9.6	Compliance with Laws		Please specify the laws, other than standard necessary and applicable labour laws, that are required to be complied.		required to be complied as mentioned in RFP
551	37	9.9	Inspection of Records		We submit that: Auditors shall NOT be given access to: 1.any information not related to the Services; 2.Bidder locations/premises (or portions thereof) that are not related to the Services; or 3.Bidder records or documents relating to the make up of Bidder's internal overhead calculations or direct costs, their relationship to the service charges, any financial cost model, calculation of service charges or Bidder's profitability; or 4. internal Bidder audit reports, or any summaries thereof. We require Independent Monitors to: 1. provide Bidder with at least thirty (30) days notice of its requirement for an audit allowed once in a year, with such notice describing the issue(s) that will be the subject of the audit; 2. be subject to Bidder site/premises security obligations and have their access controlled/monitored by Bidder; 3.pay all Bidder costs associated with the audit at current time and material rates and submit any requests for Bidder assistance with an audit as a change request. A third party auditor/inspector shall: 1. not be a competitor of Bidder or a third party in dispute / conflict with Bidder; 2. execute a confidentiality agreement acceptable to Bidder; 3. be independent.		No Change
552	39	9.12	Visitorial Rights		We submit that: Auditors shall NOT be given access to: 1.any information not related to the Services; 2.Bidder locations/premises (or portions thereof) that are not related to the Services; or 3.Bidder records or documents relating to the make up of Bidder's internal overhead calculations or direct costs, their relationship to the service charges, any financial cost model, calculation of service charges or Bidder's profitability; or 4. internal Bidder audit reports, or any summaries thereof. We require Independent Monitors to: 1. provide Bidder with at least thirty (30) days notice of its requirement for an audit allowed once in a year, with such notice describing the issue(s) that will be the subject of the audit; 2. be subject to Bidder site/premises security obligations and have their access controlled/monitored by Bidder; 3.pay all Bidder costs associated with the audit at current time and material rates and submit any requests for Bidder assistance with an audit as a change request. A third party auditor/inspector shall: 1. not be a competitor of Bidder or a third party in dispute / conflict with Bidder; 2. execute a confidentiality agreement acceptable to Bidder; 3. be independent.		No Change

553	39	9.13	Monitoring and Audit		We submit that: Auditors shall NOT be given access to: 1.any information not related to the Services; 2.Bidder locations/premises (or portions thereof) that are not related to the Services; or 3.Bidder records or documents relating to the make up of Bidder's internal overhead calculations or direct costs, their relationship to the service charges, any financial cost model, calculation of service charges or Bidder's profitability; or 4. internal Bidder audit reports, or any summaries thereof. We require Independent Monitors to: 1. provide Bidder with at least thirty (30) days notice of its requirement for an audit allowed once in a year, with such notice describing the issue(s) that will be the subject of the audit; 2. be subject to Bidder site/premises security obligations and have their access controlled/monitored by Bidder; 3.pay all Bidder costs associated with the audit at current time and material rates and submit any requests for Bidder assistance with an audit as a change request. A third party auditor/inspector shall: 1. not be a competitor of Bidder or a third party in dispute / conflict with Bidder; 2. execute a confidentiality agreement acceptable to Bidder; 3. be independent.		No Change
554	39	9.22 Addition/Deletion of Qualified Offerings	The selected bidder shall agree that the price for incremental offering cannot exceed the original proposed cost and the Company reserves the right to re-negotiate the price. At the unit rates provided for TCO calculations, the Company has the right to order as much as it wants at those rates. However, this excludes the hardware to be provided by the Bidder at their cost due to under sizing.		Request to include a clearly defined project scope of work and any changes to be captured by way of change requests at mutually discussed prices / charges.		The selected bidder shall agree that the price for incremental offering cannot exceed the original proposed cost and the Company reserves the right to re-negotiate the price. At the unit rates provided for TCO calculations, the Company has the right to order as much as it wants at those rates.
555	40	9.15	Force Majeure		Request to ensure that all payments to Bidder made up to date of force majeuere event for all deliverables provided.		Payments made to bidder will be as per BOBCARD payment clause

556	42	9.24 Liquidated Damages and penalty	The proposed rate of penalty would be 0.5% of the entire project cost/TCO per week of delay or non-compliance. Company at its discretion may apply this rule to any major non-delivery, non-adherence, non-conformity, non-submission of agreed or mandatory documents as part of the Project. II. Thereafter, at the discretion of the Company, the contract may be cancelled. Company also has the right to invoke the Performance Guarantee, Penalty Clause on delay which is not attributable to Company and is attributable to the selected Bidder. III. Inability of the selected bidder to provide services at the service levels defined would result in breach of contract and would invoke this clause. IV. Notwithstanding anything contained above, no such penalty will be chargeable on the selected bidder for the inability occasioned, if such inability is due to reasons entirely attributable to Company. V. The maximum amount that may be levied by way of penalty pursuant to clause above shall not exceed 10% of the Total Contract value.		Request to delete this clause as there are already penalties and indemnities in place.		The maximum amount that may be levied by way of penalty pursuant to clause above shall not exceed 5% of the Total Contract value. All clauses remain same
557	43	9.27	Sensitive Information		Please specify if this includes any PII.		Yes, not limited to only PII
558	42	9.25	Set-off		Request to ensure there is no inter-se set off and limited to this engagement only.		The maximum amount that may be levied by way of penalty pursuant to clause above shall not exceed 5% of the Total Contract value. All clauses remain same
559	46	9.32	Intellectual Property Rights		We submit that no transfer of ownership of any intellectual property will occur. Customer grants to us a non-exclusive, worldwide, royalty-free right and license to any intellectual property that is necessary for us and our designees to perform the ordered services. If deliverables are created by us specifically for Customer and identified as such, we grant to the Customer a worldwide, non-exclusive, fully paid, royalty-free license to reproduce and use copies of the deliverables internally upon full payments.		No Change
560	44	9.29	Confidentiality		Request to exlcude any PII from ths definition.		No Change
561	9 & 13	2.2 Tenure & Pont 17 in 3.1 Project Scope	The tenure of the contract initially would be for 1 year from the date of the issuance of first purchase order. BOBCARD can further extend to 2 years at its at mutually agreed terms. The initial term of this contract shall be 3 years and may be extended to another 2 years subject to satisfactory performance by successful bidder and OEM(s).		The two statements here are contradictory. Kindly provide clarification on the tenure of this contract.		Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
562	17	4. Service Levels	SLA Penalty Calculation: Deployment: In case of the Rollout delays by the Bidder the financial Penalty as per the BOBCARD discretion will be imposed on the Bidder at 0.5% of the total contract value per month of delay, to the maximum of 5% of the total contract value.		The Bidder requests that all penalties be capped at 5% of the affected/delayed value.		SLA Penalty Calculation: Deployment: In case of the Rollout delays by the Bidder the financial Penalty as per the BOBCARD discretion will be imposed on the Bidder at 0.5% of the total contract value per month of delay, to the maximum of 5% of the total First year value.

563	17 & 25	5.2 Price & 6.6 Validity of Bids	II. The prices and other terms offered by vendors must be firm for an acceptance period of 180 days from the opening of the commercial bid. The bids shall remain valid for a period of 180 days from the last date of submission of bids. All responses including commercial and technical bids would be deemed to be irrevocable offers/proposals from the Bidders and shall, if accepted by Company, form part of the final contract between Company and the selected Bidder. Company may seek further extensions of the bid validity, if required.		The Bidder requests that bid validity be 90 days from the last date of bid submission.	No Change
564	17	5.2 Price	IV. In case of any variation (upward or down ward) in Government levies / taxes / cess / excise / custom duty etc. which has been included as part of the price will be borne by the Vendor.		The Bidder requests that any variation(upward or down ward) in Government levies / taxes / cess / excise / custom duty etc. which has been included as part of the price after winning of the bid, be considered by the customer, considering that such changes occured post submission and are unforeseen.	No Change
565	31	8 Payment Terms	Activity- Supply of Software as prescribed under software requirement Timeline- Within 1 week - post confirmation from BOBCARD		Bidder requests that the timeline for this activity be amended to include a capping on the time taken for this activity. Bidder requests clarity on what is the timeline for confirmation from BOBCARD	Supply of Servers & Network component as prescribed under hardware requirement Within 6-8 weeks from date of PO. Rest all clause remain same
566	31	8 Payment Terms	1. Supply of Servers & Network component as prescribed under hardware requirement. Payment - 20% of Total Cost of Equipment outlined in BOM. 2. Supply of Software as prescribed under software requirement Payment- 20% of Total Cost of Equipment outlined in BOM. 3. Completion of rack mounting of Servers & Network component and Configuration. Implementation of Software Payment- 30% of Hardware and software licenses amount within 45 days from the date of acceptance of Tax Invoice by BOBCARD. 30% of one time implementation cost. 4. Acceptance / Go-live by BOBCARD Payment- Balance 50% of Hardware and software licenses amount and 70% of installation within 45 days from the date of acceptance of Tax Invoice by BOBCARD. 5. Annual Maintenance, Support / Subscription Renewal of Licenses and Hardware Payment- 100% payment on renewal of licenses support / subscription within 45 days from the date of acceptance of Tax Invoice by BOBCARD.		Bidder request that payment be amended as follows: 1. Supply of Servers & Network component as prescribed under hardware requirement. Payment- "70% of Supply of servers & network on delivery" 2. Supply of Software as prescribed under software requirement Payment- "80% of Supply of software on delivery" 3. Completion of rack mounting of Servers & Network component and Configuration. Implementation of Software Payment- "20% of Hardware and 10% of software licenses amount. 100% of one time implementation cost." 4. Acceptance / Go-live by BOBCARD Payment- "10% of Hardware & Software" 5. Annual Maintenance, Support / Subscription Renewal of Licenses and Hardware Payment- "100% payment on renewal of licenses support / subscription within 30 days from the date of invoice." 6. Support for the day-to-day operations Payment- "Monthly in arrears"	Supply of Servers & Network component as prescribed under hardware requirement Within 6-8 weeks from date of PO. Rest all clause remain same
567	32	8.1 Processing Charges	The Company will pay invoices within a period of 45 days from the date of receipt of undisputed invoices.		Bidder requests that payments be made within a period of 30 days from the date of the undisputed invoices.	No Change
568	1	Annexure 1 - Eligibility Criteria	Bidder should have experience of minimum 3 years in providing the Proposed Products/Services mentioned in the RFP.		Bidder request to consider folloiwng : Bidder should have experience of minimum 3 years in providing the Proposed / Similar Products/Services mentioned in the RFP. PO should have atlest one similar solutions required in the current RFP.	No Change

569	1	Annexure 02 Technical Evaluation Criteria	The bidder should have supplied and installed similar to proposed hardware in last three (3) financial years, i.e. 2021-2022, 2022-23, 2023-24 (Bidder to provide details in Annexure K and submit PO / Contract details)		Bidder requests to consider the following : The bidder should have supplied and installed similar to the proposed/ similar hardware in the last Five (5) financial years, i.e. 2019-2020,2020-2021,2021- 2022, 2022-23, 2023-24 (Bidder to provide details in Annexure K and submit PO / Contract details). The purchase order can have any of the similar solutions required in the current RFP. 2 deployments – 10 Marks More than 2 deployments– 15 Marks In case of OEMs part code bidder request to consider reference from its authorised partner	No Change
570	1	Annexure 02 Technical Evaluation Criteria	The bidder should have deployed and configured proposed software as per OEM standard on proposed hardware in last three (3) financial years, i.e. 2021-2022, 2022-23, 2023-24 (Bidder to provide details / submit PO / Contract details)		Bidder requests to consider following : The bidder should have deployed and configured proposed / Simialr software as per OEM standard on proposed / similar hardware in last Five (5) financial years, i.e. 2019-2020,2020-2021, 2021-2022, 2022-23, 2023-24 (Bidder to provide details / submit PO / Contract details) The purchase order can have any of the similar solutions required in the current RFP. 2 deployments – 10 Marks More than 2 deployments– 15 Marks	No Change
571	1	Annexure 02 Technical Evaluation Criteria	Presentation		Bidder request to cosnider 40 marks for presentation and technical capabilites	No Change
572		New	Project manager with total experience more than 10 years A. Educational Qualification: BE / B. Tech / MCA with MBA/M. Tech /PGDM/ or equivalent with Certification on PMP/ Prince Certification mark and Work experience in the capacity of Project/Program Manager in ICT implementation Projects (with more than 10 years of relevant experience) 5 Project Managers - 15 marks 4 Project Managers - 10 marks 3 Project Managers - 5 Marks		Bidder request to add this marking criteria	Bidder to decide the project manager criteria.
573		New	The bidder must have IT Security permanent professionals with experience in-scope solutions on their payroll with certifications such as CISSP / OSCP / CEH / CCNP / CISA / CISM / OEM Level Certification. 15 IT Security Professionals: 15 marks 10 IT Security Professionals: 10 marks 5 IT Security Professionals: 5 marks		Bidder request to add this marking criteria	Bidder to decide the project manager criteria.

574	7	7, Integrity Pact	Fall Clause- The BIDDER undertakes that it has not offered/is not offering similar product/systems or subsystems at a price lower than that offered in the present bid in respect of any other Ministry/Department of the Government of India or PSU or any other Bank and if it is found at any stage that similar product/systems or sub systems was supplied by the BIDDER to any other Ministry/Department of the Government of India or a PSU or a Bank at a lower price, then that very price, with due allowance for elapsed time, will be applicable to the present case and the difference in the cost would be refunded by the BIDDER to the COMPANY, if the contract has already been concluded.		Request to delete this clause from the Integrity Pact		No Change
575	17	4. Service Levels	SLA Penalty Calculation: Deployment: In case of the Rollout delays by the Bidder the financial Penalty as per the BOBCARD discretion will be imposed on the Bidder at 0.5% of the total contract value per month of delay, to the maximum of 5% of the total contract value.		Request to limit this to 5% of the undelivered or delayed deliverables only.		SLA Penalty Calculation: Deployment: In case of the Rollout delays by the Bidder the financial Penalty as per the BOBCARD discretion will be imposed on the Bidder at 0.5% of the total contract value per month of delay, to the maximum of 5% of the total First year value.
576	31	8 Payment terms	Absent		Request that all payments be made within 30 days of submission of the invoice		Supply of Servers & Network component as prescribed under hardware requirement Within 6-8 weeks from date of PO. Rest all clause remain same
577	32	9.2 Indemnity	Entire clause		We submit replacing the current language with the following: "The Indemnifying Party ("Bidder") shall defend (settle and/or pay damages awarded by the court) the Indemnified Party against any third party claims arising from the following: a. Claims for loss or damage to third party tangible property; b. claim by any person in respect of bodily injury or death; c. claims by any third party in respect of any IP infringement; brought against or recovered from Indemnified Party by reasons of any act or omission of the Indemnifying Party , his agents or employees in the performance of the contractual obligation." We request removal of indemnity clause from NDA.		No Change
578	33	9.3 No liability	Exclusion of indirect damages		Request this to be made mutual - ie "Under no circumstances will either party shall be liable to the other for direct, indirect, incidental, consequential, special or exemplary damages arising from termination of this project, even if either party has been advised of the possibility of such damages, such as, but not limited to, loss of revenue or anticipated profits or lost business"		No Change

579	Absent	Limitation of Liability	Absent		Request to include indemnities under Section 9.2 within the LOL cap. We suggest the following instead: HPE suggests the following: "NOTWITHSTANDING ANYTHING TO THE CONTRARY ELSEWHERE CONTAINED IN THIS AGREEMENT, NEITHER PARTY SHALL, IN ANY EVENT, REGARDLESS OF THE FORM OF CLAIM, BE LIABLE FOR (1) ANY INDIRECT, SPECIAL, PUNITIVE, EXEMPLARY, SPECULATIVE OR CONSEQUENTIAL DAMAGES, INCLUDING, BUT NOT LIMITED TO, ANY LOSS OF USE, LOSS OF DATA, BUSINESS INTERRUPTION, AND LOSS OF INCOME OR PROFITS, IRRESPECTIVE OF WHETHER IT HAD AN ADVANCE NOTICE OF THE POSSIBILITY OF ANY SUCH DAMAGES; OR (2) DAMAGES RELATING TO ANY CLAIM THAT ACCRUED MORE THAN TWO (2) YEARS BEFORE THE INSTITUTION OF ADVERSARIAL PROCEEDINGS THEREON. The maximum liability, REGARDLESS OF THE FORM OF CLAIM, shall be limited to 100% of contract value except in case of fraud and/or wilful negligence. HPE shall not be liable for consequential losses on account of production revenue or profit.		No Change
580	34	9.5 Termination of Contract	Termination of contract		Request to insert termination for convenience for both parties of 90 days. We also request termination right for Bidder for non-payments by customer.		No Change
581	34	9.4 Extension of Contract Post Expiry	The Company desires to appoint the vendor for a total period specified in the RFP, considering the effort and investments required in the arrangement. However, understanding the complexities of the entire arrangement, Company would like to safe guard the interests of all the entities involved in the arrangement. Therefore, the Company would like to have options to revisit the arrangements and terms of contract as well as to re-price the same (rates similar or less than existing arrangement) after the contract expiry, if necessary.		Request to clarify that the rates / prices should be finalised after consultation and mutual agreement by both the parties.		No Change
582	36	9.5 Termination of Contract	The company shall recover all the cost of replacing vendor and or the company shall impose the liquidated damages.		Request to limit any cost of replacement of vendor up to 10% of the undelivered deliverables and request to delete the imposition of LD.		No Change
583	36	9.5 Termination of Contract	Reverse Transtion		Request payments for termination assistance and reverse transition services at mutually agreed rates / prices. Further all knowledge transfer and reverse transition services to be completed upon full payment for all deliverables.		No Change
584	37	9.6	Compliance with Laws		Please specify the laws, other than standard necessary and applicable labour laws, that are required to be complied.		No Change

| 585 | 37 | 9.9 | Inspection of Records | | We submit that:
Auditors shall NOT be given access to:
1.any information not related to the Services;
2.Bidder locations/premises (or portions thereof) that are not related to the Services; or
3.Bidder records or documents relating to the make up of Bidder's internal overhead calculations or direct costs, their relationship to the service charges, any financial cost model, calculation of service charges or Bidder's profitability; or
4. internal Bidder audit reports, or any summaries thereof.
We require Independent Monitors to:
1. provide Bidder with at least thirty (30) days notice of its requirement for an audit allowed once in a year, with such notice describing the issue(s) that will be the subject of the audit;
2. be subject to Bidder site/premises security obligations and have their access controlled/monitored by Bidder;
3.pay all Bidder costs associated with the audit at current time and material rates and submit any requests for Bidder assistance with an audit as a change request.
A third party auditor/inspector shall:
1. not be a competitor of Bidder or a third party in dispute / conflict with Bidder;
2. execute a confidentiality agreement acceptable to Bidder;
3. be independent. | | No Change |
| 586 | 39 | 9.12 | Visitorial Rights | | We submit that:
Auditors shall NOT be given access to:
1.any information not related to the Services;
2.Bidder locations/premises (or portions thereof) that are not related to the Services; or
3.Bidder records or documents relating to the make up of Bidder's internal overhead calculations or direct costs, their relationship to the service charges, any financial cost model, calculation of service charges or Bidder's profitability; or
4. internal Bidder audit reports, or any summaries thereof.
We require Independent Monitors to:
1. provide Bidder with at least thirty (30) days notice of its requirement for an audit allowed once in a year, with such notice describing the issue(s) that will be the subject of the audit;
2. be subject to Bidder site/premises security obligations and have their access controlled/monitored by Bidder;
3.pay all Bidder costs associated with the audit at current time and material rates and submit any requests for Bidder assistance with an audit as a change request.
A third party auditor/inspector shall:
1. not be a competitor of Bidder or a third party in dispute / conflict with Bidder;
2. execute a confidentiality agreement acceptable to Bidder;
3. be independent. | | No Change |

587	39	9.13	Monitoring and Audit		We submit that: Auditors shall NOT be given access to: 1.any information not related to the Services; 2.Bidder locations/premises (or portions thereof) that are not related to the Services; or 3.Bidder records or documents relating to the make up of Bidder's internal overhead calculations or direct costs, their relationship to the service charges, any financial cost model, calculation of service charges or Bidder's profitability; or 4. internal Bidder audit reports, or any summaries thereof. We require Independent Monitors to: 1. provide Bidder with at least thirty (30) days notice of its requirement for an audit allowed once in a year, with such notice describing the issue(s) that will be the subject of the audit; 2. be subject to Bidder site/premises security obligations and have their access controlled/monitored by Bidder; 3.pay all Bidder costs associated with the audit at current time and material rates and submit any requests for Bidder assistance with an audit as a change request. A third party auditor/inspector shall: 1. not be a competitor of Bidder or a third party in dispute / conflict with Bidder; 2. execute a confidentiality agreement acceptable to Bidder; 3. be independent.		No Change
588	39	9.22 Addition/Deletion of Qualified Offerings	The selected bidder shall agree that the price for incremental offering cannot exceed the original proposed cost and the Company reserves the right to re-negotiate the price. At the unit rates provided for TCO calculations, the Company has the right to order as much as it wants at those rates. However, this excludes the hardware to be provided by the Bidder at their cost due to under sizing.		Request to include a clearly defined project scope of work and any changes to be captured by way of change requests at mutually discussed prices / charges.		The selected bidder shall agree that the price for incremental offering cannot exceed the original proposed cost and the Company reserves the right to re-negotiate the price. At the unit rates provided for TCO calculations, the Company has the right to order as much as it wants at those rates.
589	40	9.15	Force Majeure		Request to ensure that all payments to Bidder made up to date of force majeuere event for all deliverables provided.		Payments made to bidder will be as per BOBCARD payment clause

590	42	9.24 Liquidated Damages and penalty	The proposed rate of penalty would be 0.5% of the entire project cost/TCO per week of delay or non-compliance. Company at its discretion may apply this rule to any major non-delivery, non-adherence, non-conformity, non-submission of agreed or mandatory documents as part of the Project. II. Thereafter, at the discretion of the Company, the contract may be cancelled. Company also has the right to invoke the Performance Guarantee, Penalty Clause on delay which is not attributable to Company and is attributable to the selected Bidder. III. Inability of the selected bidder to provide services at the service levels defined would result in breach of contract and would invoke this clause. IV. Notwithstanding anything contained above, no such penalty will be chargeable on the selected bidder for the inability occasioned, if such inability is due to reasons entirely attributable to Company. V. The maximum amount that may be levied by way of penalty pursuant to clause above shall not exceed 10% of the Total Contract value.		Request to delete this clause as there are already penalties and indemnities in place.		The maximum amount that may be levied by way of penalty pursuant to clause above shall not exceed 5% of the Total Contract value. All clauses remain same
591	43	9.27	Sensitive Information		Please specify if this includes any PII.		Yes, not limited to only PII
592	42	9.25	Set-off		Request to ensure there is no inter-se set off and limited to this engagement only.		No Change
593	46	9.32	Intellectual Property Rights		We submit that no transfer of ownership of any intellectual property will occur. Customer grants to us a non-exclusive, worldwide, royalty-free right and license to any intellectual property that is necessary for us and our designees to perform the ordered services. If deliverables are created by us specifically for Customer and identified as such, we grant to the Customer a worldwide, non-exclusive, fully paid, royalty-free license to reproduce and use copies of the deliverables internally upon full payments.		No Change
594	44	9.29	Confidentiality		Request to exlcude any PII from ths definition.		No Change
595	31	8. Payment Terms	Activity	Payment			Supply of Servers & Network component as prescribed under hardware requirement Within 6-8 weeks from date of PO. Rest all clause remain same
596			Supply of Servers & Network component as prescribed under hardware requirement.	20% of Total Cost of Equipment outlined in BOM.	70% of Total Cost of Equipment outlined in BOM.		No Change
597			Supply of Software as prescribed under software requirement	20% of Total Cost of Equipment outlined in BOM.	70% of Total Cost of Equipment outlined in BOM.		No Change
598			Completion of rack mounting of Servers & Network component and Configuration. Implementation of Software	30% of Hardware and software licenses amount within 45 days from the date of acceptance of Tax Invoice by BOBCARD. 30% of one time implementation cost.	15% of Hardware and software licenses amount within 45 days from the date of acceptance of Tax Invoice by BOBCARD. 80% of one time implementation cost.		No Change
599			Acceptance / Go-live by BOBCARD	Balance 50% of Hardware and software licenses amount and 70% of installation within 45 days from the date of acceptance of Tax Invoice by BOBCARD.	Balance 15% of Hardware and software licenses amount and 20% of installation within 45 days from the date of acceptance of Tax Invoice by BOBCARD.		No Change

600	31	8. Payment Terms	Activity	Timeline		Supply of Servers & Network component as prescribed under hardware requirement Within 6-8 weeks from date of PO. Rest all clause remain same
601			Supply of Servers & Network component as prescribed under hardware requirement.	Within 5-6 weeks from date of PO	Within 6-8 weeks from date of PO	No Change
602			Supply of Software as prescribed under software requirement	Within 1 week – post confirmation from BOBCARD	Within 2 week – post confirmation from BOBCARD	Within 1-2 week – post confirmation from BOBCARD
603			Completion of rack mounting of Servers & Network component and Configuration. Implementation of Software	Within 4-6 weeks post-delivery of servers & Network Component	Within 6-8 weeks post-delivery of servers & Network Component	No Change
604		Annexure 02 Technical Evaluation Criteria	The bidder should have supplied and installed similar to proposed hardware in last three (3) financial years, i.e. 2021-2022, 2022-23, 2023-24 (Bidder to provide details in Annexure K and submit PO / Contract details)		We request to read the clause as "The bidder should have supplied and installed similar to proposed hardware (WAF/Firewall/ Server/Storage) (Bidder to provide details in Annexure K and submit PO / Contract details)"	The bidder should have supplied and installed proposed OEM hardware in last three (3) financial years, i.e. 2021-2022, 2022-23, 2023-24 (Bidder to provide details in Annexure K and
605			The bidder should have deployed and configured proposed software as per OEM standard on proposed hardware in last three (3) financial years, i.e. 2021-2022, 2022-23, 2023-24 (Bidder to provide details / submit PO / Contract	The bidder should have deployed and configured software(HCI/Virtuaization) as per OEM standard on hardware (Bidder to provide details / submit PO / Contract details)		The bidder should have deployed and configured proposed software as per OEM certified and standard hardware in last three (3) financial years, i.e. 2021-2022, 2022-23, 2023-24 (Bidder to provide details / submit PO / Contract
606		Virtual Platform Point 30		The proposed solution should be capable of adding additional combined server and storage components, seamlessly, with node owntime, to scale performance and capacity on demand.	There seems to be a typo in this point: Please confirm if the solution is expected to be capable of adding additional combined server compute and storage capacity with adding new nodes without any cluster downtime to scale the performance and capacity on demand Revised point: "The proposed solution should be capable of adding additional combined server and storage components, seamlessly, with no downtime, to scale performance and capacity on demand."		The proposed solution should be capable of adding additional combined server and storage components, seamlessly, with no downtime, to scale performance and capacity on demand.
607		Virtual Platform Point 2		The Bidder should provide 1 Technical Resource from Software OEM for a period of 1 Year to provide timely health check, suggest OEM best practice, conduct timely health check of the deployed solution and submit a report indicating	Please confirm if the Onsite resource which has been asked for needs to be a HCI Software OEM resource		Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
608		Appendix 03 Bill of Material Optional commercial Sr.no. 5		One year support cost of on site L3 resource (1 server & Virtual platform)	Please confirm if the Onsite resource which has been asked for needs to be a HCI Software OEM resource		Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
609		Appendix 02 Perimeter Firewall Point 15		Solution should have minimum 450 GB SSD pair, system storage	Requesting change as "SSD's are by default high performance drives with inbuilt resiliencey"	Request you to change the Point to "Solution should have minimum 450 GB SSD , system storage"	No Change
610		Internal Firewall Section 1 - NG Firewall Point 8		Should have the capability of passively gathering information about virtual machine traffic, network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance.	Host information like IP address, OS, MAC etc can be detected by Firewall Also, applications being access by host will be visible in Web filter logs. However, Open ports and vulnerabilities are usually inspected by 3rd party assessment tools and not by Firewall. Firewall can inspect traffic and detect if vulnerabilities are getting exploited by applying IPS signatures, Web filters and find exploitation attempts like C&C connections etc.	Hence request you to modify this clause as following Should have the capability of passively gathering information about virtual machine traffic / network hosts and their activities, such as operating system, services & ports being accessed, applications being accessed to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance.	Should have the capability of passively gathering information about virtual machine traffic / network hosts and their activities, such as operating system, services & ports being accessed, applications being accessed to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance

611		Internal Firewall Section 6 - Performance & Scalability Point 1		Shall support minimum 5 Gbps of NGFW throughput (Firewall + Application Visibility Control)	As there are IPS and malware inspection features also asked in the RFP specs, throughput requirement should be considered along with IPS, App control and AV, Malware inspection services, hence request you to modify this clause as below	Hence request you to modify this clause as following Shall support minimum 5 Gbps of threat prevention throughput (Firewall + Application Visibility Control + IPS+ Antivirus+ AntiMalware)	No Change, additional feature will be consider as value add
612		Internal Firewall Section 6 - Performance & Scalability Point 2		Solution should support at least 1.5 million concurrent sessions with Application Visibility Control.	Considering the throughput asked in the RFP specs, concurrent sessions support should be on higher side. This will ensure that Firewall would not compromise during the DDOS attack as it will have enough state table (concurrent connections and sessions per sec) to accomodate DDOS attack	Hence request you to modify this clause as following Solution should support at least 5 million concurrent sessions	No Change, additional new connection per second will be consider as value add
613		Internal Firewall Section 6 - Performance & Scalability Point 3		Solution should support at least 90,000 new connections per second with Application Visibility Control.	Considering the throughput asked in the RFP specs, concurrent sessions support should be on higher side. This will ensure that Firewall would not compromise during the DDOS attack as it will have enough state table (concurrent connections and sessions per sec) to accomodate DDOS attack	Hence request you to modify this clause as following Solution should support at least 400,000 new connections per second	No Change, additional new connection per second will be consider as value add
614		Internal Firewall Section 1 - NG Firewall Point 9		The Firewall solution Should support more than 4000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness and should be able to create 40 or more application categories for operational efficiency. Dedicated IPS solution shall be in corporated by the bidder to achive this scale of IPS AVC signatures in this solution.	Every OEM has their own methods of creating application signatures and seggregating them into different categories. Custom application signatures can be created on Fortigate, however categorization of signatures is done by threat intelligence engine i.e. Fortiguard.	Hence request you to modify this clause as following The Firewall solution Should support more than 4000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness. Dedicated IPS solution shall be in corporated by the bidder to achive this scale of IPS AVC signatures in this solution.	No Change, if required any additional component bidder can add it
615		Internal Firewall Section 1 - NG Firewall Point 10		Should be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention.	IPS signature tuning is typically done by threat intelligence engine as it requires large amount of resources like malware samples/IOCs etc.	Request you to modify this clause as below - Should be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) using threat intelligence engine with minimal human intervention.	No Change
616		Internal Firewall Section 1 - NG Firewall Point 11		The firewall solution should support at least 30,000 out of the box IPS signatures from Day 1. Should support capability to configure correlation rule where multiple rules/event can be combined together for better efficacy. Dedicated IPS solution shall be in corporated by the bidder to achive this scale of IPS signatures in this solution.	Every OEM has their own language for creating signatures and ways to optimize the number of signatures hence comparing number of signatures will not help to identify effectiveness of a Firewall. Instead, you can ask for 3rd party reports for testing Firewall effectiveness and performance. Also, dedicated IPS solution is asked in RFP, so please confirm whether IPS features needs to be considered for internal Firewall or not.	Request you to modify this clause as below- The firewall solution should support minimum 18,000 out of the box IPS signatures from Day 1. Should support capability to configure correlation rule where multiple rules/event can be combined together for better efficacy. Vendor should also ensure security effectiveness of the proposed solution to protect BOB's environment by providing 3rd party security testing reports like Cyber ratings / NSS labs	No Change
617		Internal Firewall Section 4 - Management platform and support Point 2		The management platform must be a dedicated OEM appliance and VM running on server will not be accepted.	It is recommended to use a Virtual machine as it provides ability to scale it in future when number of devices managed by management device increases. Hardware appliance will have a fix number of capacity in terms of devices being managed by it, which cannot be increased further.	Request you to modify this clause as below The management platform must be a dedicated OEM appliance or VM running on server. Required server hardware / resources should be provieded by the bidder.	No Change

| 618 | | Internal Firewall Section 4 - Management platform and support Point 4 | | The management appliance should have integrated redundant power supply from day one. | It is recommended to use a Virtual machine as it provides ability to scale it in future when number of devices managed by management device increases. Hardware appliance will have a fix number of capacity in terms of devices being managed by it, which cannot be increased further. | Request you to modify this clause as below

In case OEM hardware appliance for management is proposed, it should have integrated redundant power supply from day one. | No Change |
|---|---|---|---|---|---|---|---|
| 619 | | Internal Firewall Section 4 - Management platform and support Point 5 | | The management platform must be able to store record of at least 600,000 users or hosts. | Logging solution is sized based on the logs getting generated on Firewalls per day. | Request you to provide the expected log size getting generated on Firewall on per day bassis. (e.g 10 Gb, 50 Gb etc) | No Change. The management platform must be able to store record and have 1.5TB local Storage |
| 620 | | Internal Firewall Section 5 - Hardware Architecture Point 2 | | The appliance should support 8x1G Copper ports and 8*10G SFP+ ports on board plus option of having another 1/10G port 8 numbers for expansion | Considering the throughput asked in the specifications, number of ports ask is on very higher side. These many number of 10G ports are typically supported on appliances more than 10 Gbps Threat prevention capacity. | Request you to modify this clause as below

The appliance should support 8x1G Copper ports and 8*10G SFP+ ports on board plus option of having additional copper 1G port x 8 numbers for expansion or inbuilt additional 1G copper x 8 ports from day 1 | another 1/10G port 8 numbers for expansion will be consider as value add |
| 621 | | Internal Firewall Section 5 - Hardware Architecture Point 3 | | 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 8x64 GB of RAM. | Every OEM has a different hardware architecture and different ways of utilizing hardware resources like RAM / Flash.

RAM and CPU are not sizing parameters for any Firewall, it is usually considered for servers and storage. | Request you to modify this clause as below

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 16 GB of RAM. | 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. |
| 622 | | Internal Firewall Section 5 - Hardware Architecture Point 5 | | The appliance shall have redundant and hot swappable power supply and fan(s) module(s). | Redundant / Hotswappable fans are specific to one OEM

It is typically supported in very higher series appliances, hence request you to modify this clause | Request you to modify this clause as below

The appliance shall have redundant and hotswappable power supply | No Change |
| 623 | | Internal Firewall Section 1 - NG Firewall Point 28 | | Solution should be able to detect HTTP/3 and SMB over QUIC. Should detect applications over QUIC without enabling decryption. Should be able to assign access control rules based on the service detected over QUIC protocol. | It is recommended practice to enable SSL inpsection for better security controls, because some of the applications might not be detected without SSL inspection, regardless of any OEM technology.

Most of the today's applications runs over http and https, hence it will make more sense to run http / https traffic over QUIC protocol for better performance for roaming devices. | Hence request you to modify this clause as below -

Solution should be able to inspect and detect HTTP/3 and QUIC traffic. Should detect applications over QUIC. Should be able to assign access control rules based on the service detected over QUIC protocol. | Solution should be able to inspect and detect HTTP/3 and QUIC traffic. Should detect applications over QUIC. Should be able to assign access control rules based on the service detected over QUIC protocol. |

624		Internal Firewall Section 1 - NG Firewall Point 29		Solution should be able to generate indications of compromise (IoC) connection events based unsafe client applications detected by the system. IoC events should be triggered for encrypted sessions, without decryption, generated from a host using a malicious client. The system should capture the following information in the event viewer/dashboard "such as IP address, MAC address, and OS information of the malicious host, and the timestamp of the suspicious activity". The feature should work with all the TLS versions including TLS 1.3	It is recommended practice to enable SSL inpsection for better security controls, because not all the applications or threats can be detected without SSL inspection, regardless of any OEM technology. Also, information like MAC address, OS information can be available provided Firewall has reachability to users at layer 2	Hence request you to modify this clause as below - Solution should be able to generate indications of compromise (IoC) connection events based unsafe client applications detected by the system. IoC events should be triggered for sessions generated from a host using a malicious client. The system should capture the following information in the event viewer/dashboard "such as IP address, and OS information of the malicious host, and the timestamp of the suspicious activity". The feature should work with all the TLS versions including TLS 1.3	No Change
625		Internal Firewall Section 1 - NG Firewall Point 30		Solution should be able to block malicious communications in encrypted traffic based on threat score without decrypting the traffic. Solution should be able to reassemble fragmented Client Hello packets for detection purposes.	Without decryption, any Firewall has limited visibility into applications and threats and such limited visibility can also lead to false positives.	Hence request you to modify this clause as below - Solution should be able to block malicious communications in encrypted traffic based on threat score. Solution should be able to reassemble fragmented Client Hello packets for detection purposes.	No Change
626		Internal Firewall Section 1 - NG Firewall Point 31		Solution should be able to identify flows which are extremely large (in total bytes) flows measured over a network link. These flows are larger than 1 GB/10 seconds. Solution should be able to bypass and throttle these flows.	This clause is specific to the OEMs which do not support or has performance impact when processing large flows. This feature may be required in future to support high bandwidth sessions for east-west traffic	Hence Request you to either remove this clause or modify this clause as below Solution should be able to identify flows which are extremely large (in total bytes) flows measured over a network link. These flows are larger than 1 GB/10 seconds. Solution should be able to process these flows.	No Change
627		Internal Firewall Section 3 - Anti-APT Fearures Point 1		Should support the capability of providing network-based detection of malware by checking the disposition of unknown files using SHA-256 file-hash or signature (update to be provided in 300 seconds) as they transit the network and capability to do dynamic analysis.	If Sandboxing solution is required, it is recommended to enable inline sandboxing so that firewall can hold the file till the time Sandbox returns the verdict. This way Firewall will be able to avoid patient zero infection.	Hence request you to modify this clause as below - Should support the capability of providing network-based detection of malware by checking the disposition of unknown files using SHA-256 file-hash or signature (update to be provided in 300 seconds) as they transit the network and capability to do dynamic analysis using onprem hardware based sandbox. For dynamic analysis for files, Sandboxing solution is required. Please provide the sandbox sizing details - - Files needs to be scanned per hr - Number of Sandbox appliance in DC and DR We recommed to include below specification for sandboxing - 1) The solution should include onprem sandboxing appliance at DC and DR with required hardware, software and licenses included from Day-1.	No Change

628		Internal Firewall Section 4 - Management Platform and Support Point 9		The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows.	3rd party vulnerability exposures are managed by Fortiguard threat intelligence database on continuous bassis and required signatures are automatically pushed to Fortigate devices. Hence request you to modify this clause as following	The proposed solution must be capable of detecting third party vulnerability exposure and apply required signatures to Firewall policies to protect internal servers / apps from getting expoited	No Change
629		Internal Firewall Section 4 - Management Platform and Support Point 15		The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows.	Every OEM has different ways of sizing the solution. And for any logging appliance there would always be log capacity that it can handle. Logging solution is sized based on number of logs received on per day basis.	Hence request you to modify this clause as below - Solution should be able to provide insights of hosts/user on basis of indicators of compromise, any license required for this to be included from day one.	No Change
630		IPS Section 1 - Platform Requirement Point 3		The device should have functionality of in-built hardware based fail-open & software fail-open	Hardware based fail-open is OEM specific feature. We can propose IPS in HA to take care of redundancy part.	Hence request you to modify this clause as below - The device should have functionality of in-built software fail-open	No Change
631		IPS Section 2 - Performance and scalability Point 2		Solution should support at least 1.5 million concurrent sessions with Application Visibility Control.	Considering the throughput asked in the RFP specs, concurrent sessions support should be on higher side. This will ensure that Firewall would not compromise during the DDOS attack as it will have enough state table (concurrent connections and sessions per sec) to accomodate DDOS attack	Solution should support at least 2.5 million concurrent sessions	No Change, additional new connection per second will be consider as value add
632		IPS Section 2 - Performance and scalability Point 3		The appliance should support 8x1G Copper ports and 8*10G SFP+ ports on board plus option of having another 1/10G port 8 numbers for expansion	Considering the throughput asked in the specifications, number of ports ask is on very higher side. These many number of 10G ports are typically supported on appliances more than 10 Gbps Threat prevention capacity.	Hence request you to modify this clause as below - The appliance should support 8x1G Copper ports and 4*10G SFP+ ports on board and option of having additional 1G port x 8 numbers for expansion or inbuilt additional 1G copper x 8 ports from day 1	another 1/10G port 8 numbers for expansion will be consider as value add
633		IPS Section 3 - Features Point 1		Should have the capability of passively gathering information about virtual machine traffic, network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance.	Host information like IP address, OS, MAC etc can be detected by Firewall Also, applications being access by host will be visible in Web filter logs. However, Open ports and vulnerabilities are usually inspected by 3rd party assessment tools and not by Firewall. Firewall can inspect traffic and detect if vulnerabilities are getting exploited by applying IPS signatures, Web filters and find exploitation attempts like C&C connections etc.	Hence request you to modify this clause as following Should have the capability of passively gathering information about virtual machine traffic / network hosts and their activities, such as operating system, services & ports being accessed, applications being accessed to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance.	Should have the capability of passively gathering information about virtual machine traffic / network hosts and their activities, such as operating system, services & ports being accessed, applications being accessed to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance
634		IPS Section 3 - Features Point 2		Should be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention.	IPS signature tuning is typically done by threat intelligence engine as it requires large amount of resources like malware samples/IOCs etc.	Request you to modify this clause as below - Should be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) using threat intelligence engine with minimal human intervention.	No Change

635		IPS Section 3 - Features Point 16		Should support more than 50,000 (excluding custom signatures) IPS signatures or more	Every OEM has their own language for creating signatures and ways to optimize the number of signatures hence comparing number of signatures will not help to identify effectiveness of a IPS. Instead, we should ask for 3rd party reports for testing IPS effectiveness and performance.	Request you to modify this clause as below- The firewall solution should support minimum 18,000 out of the box IPS signatures from Day 1 and provide 3rd party security testing reports like Cyber ratings / NSS labs to ensure security effectiveness of the solution	No Change
636		IPS Section 3 - Features Point 26		Solution should be able to detect the operating system type and version of the client that initiated the TLS connection without decrypting the TLS traffic. The feature should work with all the TLS versions including TLS 1.3	It is recommended practice to enable SSL inpsection for better security controls, because some of the applications might not be detected without SSL inspection, regardless of any OEM technology.	Hence request you to modify this clause as below - Solution should be able to detect the operating system type and version of the client that initiated the TLS connection. The feature should work with all the TLS versions including TLS 1.3	No Change
637		IPS Section 3 - Features Point 27		Solution should be able to detect HTTP/3 and SMB over QUIC. Should detect applications over QUIC without enabling decryption. Should be able to assign access control rules based on the service detected over QUIC protocol.	It is recommended practice to enable SSL inpsection for better security controls, because some of the applications might not be detected without SSL inspection, regardless of any OEM technology. Most of the today's applications runs over http and https, hence it will make more sense to run http / https traffic over QUIC protocol for better performance for roaming devices.	Hence request you to modify this clause as below - Solution should be able to inspect and detect HTTP/3 and QUIC traffic. Should detect applications over QUIC. Should be able to assign access control rules based on the service detected over QUIC protocol.	Solution should be able to inspect and detect HTTP/3 and QUIC traffic. Should detect applications over QUIC. Should be able to assign access control rules based on the service detected over QUIC protocol.
638		IPS Section 3 - Features Point 28		Solution should be able to generate indications of compromise (IoC) connection events based unsafe client applications detected by the system. IoC events should be triggered for encrypted sessions, without decryption, generated from a host using a malicious client. The system should capture the following information in the event viewer/dashboard "such as IP address, MAC address, and OS information of the malicious host, and the timestamp of the suspicious activity". The feature should work with all the TLS versions including TLS 1.3	It is recommended practice to enable SSL inpsection for better security controls, because not all the applications or threats can be detected without SSL inspection, regardless of any OEM technology. Also, information like MAC address, OS information can be available provided Firewall has reachability to users at layer 2	Hence request you to modify this clause as below - Solution should be able to generate indications of compromise (IoC) connection events based unsafe client applications detected by the system. IoC events should be triggered for sessions generated from a host using a malicious client. The system should capture the following information in the event viewer/dashboard "such as IP address, and OS information of the malicious host, and the timestamp of the suspicious activity". The feature should work with all the TLS versions including TLS 1.3	No Change

639		IPS Section 3 - Features Point 29		Solution should be able to block malicious communications in encrypted traffic based on threat score without decrypting the traffic. Solution should be able to reassemble fragmented Client Hello packets for detection purposes.	Without decryption, any Firewall has limited visibility into applications and threats and such limited visibility can also lead to false positives.	Hence request you to modify this clause as below - Solution should be able to block malicious communications in encrypted traffic based on threat score. Solution should be able to reassemble fragmented Client Hello packets for detection purposes.	No Change
640		IPS Section 4 - Management Point 2		The management platform must be a dedicated OEM appliance and not VM	It is recommended to use a Virtual machine as it provides ability to scale it in future when number of devices managed by management device increases. Hardware appliance will have a fix number of capacity in terms of devices being managed by it, which cannot be increased further.	Request you to modify this clause as below The management platform must be a dedicated OEM appliance or VM running on server. Required server hardware / resources should be provieded by the bidder.	No Change
641		IPS Section 4 - Management Point 8		The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows	3rd party vulnerability exposures are managed by Fortiguard threat intelligence database on continuous bassis and required signatures are automatically pushed to Fortigate devices.	Hence request you to modify this clause as following The proposed solution must be capable of detecting third party vulnerability exposure and apply required signatures to Firewall policies to protect internal servers / apps from getting expoited	No Change
642	11	3.1 Project Scope Point #1		The supplied Hardware and Software shall be of the latest versions and should not be end of life / end of support for the next 7	Request the start Date for 7 Yrs mention in the clause be specified. Is it RFP Date or Date of PO Issuance/GoLive Date or something else?	Right tenure will help align the final BOM and any discrepent inpurs will impact pricing , so requesting clarification	The supplied Hardware and Software shall be of the latest versions and should not be end of life / end of support for the next 5 years from the date of
643	12	3.1 Project Scope Point #4		All Software licenses effective date shall be effective as on Go-LIVE sign off or put in use for BOBCARD operations.	Contract Start period is mentioned as PO Issuance while the SW licenses effective date is mentioed as GoLive Sign off Dates as noticed. Request Bank to keep this synchronized if this is genuine or clarify the intent	Right tenure will help align the final BOM and any discrepent inpurs will impact pricing , so requesting clarification	License effectiveness should be start from the software is ready to use. License cost will not impact to BOBCARD due to implementation delay. No license activate without informing BOBCARD.
644	12	3.1 Project Scope Point #12		Hardware RMA (Return Merchandise Authorization) should be within 24 hours	Request this be modified as below Hardware RMA (Return Merchandise Authorization) should be within 24 hours on Next business Day Basis.	RMA for a request raised on Friday may be honored by Monday due to the wekend in between , so requesting to keep this clearly specified.	Hardware RMA (Return Merchandise Authorization) should be within 24 hours on Next business Day Basis.
645	19	5.3 Price Comparisons Point #c iv		End of Sales/ End of support: The Vendor has to ensure that any application, related software supplied / put to use as part of this RFP should not have reached end of support. In the event	End of Life/End of Sale Clause here should specifiy the start date as to if PO issuance, RFP Date or any other . Further the tenure within which EOS/EOL should not happen must be mentioned like 7 years in clause Project Scope point #1	Right tenure will help align the final BOM and any discrepent inpurs will impact pricing , so requesting clarification	The supplied Hardware and Software shall be of the latest versions and should not be end of life / end of support for the next 5 years from the date of delivery
646	9	2.2 Tenure		The tenure of the contract initially would be for 1 year from the date of the issuance of first purchase order.	Contract Tenure mentioend 1 Year from PO Issuance here while its 3 years in clause 3.1 Point 17/ Pls clarify the right tenure?	Right tenure will help align the final BOM and any discrepent inpurs will impact pricing , so requesting clarification	Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live

647	13	3.1 Project Scope Point #17		The initial term of this contract shall be 3 years and may be extended to another 2 years subject to	Mentioned here is 3 years of initial contract and in 2.2 section the contract mentioned is 1 Year/ pls clarify the right tenure	Right tenure will help align the final BOM and any discrepent inpurs will impact pricing , so requesting clarification	Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
648	30	7.2 Evaluation Methodology for Eligible Bidder Commercial Bid Evaluation		The key considerations of the TCO would be the total payouts for entire project through the contract period of 5	Mentioned here is 5 years contract but in 2.2 the tenure of contrat is 1 Year, pls clarify the number to consider	Right tenure will help align the final BOM and any discrepent inpurs will impact pricing , so requesting clarification	Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
649	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Server Prod > HCI Rack Servers > 1		Total QTY is 14	Clarifictaion Needed: 1. Please provide split of quantity of servers / Nodes per location. 2. Kindly specify the number of clusters and nodes per cluster also.	clarifiction will help arrive at the boq rightly	This will be shared with only elected bidder
650	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Server Prod > HCI Rack Servers > 7		Each Rack Server Controller Cards / Controller Drive should be provided in HA mode in RAID -1.	Request Change: Each HCI Server should be configured with two BOOT drives with hardware RAID Controller. For NVMe storage drives: Provides as per Certifed HCI Node with NVMe configuration	From the HCI Rack server or Pre configured HCI NODE - RAID Controller card is not required for NVMe drives. Also, is this ask for Boot drive with RAID Controller?	Yes, we need boot drive for HCI hypervisor provided in HA mode in RAID -1
651	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Server UAT > HCI Rack Servers > 7		Each Rack Server Controller Cards / Controller Drive should be provided in HA mode in RAID -1.	Request Change: Each HCI Server should be configured with two BOOT drives with hardware RAID Controller. For NVMe storage drives: Provides as per Certifed HCI Node with NVMe configuration	From the HCI Rack server or Pre configured HCI NODE - RAID Controller card is not required for NVMe drives. Also, is this ask for Boot drive with RAID Controller?	Yes, we need boot drive for HCI hypervisor provided in HA mode in RAID -1
652	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Server Prod > HCI Rack Servers > 6		Each Rack servers should have minimum usable Storage Capacity of 10 TB of all caching SSD and other HDD. 20% disk slot on each node should be free for future expansion	Clarification needed: In virtualized environment, the storage (usable) capacity is calcluated across the cluster. Need clarification on the total capacity required across the number of nodes in a cluster.	clarifiction will help arrive at the boq rightly	as mentioned in RFP 10TB usable storage per node * no of node = total usable capacity
653	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Server UAT > HCI Rack Servers > 6		Each Rack servers should have minimum usable Storage Capacity of 10 TB of all caching SSD and other HDD. 20% disk slot on each node should be free for future expansion	Clarification needed: In virtualized environment, the storage (usable) capacity is calcluated across the cluster. Need clarification on the total capacity required across the number of nodes in a cluster.	clarifiction will help arrive at the boq rightly	as mentioned in RFP 10TB usable storage per node * no of node = total usable capacity
654	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Server Prod > HCI Rack Servers > 13 >Server Security		Request New Point to be added	Request to add the below point for security and management features for HCI Nodes Day2 operations and management of HCI Nodes for updates on Hardware and Software. HCI Node management tool should integrate with Virtual platform and Network switches. Should be able to do Firmware updates, Manage Cluster and deployment, Full stack visibility of HCI Node, TAC/Case Support, Continuous Health checks on Networking, Server, VMs , Anomalies detection, Security advisories, patch management etc.	HCI Node should integrate with Virtual platform and Network switches, Should have management software for a Firmware update, Manage Cluster and deployment, Full stack visibility HCI Node, TAC/Case Support, Continuous Health checks on Networking, Server, VMs , Anomalies detection, Security advisories, patch management,	No Change, additional feature will be consider as value add

655	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Server UAT > HCI Rack Servers > 13> Server Security		Request New Point to be added	Request to add the below point for security and management features for HCI Nodes Day2 operations and management of HCI Nodes for updates on Hardware and Software. HCI Node management tool should integrate with Virtual platform and Network switches. Should be able to do Firmware updates, Manage Cluster and deployment, Full stack visibility of HCI Node, TAC/Case Support, Continuous Health checks on Networking, Server, VMs , Anomalies detection, Security advisories, patch management etc.	HCI Node should integrate with Virtual platform and Network switches, Should have management software for a Firmware update, Manage Cluster and deployment, Full stack visibility HCI Node, TAC/Case Support, Continuous Health checks on Networking, Server, VMs , Anomalies detection, Security advisories, patch management,	No Change, additional feature will be consider as value add
656	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmentation > 1		The Solution should be capable of supporting major hardware OEMs like Juniper, Arista, Cisco, HPE and Dell. The proposed solution should be a purely software-based solution and should not be dependent on any hardware make and model.	Request below modified clause be considered: The Solution should be capable of supporting major hardware OEMs like Juniper, Arista, Cisco, HPE and Dell. The proposed solution should be a purely software-based solution and should not be dependent on any hardware make and model by creating overlay tunnels between the hosts.	The key benefits of no dependecy on hardware is by using software defined networking i.e overlay. Overlay is mandatory for network & Security automation as part of software defined data center.	No Change
657	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmentation > 2		The solution should provide a distributed firewall such that the firewalling for Virtual Machines can be provided closest to the application within the server itself without traffic going to a Physical Firewall.	Request below modified clause be considered which includes additonal points The solution should provide a distributed firewall such that the application aware and identity based statefull firewalling for Virtual Machines can be provided closest to the application within the server itself without traffic going to a Physical Firewall or regardless of underlying L2 Netwrork topology. The solution should also provide an integrated networking solution (CNI implementations) as well as provide advance turnkey container networking & firewalling services. Solution should support for container networking plug-ins, support for pod to pod communication and support for ingress controllers. The micro-segmentation solution should have a capability for stateful firewalling and ALGs (Application Level Gateway) on a per-workload granularity regardless of the underlying L2 network topology (i.e. possible on either logical network overlays or underlying VLANs), embedded in the hypervisor kernel, distributed	As per security framework its recommended not to use standard ports for your applications and hence to have effective security on per VM basis an application/L7 firewalling is must. Containers & Kubernetes are now part of all modern applications hence networing and security for container shall also be considered for end to end application security. there is App ID requirement is mentioned in RFP as part of "Internal Firewall" spec point # 23 hence same should be considered for mirosegmenation as well otherwise it will create non standard architecture.	No Change

658	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmenation >5		The proposed solution should provide the ability to define firewall rules at VM level for east-west traffic in order to implement Zero Trust Security	Request below modified clause be considered: The proposed solution should provide the ability to define Layer 7 application firewall rules at VM level for east-west traffic in order to implement Zero Trust Security alongwith URL Filtering and TLS inspection for encrypted traffic	Zero trust Security framework mandates TLS inspection for encrypted traffic, URL Filtering and Layer 7 application firewalling.	No Change
659	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmenation >4		The Proposed Solution including Hypervisor, SDS and Micro segmentation must be from the same OEM.	Request below modified clause be consideredL The Proposed Solution including Hypervisor, SDS, SDN and Micro segmentation must be from the same OEM.	SDN is missing in the spec, SDN will be mandatory to create complete automated Software Defined data center by creating an abstraction of the network enabling programming of network behavior in a centrally controlled manner through software applications.	No Change, SDN will be consider as value add
660	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmenation >6		The proposed solution should allow users to define granular firewall rules based on IP Addresses, Tags/Categories and Subnets to segment User Applications	Request below modified clause be considered which includes additonal points The proposed solution should allow users to define granular firewall rules for both VM and conatiners based on IP Addresses, VM Names, Tags/Categories and Subnets to segment User Applications by creating dynamic security groups. The solution should have capability to provide stateful micro-segmentation for virtual machines and Kubernetes workloads from a single console. The solution should also support enforcement of stateful distributed firewall for IPv6 VM workloads. These firewall rules can use IPv6 addresses, IPv6 CIDR, IP Sets that include both IPv4 and IPv6 addresses and security groups that can include logical ports that have both IPv4 and IPv6 addresses. IPv6 capability should be available both at management and data plane	Its necessary to have dynamic security group capability to ensure complete automation. Mentioned in the RFP page 8 -> 2.0 --> Requirement Summary--> 2.1 Intent--> mentions requirement for IPv6 "The proposed solution should support both IPv4 and IPv6."	No Change
661	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmenation >7		Solution should provide capability to create network segments by defining them entirely in software and avoid the need to re-architect your network or deploy physical appliances	Request below modified clause be accmodated: Solution should provide capability to create network segments and L2 Streching between DC and DR by defining them entirely in software and avoid the need to re-architect your network or deploy physical appliances	L2 Streching is required for better application availability considering RFP asks for 99.99 % availability on monthly basis. RFP Page 17 -> "4. Service Levels "-->"SLA: The solution is expected to be available for 99.99% on 24x7 and up time availability will be calculated on monthly basis."	No Change, L2 stretching implementation will be discuss with elected bidder.

662	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Container >2		The solution must be able to manage Kubernetes clusters. Licenses for managing Kubernetes clusters should be implemented from Day-1	Request below modified clause be accmodated: The solution must be able to manage Kubernetes clusters. Licenses for managing Kubernetes clusters along with components such as backup, container registry and monitoring alongwith Windows Container support should be implemented from Day-1	Kubernetes Cluster doesn't work in isloation but require other components such as container registry and backup solution. If not included than Bob Card will have procure them separately. And Not aving Windows Container support will block any windows based apps to be deployed on Kubernetes Platform.	Yes, BOBCARD will take care such requirement
663	NA	Appendix02 Techno Functional Requirements- Network components > internal FW NG Firewall Features NEW POINT		Must have provisioning, operations and lifecycle management of Kubernetes, automated deployment, scaling, and operation of Kubernetes clusters	Request below modified clause be accmodated: Must have provisioning, operations and lifecycle management of Kubernetes, automated deployment, Auto scaling & Auto Healing, and operation of Kubernetes clusters	Complete Automation is not possible without Auto Scaling and Auto Healing of Kubernetes Clusters. One has to manually add nodes in case of failure or unprovisioned increase in load.	No Change
664	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Container >4		Container Platform should provide single pane of Glass for Lifecycle Management of all K8S clusters deployed on prem.	Request below modified clause be accmodated: Container Platform should provide single pane of Glass for Lifecycle Management of all K8S clusters alongwith ingress, backup and container registry deployed on prem.	Kubernetes Cluster doesn't work in isloation but require other components such as container registry and backup solution. These shall too be considered for life cycle management	Yes, BOBCARD will take care such requirement
665	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management >1		The solution should provide capability of generating reports for usage, performance, compliance, health, forecasting and capacity.	Request below modified clause be accmodated: The solution should provide capability of generating reports for health, Capacity Optmization - Right Sizing (Under sized, Oversized), Reclamation (Idle, Powered off , Snapshot, Orphaned Disk , Forecasting - Capacity Forecasting, Migration assessment, Migration Planning Usage - Process and service utlization Compliance - Regulatory Benchmark (PCIDSS and ISO) Security Guidelines for Infrastructure and Cloud Management	Bob Cards will need capacity optimization capabilities to identify over-provisioned & under-provisioned resources and provide recommendations, alerts and automated actions on right-sizing and resource consumption so they can be right-sized for adequate performance and avoid resource wastage. Should provide visibility of capacity and VMs which can be reclaimed and cost visibility of the reclaimed capacity and VMs.	No Change, additional feature will be consider as value add

666	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management >11		The solution should have intelligent operations with anomaly detection which will allow monitoring seasonal trends and automatically send email alert	The solution should have AI/ML driven intelligent operations & troubleshooting workbench with anomaly detection,third party infra (Server, Storage , Network, database and Application) along with parent child relatiohship mapping, service and process monitoring which will allow monitoring seasonal trends and automatically send email alert. The solution should also have log management capability for infrastructure and applications . log management solution should delivers intuitive, actionable dashboards, sophisticated analytics, and broad third-party extensibility across physical, virtual, and cloud environments.	BoB Cards will not be able to manage the infrastructure without comprhesive log management capability. Its also mandatory for from regulation/compliance perspective to have log stored for given period of time for audit. BoB Card would need apps (database and Application) to infra (Server, Storage , Network) level visibility for toubleshooting and performance monitoring.	No Change, additional feature will be consider as value add
667	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management >7		The solution must have an approval process to review, reject or approve the deployment requests from the marketplace.	Request below modified clause be considered: The Solution must support multiple levels of approval with E-mail notifications with ability to automate manual provisioning and de-provisioning of the tasks and policies embedded in each layer of their application including auto -approve and auto-reject capability based on application criticality	The solution must have an approval process to review, multi level & auto reject or approve the deployment requests from the marketplace.	No Change, additional feature will be consider as value add
668	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 6		Hypervisor should support container and opensource integration for cloud native application from day-1. Must be a Kubernetes ready from day-1.	Request below modified clause be accmodated: Hypervisor should support container both Linux and Windows along with other kubernetes ecosystems such as container registry, backup, ingress & monitoring and opensource integration for cloud native application from day-1. Must be a Kubernetes ready from day-1.	Kubernetes does't work in isolation and requires multiple components for production setup.	Yes, BOBCARD will take care such requirement
669	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 16		Virtualization Manager should provide feature which can perform quick, as-needed deployment of additional virtualized hosts. When the service is running, it can push out update images, eliminating patching and update without impacting production.	Please clarify the scenario and expected outcome out of the below point in this clause: "When the service is running, it can push out update images, eliminating patching and update without impacting production."		No Change
670	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 22		Unlimited VM replication from DC to DR (No restriction on VM replication and DR orchestration) with the capability to define Recovery Plans	Request to provide the number of VMs to be orchestrated for automated recovery and not keep open as unlimited since this approach is OEM specific . The VMs to be protected/orchestrated are limited to what can be provisioned on these 14 servers of production. Furehr pls clarify the need for Recovery Plans		No Change, can not predict the exact number of VMs for next 5 Years which need to be replicated.

671	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 23		Proposed solution should have a self-service restore feature on a per-VM basis to allow trusted application administrators to recover their own files with the ability to mount snapshots as a drive in Windows VMs	Request this be modified as below or clarify the requriement: Proposed solution should have a self-service restore feature on a per-VM basis to allow trusted application administrators to recover their own VMs from the snapshot	Please clarify this requirement, this looks like back and restore requirements so the modified clause	No Change
672	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 24		Hypervisor should provide Visibility for Running VM and their connectivity co-relationship with Network Ports on attached Physical TOR / Core Direct which Include Network RX/TX Bytes.	Request below modified clause with additional inputs be considered : Hypervisor should provide Visibility for Running VM and their connectivity co-relationship with Network Ports on attached Physical TOR / Core Direct which Include Network RX/TX Bytes.Solution Should provide end to end visibility across physical firewall, switch and storage, Flow Analysis and Security Planning,Guided Troubleshooting, Microsegmentation planning, RCA (Connectivity Problem, Packet Loss, N/W latency), Application Discovery, Service Monitoring , Application Dependency Mapping and monitoring of non compliant ports	Monitoring is not considering all components of the stack. Unless end to end visibility is provided as part of this solution BoB Card has to spend separately on monitoring.	Yes, BOBCARD will take care such requirement. However Hypervisor should provide Visibility for Running VM and their connectivity co-relationship with Network Ports on attached Physical TOR / Core Direct which Include Network RX/TX Bytes.
673	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 30		Virtualization software or the solution should provide Cluster level encryption protects unauthorized data access at-rest.	Request below modified clause be considered : Virtualization software or the solution should provide Cluster level, VM Level encryption protects unauthorized data access at-rest and in transit.	Having capability to do the enscryption at app VM level and in transit is required to complete solution.	No Change, additional feature will be consider as value add
674	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Software Defined Storage > 1		Maintain primary working set copy of active data on the Local Node as VM's are hosted to provide high IOPS and low latency. Proposed solution must be proposed for faster reads and write for Business-critical Apps.	Request below additional point be added in theis clause : Proposed solution must be proposed for faster reads and write for Business-critical Apps.	Architecture is specific to one vendor, request BoB Cards to consider on outcome than specific architecture. There is no specific latency requirements mentioned in the spec.	No Change.
675	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Software Defined Storage >2		The solution must have De-duplication and Compression features licensed and implemented from day one (Should not have dependency on any proprietary hardware device).	Request below modified clause be considered: The solution must have De-duplication/Compression features licensed and implemented from day one (Should not have dependency on any proprietary hardware device).	Solution should have flexibility to implement either compression and de-duplication. BoB Cards should conisder overhead while deciding on both.	No Change
676	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Software Defined Storage >24		The proposed solution should support 1 min RPO & 1 hour RTO for critical workload in case BOB Cards wants to have this capability replication for Future use. The proposed solution should have native Replication and DR Orchestration from Day-1	What is the use case for 1 min RPO and 1 Hour RTO? is this linked with some regulatory requirement?	Replication is best handled at application level as having additional solution for infrastructure will complexity and cost for BoB Cards Its best to use extends the existing DR orchestration solution for this environment as well.	This is required for BOBCARD mission critical application. The solution should capable to support 1min RPO. The propose replication solution should be same OEM as the virtualization solution to provide seamless integration.

677	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Software Defined Storage >25		The solution provided should function even after one node failure.	Request below modified clause be considered: The solution provided should function even after two node failure.	RFP asks for 99.99 % availability SLA for the proposed solution. It will require minimum N+2 configuration for required resiliency and uptime.	No Change, additional feature will be consider as value add
678	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Software Defined Storage >31		The solution should provide enterprise data services such as compression completely in software. Software Defined Storage solution must have de-duplication and compression features Licensed and implemented from day one. These functionalities should be part of the proposed solution. The solution must have functionality to support compression and or deduplication online on data container without any downtime	Request below modified clause be considered: The solution should provide enterprise data services such as compression completely in software. Software Defined Storage solution must have de-duplication or compression features Licensed and implemented from day one. These functionalities should be part of the proposed solution. The solution must have functionality to support compression and or deduplication online on data container without any downtime and data loss as per business requirement.	Solution should have flexibility to implement either compression and de-duplication. BoB Cards should conisder overhead while deciding on both.	No Change
679	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmentation > new point		Additional Point for consideration	The solution must ensure that there is not alteration in the IP address of the Virtual machine, by blocking the traffic from or to the VM inherited as a feature in the Solution.	IP/MAC spoofing is major security concern for organizations like BoB Cards handing customers data.	No Change, additional feature will be consider as value add
680	NA				The solution should support multi-tenancy to isolate networking/security for different departments/function within BoB Cards upto a minimum of 4 tenants and 5 VPCs	VPC will enable Bob Cards to create isolation from access , resources, network and security.	ange, additional feature will be consider as valu
681	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Container > 6		Should support cluster scale out i.e addition of worker nodes as and when required.	Request below modified clause be considered: Should support Automated cluster scale out i.e addition of worker nodes as and when required.	Complete Automation is not possible without Auto Scaling and Auto Healing of Kubernetes Clusters. One has to manually add nodes in case of failure or unprovisioned increase in load.	No Change, additional feature will be consider as value add
682	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > 3		The solution shall provide a single pane of glass for automated provisioning with model-based orchestration of compute, network and storage through a unified multi-tenant self-service catalog.	Request below modified clause be consiered The solution shall provide a single pane of glass for automated provisioning with model-based orchestration of compute, network , storage and Kubernetes through a unified multi-tenant self-service catalog .	All modern applications are combination of both container and VM form factor.	No Change, additional feature will be consider as value add
683	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > 5		The solution must provide a self-service portal to allow user to consume the creation of infrastructure easily.	Request below modified clause be considered: The solution must provide a self-service portal to allow user to consume the creation of infrastructure easily for both VM and Kubernetes	All modern applications are combination of both container and VM form factor.	No Change, additional feature will be consider as value add
684	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > 8		The software must allow the designer to use shell script, PowerShell script to code the automation.	Request below modified clause be considered: The software must allow the designer to use shell script, PowerShell script, Python and node JS to code the automation.	Python and nodeJs are very popular language for scrpting in terms resource availability and community support	No Change, additional feature will be consider as value add

685	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > 9		The software must allow the designer to design VM blueprints.	Request below modified clause be considered: The software must allow the designer to design Multi VM & Kubernetes blueprints.	All modern applications are combination of both container and VM form factor.	No Change, additional feature will be consider as value add
686	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > 12		The solution should have simple low-code, no-code automation engine which allows automating day-to-day routine tasks	Request below modified clause and adidtoinal inpurs on the clause be considered: The solution should have simple low-code, no-code automation engine which allows automating day-to-day routine tasks such as Snapshot creation, Addition of Disk, Power Cycle (Suspend , Shutdown, Reboot, reset), Resize, Rebuild, Additional of Network, VM Unregister , Delete,connect remote console, Change Security Group with capability to create additional resource actions as out of the box capability.	All modern applications are combination of both container and VM form factor.	No Change, additional feature will be consider as value add
687	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > New Point		New Point	Solution should provide capability to define and showcase cost to create cloud like experience to the business unit with the overall cost spend on the infrastructure [server hardware, storage, licenses, application, maintenance, labor, network, facilities , etc.	Bob Cards will need Cost transparency (Showback and Chargeback capability) across private, hybrid to optimize planning and prioritization of VM/ Server/Application onboarding/provisioning	No Change, additional feature will be consider as value add
688	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF & IPS		New Point	We request BoB Card to allow for both software and hardware based solution for Load Balancer, WAF, IPS/IDS. As these components are dynamic as per application consumption requirements and considering bob card is directly managing customer data, its very critcal that these components are added as part of sofwate defined stack.	Modern applications increasingly require software-defined networking (SDN) and security solutions due to their need for greater flexibility, agility, and scalability. Traditional networking and security methods often lack the adaptability to support the dynamic nature of modern application environments, especially in cloud	No Change
689	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF C.Solution Capabilites Pont #5		The solution must support and integrate the web application vulnurability tools (Web application scanners) being proposed by bidder as part of this RFP at minimum to virtually patch web application vulnurabilies or else solution should have ready plug-ins to integrate banks VAPT tool.	Requesting you to modify the clause as below: The solution must support and integrate the web application vulnurability tools (Web application scanners) being proposed by bidder as part of this RFP, solution should have ready plug-ins to integrate banks VAPT tool.	Solution should be capable to protect against zero-day vulnerability using positive security model without being dependent on virtual patching. Virtual patch can even lead to false positive.	No Change
690	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #2		Appliance/Chassis based Hardware should support scalability with license upgrade. -18 vCPU from day 1	Scalable to 32 vCPU -128 GB DDR RAM from day 1 -1 TB X 1 SSD M.2 SSD (in Raid)	The clause represents single OEM offering for sizing		No Change

691	NA	7/B.Hardware & InAppendix02 Techno Functional Requirements-Network components > LB+WAF B.Hardware & Interfaces requirement Point #7		The proposed appliance shoulde provide minimum 1.2 Gbps of real world WAF throughput from day 1 and should be scalable to 2.2 Gbps with license upgrade on the same hardware or additional blades in case of a chassis based solution. The WAF throughput	The clause represents single OEM offering for sizing		No Change
692	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #8		The appliance should support the layer 7 throughput should be at least 58 Gbps scalable to 92 Gbps on same hardware with license upgrade. (Data rerernces for above should be verified from publicly available	The clause represents single OEM offering for sizing		No Change
693	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #9		The proposed appliance must have minimum hardware compression of 34 Gbps for HTTP traffic form day 1 and scalable upto 48 Gbps with add on license on same hardware. (Data rerernces for above should	The clause represents single OEM offering for sizing		No Change
694	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #10		The proposed appliance should support minimum hardware based SSL offloading from day 1 up to : 34 Gbps Scalable upto 48 Gbps on same hardware with license upgrade. (The SSL encryption & decryption	The clause represents single OEM offering for sizing		No Change
695	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #11		The solution must support minimum SSL TPS/CPS: -29 K ECDSA P-256-bit keys from day 1 -58 K RSA 2048-bit keys from day 1 scalable to minimum SSL	The clause represents single OEM offering for sizing		No Change
696	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #12		The proposed appliance should support minimum 74 million L4 concurrent connections from day one and scalable upto 99 Million on same hardware with license upgrade.	The clause represents single OEM offering for sizing		No Change
697	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #13			The clause represents single OEM offering for sizing		No Change
698	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF General Requirement Point #13		The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide traffic performance statistics for last 30 days including Active Connections, Active Sessions, CPU Usage By Core, HTTP	The clause should mention the functionality should be achieved without being dependent on tools.	The clause represents single OEM offering.	No Change
699	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #14		The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide a security event timeline dashboard where critical events like Audit logs, Pool status change, Failover status change, DOS attacks etc. must be	The clause should mention the functionality should be achieved without being dependent on tools.	The clause represents single OEM offering.	No Change

700	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #15		The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide a Bug tracker option, where an admin can login and find any bugs affecting the devices	The clause should mention the functionality should be achieved without being dependent on tools.	The clause represents single OEM offering.	No Change
701	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #16		The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide an upgrade Options suggestions for next hotfix and stability release for ease of day-2 operations with single click access to release notes a nd EOS	The clause should mention the functionality should be achieved without being dependent on tools.	The clause represents single OEM offering.	No Change
702	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #17		The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide an ability to execute CLI commands which are essential for diagnostics which will show historic data or data at the time of file captured. E.g show	Request you to remove this clause	Database Load Balancer is provided as inbuilt feature from database solution provider and hence not needed from SLB solution	No Change
703	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF C.Solution Capabilities Point #23		Solution should have the capability to highlight (In red / any color code) only malicious payload from the entire attack payload on the event analysis dashboard for detailed fornsics analysis. This is extermly critical when our incident response teams are in combat with the attackers during wartime.	Forensics are not required for LB or WAF kind of solution. This is required for DDoS kind of solution and it is not recommended to have DDoS solution within WAF+LB as DDoS should be a stateless technology and it's placement should be at perimeter level above firewall to protect complete infrastruture		No Change
704	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF C.Solution Capabilities Point #36		The Proposed WAF Solution should provide built-in L7 layer DDoS detection and mitigation features based on machine learning and behavioral analytics and dynamic signatures. It should have CAPTCHA support or other mechanism to avoid distributed attack. This feature/functionality has to be	Request to remove this point	DDoS should be a stateless device and it's placement should be at perimeter level above firewall. This ensures protection to network from any advanced DDoS attacks. Hence, it should not be expected to be part of other security solutions within the network.	No Change
705	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF C.Solution Capabilities Point #58		The Solution should have IPSEC tunneling capabiltiies	Request to remove this point	VPN is recommended to be a dedicated solution since it relies on TLS protocol. It is also recommended to terminate the traffic on Firewall or before Firewall as it will check for security parameters on the same. If this is done on ADC, there won't be any security check and can possess threat or security flaw.	No Change
706	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF C.Solution Capabilities Point #59		The proposed solution should support a comprehensive list of ways in which LB can monitor the backend services including Daimeter, DNS, FTP, Gateway ICMP, HTTP, HTTPS, TCP half open, TCP , LDAP, MSSQL, MYSQL, MQTT , POSTGRESQL, POP3 , IMAP, NNTP, Radius , SIP and custom external scripts	Request to modify the clause as below: The proposed solution should support a comprehensive list of ways in which LB can monitor the backend services including DNS, FTP, Gateway ICMP, HTTP, HTTPS, TCP half open, TCP , LDAP, MSSQL, MYSQL , POSTGRESQL, POP3 , IMAP, NNTP, Radius and custom external scripts	SIP, Diameter & MQTT Traffic are used in Service Provider environment and are not relevant and used in any Enterprise environment like BOB Cards.	No Change

707	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF C.Solution Capabilities Point #61		The proposed solution should support various types of LB config for handling traffic, including standard reverse proxy, forwarding in L2 , Forwarding in IP, High performance mode, Stateless mode , Reject mode, DHCP relay, and Message routing for SIP, Diameter and MQTT traffic.	Request this clause be modified as below: The proposed solution should support various types of LB config for handling traffic, including standard reverse proxy, forwarding in L2 , Forwarding in IP, High performance mode, Stateless mode , Reject mode, DHCP relay	SIP, Diameter & MQTT Traffic are used in Service Provider environment and are not relevant and used in any Enterprise environment like BOB Cards.	No Change
708	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF C.Solution Capabilities Point #70		The proposed solution should support native integration with kubernetes based platforms hosting microservices e.g. Openshift, TKG cluster etc. Solution should update the configuration of LB automatically	Solution should be able to support by means of same solution.		No Change
709	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF C.Solution Capabilities Point #81		The proposed LB solution should also support secure remote access to admin users (concurrency of not more than 10); where the solution can do endpoint checks for the admins and establist a secure tunnel with autentication	The clause represents single OEM offering.		No Change
710	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF D.Availability #2		The solution should support SQL-based querying for the following databases for the health checks: for Oracle, MSSQL, MySQL, PostgresSQL and other databases if required in future.	Request this clause be removed	Database Load Balancer is provided as inbuilt feature from database solution provider and this is proprietary load balancing feature of Database solution provider and hence not needed from ADC solution.	No Change
711	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #7		The Firewall appliance should have certifications like ICSA /EAL4/CCNDPP	Request this be modified as below: The Firewall solution should have certifications like ICSA /EAL4/CCNDPP	Every OEM has its own solution offering and certification ask may align to the approach solution is provided rather than mandating it on the appliance inline to a particular OEM	No Change
712	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #9		OEM/Bidder should provide below transceivers from Day-1. Firewall and SFP should be from same OEM. Below mentioned SFP quantity is required per appliance. 4 X 10GE SR SFP+	OEM/Bidder should provide below transceivers from Day-1. Firewall and SFP should be from same OEM. Below mentioned SFP quantity is required per appliance. 4 X 1G RJ 45 4 X 10G SFP+ 4 x 25G SFP28	Requesting if 1G can be considered using Copper Links and not SFP	No Change
713	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #15		Solution should have minimum 450 GB SSD pair, system storage	Request to modify this as below Solution should have minimum 900 GB SSD pair, system storage	Perimeter Firewall needs high storage numbers as visible with mid/large scale deployments for storing logs considering 3/6 months retention in case the remote Management device is impacted , so good to ask for more	No Change, additional feature will consider as value add
714	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #16		Solution should have minimum 32 GB	Request clause to be modifiedL Solution should have minimum 128 GB RAM	Perimeter Firewall has to have good RAM and such baselining will help with operations of critical banking infra	No Change, additional feature will consider as value add

715	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #19		"The proposed firewall must provide minimum 10 Gbps of Threat prevention throughput with Real world traffic. (Throughput must be derived from Appmix traffic and not Video/JPEG based traffic) (enterprise testing condition). The throughput must remain 10 Gbps even after enabling NGFW + IPS/IDS + Antivirus + Anti Spyware + Anti Bot + DoS/DDOS + All signature enabled + Logging enabled + Bidirectional inspection + File Blocking. OEM to provide publicly available The Test methodology and result should be compliant to the benchmark testing methodology for the above parameters provided in the Internet Engineering Task Force (IETF)- 'Benchmarking Methodology for	Request below modified clause be considered , instead of Appmix traffic , real world traffic should be mentioned for deriving throughput "The proposed firewall must provide minimum 10 Gbps of Threat prevention throughput with Real world traffic. (Throughput must be derived from real world traffic and not Video/JPEG based traffic) (enterprise testing condition). The throughput must remain 10 Gbps even after enabling NGFW + IPS/IDS + Antivirus + Anti Spyware + Anti Bot + DoS/DDOS + All signature enabled + Logging enabled + Bidirectional inspection + File Blocking. OEM to provide publicly available The Test methodology and result should be compliant to the benchmark testing methodology for the above parameters provided in the Internet Engineering Task Force (IETF)- 'Benchmarking Methodology for Network Security Device	instead of appmix traffic real world traffic will be rifht measure of throuhgput , so requesting the change	No Change
716	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #21		NGFW appliance must be capable of handling minimum 2 M concurrent sessions utilizing HTTP transactions with all Security feature Turned ON and not based on UDP / Lab environment / ideal testing environment, this claim has to be supported with declaration of concurrent connections claim from OEM	Request below modified clause to accomodate support for 5M concurrent sessions NGFW appliance must be capable of handling minimum 5 M concurrent sessions utilizing HTTP transactions with all Security feature Turned ON and not based on UDP / Lab environment / ideal testing environment, this claim has to be supported with declaration of concurrent connections claim from OEM	Mid/Large scale deployments need higher concurrent session support and baselining this to 50 Lakh concurrent sessions will be in the interest of the Bank , so the requested change	No Change, additional feature will consider as value add
717	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #49		Solution should support creation of minimum 1 virtual context / instance from Day-1 without any compromise on system performance and network bandwidth.	Solution should support creation of minimum 5 virtual context /instance from Day-1 without any compromise on system performance and network bandwidth.	Support for only 1 Virtual context may not be scalable for the DC design and min support for 5 instances is the need for any DC infra Perimeter Firewall understanding furture state architecure and growing needs.	No Change, additional feature will consider as value add

718	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #54		The proposed NGFW solution architecture should have Control Plane separated from the Data Plane in the Firewall appliance architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup, QoS, NAT etc). Control plane must have dedicated resources such as CPU, RAM etc. This is to ensure Bank always has management access to NGFW irrespective of Firewall load / Traffic Spike / Cyber Attack driving higher CPU utilization. Bank should able to login to the firewall and carry out reporting /	Request below modified clause be considered The proposed NGFW solution architecture should have Control Plane separated from the Data Plane in the Firewall solution architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup, QoS, NAT etc). Control plane must have dedicated resources such as CPU, RAM etc. This is to ensure Bank always has management access to NGFW irrespective of Firewall load / Traffic Spike / Cyber Attack driving higher CPU utilization. Bank should able to login to the firewall and carry out reporting / management / packet capture etc to identify the root cause and accordingly take necessary action to remediate it.	OEMs have different approaches to achieving the use case and instead of the ask on the appliance itself , the Firewall Solution will be a generic term to use in requirements so this suggestion	No Change
719	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #72		IPS should provide detailed information on each protection, including: Vulnerability and threat descriptions, Threat severity, Performance impact, Release date, Industry Reference, Confidence level etc.	Request below changed clause : IPS should provide detailed information on each protection, including: Vulnerability and threat descriptions, Threat severity, Release date, etc	Performance impact, industry reference and confidence level are subject to configuration and infrastructure in the bank.	No Change
720	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #76		Should have more than 60+ predefined Categories based on Urls, Application types, Security Risk level etc. However solution should be able to create custom categories for URL and application.	Request below modified clause with increased number of categories: Should have more than 80+ predefined Categories based on Urls, Application types, Security Risk level etc. However solution should be able to create custom categories for URL and application.	Having more predefined categories support would help bank with improved threat detection and better granular policy control with less manual effort.	No Change, additional feature will consider as value add
721	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #89		Solution should give information related to Performance impact and confidence level of protections while creating profiles.	Request this clause be deleted	performance can be subject to policy configurations and existing infra at bank.	No Change

722	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #114		"Management server should support the following for rule optimization: • Unused Rules Calculation for specific time-period based on Firewall Traffic Logs. • Analysis on Covered/Shadow/Hidden Rules • Analysis on Rules Consolidation (Merging of similar kind of rules) • Analysis on Redundant Rules • Tightening of Overly Permissive Rules (Any-Any)	"Management server should support the following for rule optimization: • Unused Rules Calculation for specific time-period based on Firewall Traffic Logs / HIt count • Analysis on Covered/Shadow/Hidden Rules • Analysis on Redundant Rules • Analysis on Unattached/Unused Objects to simplify objects management • Analysis on Disabled/Expired Rules for enhanced visibility on the Firewall Rules sets"	OEMs could be handling the use case suggested for removal differently or have no dependency on the performance of the Firewall , so requesting these be removed from the ask	No Change
723	NA	Appendix02 Techno Functional Requirements- Network components > IPS Features Point #15		Should support more than 3000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security	Should support more than 5000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness	Increasing number of signature support is beneficial for the Bank's operations and for Effective Security reasons	No Change
724	NA	Appendix02 Techno Functional Requirements- Network components > internal FW Point #11		The Firewall solution Should support more than 4000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness and should be able to create 40 or more application categories for operational efficiency. Dedicated IPS solution shall be in corporated by the bidder to achive this scale of IPS	Request this clause be modfied as below: The Firewall solution Should support more than 6000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness and should be able to create 40 or more application categories for operational efficiency. Dedicated IPS solution shall be in corporated by the bidder to achive this scale of IPS AVC signatures in this solution.	Increasing number of signature support is Beneficial for the Bank's operations and for Effective Security reasons	No Change, additional feature will consider as value add
725	NA	Appendix02 Techno Functional Requirements- Network components > internal FW NG Firewall Features NEW POINT		New Point to be added	The solution should provide Change Management capability for the organizations needs to implement more formal processes for configuration changes, including audit tracking and official approval before changes are deployed.	By leveraging these features and integrating with external change management tools, organizations can implement a robust change management process that includes formal approval, audit tracking, and compliance reporting within Cisco FMC.	No Change
726	NA				The solution should provide traffic hit count, Rule Conflict Detection (Redundant & Shadowed) and policy warning for streamlining firewall policies.	These features are crucial for optimizing firewall policies, ensuring efficient traffic flow, and maintaining security posture.	No Change, additional feature will be consider as value add
727	NA	Appendix02 Techno Functional Requirements- Network components > internal FW Hardware Architecture Point #3		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 8x64 GB of RAM.	Request below modified clause be considered as correction on the ask which seems typo: 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.		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.

728	NA	Appendix02 Techno Functional Requirements- Network components > Mngmt Switch 6 Product Support Point #2		The OEM support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support	Request below modified clause be considered The OEM/OEM certified partner support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support	OEM Certified partner has thorough experience of OS version upgrades and maintaining network operations troubleshooting issues and it will be cost effective to include this in the ask	The OEM/OEM certified partner support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support
729	NA	Appendix02 Techno Functional Requirements- Network components > Mngmt Switch 9 Miscellaneous Points Point #1		Console cable and power cable (As per Indian standards) as per customer requirement to be provided. All Cables shall be factory-terminated.	Since Console Cables are common for all devices per OEM , Request Bank to clarify the count of console cables to be provided , is it one each with each Switch or one per DC and DR Each ?.		No Change
730	NA	Appendix02 Techno Functional Requirements- Network components > Mngmt Switch 10 Product Support Point #2		The OEM support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support	Request below modified clause be considered The OEM/OEM certified partner support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support	OEM Certified partner has thorough experience of OS version upgrades and maintaining network operations troubleshooting issues and it will be cost effective to include this in the ask	The OEM/OEM certified partner support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support
731	NA	Appendix02 Techno Functional Requirements- Network components > Core Swtich >9 Manageability > Appliance point 9.4		Switch Anomolies related with Advisories , PSIRT and Field Notices	Request this clause be removed from the telemetry asks	This feature is not requireed for the design at the BOB DataCenter and may be removed	No Change
732	NA	Appendix02 Techno Functional Requirements- Network components > Core Swtich >13 Fabric Management > Appliance point 13.1		Solution must provide Centralized Management Appliance – Single pane of glass for managing, monitoring and provisioning the entire Solution within Data Center & across all Data Centers	Request BOBCards to provide VM compute resources for spinning up the VMs to provide this functionality while we can provide the necessary sw and support.		Requested product functionality should be comply, BOBCards will provide VM compute resources for spinning up the VMs to provide this functionality however bidder should provide the necessary sw and support.
733	NA	Appendix02 Techno Functional Requirements- Network components > Core Swtich >5 Layer 2 Features > Appliance point 5.11		Switch Hardware should have capability to support BGP EVPN Route Type 1, Type 2, Type 3, Type 4, Route Type 5, Type 6/Type 7/Equivalent routes	Request this point be removed	BOBCards design doesn't have Fabric so this is not applicable	No Change
734	NA	Appendix02 Techno Functional Requirements- Network components > Core Swtich >13 Fabric Management > Appliance point 13.36		Solution should provides reports using predefined templates, including inventory, use, and health reports.	Request below modified clause be considered: Solution should provides reports including inventory, use, and health reports.		No Change
735	8	2. Requirements Summary 2.1 Intent	The successful bidder will be expected to provide all the components mentioned in the RFP along with required necessary tools, hardware and software licenses to implement as complete cloud platform solution to run VMs on this setup. Provide training for all proposed Hardware and Software to BOBCARD IT Team and handover the solution.		Is bidder expected to provide class room based handson traing. If yes then please share no. of participants for the same.		Training need to be provided in BOBCARD Office inperson for implemented solution.

736	8	2. Requirements Summary 2.1 Intent	The price quoted by the bidder should cover all the support to the solution including any updates/upgrades and fixing any issues faced. Bidder should provide onsite support to fix the issues for the period of 1 Year. Remote access would not be permitted for any support / training / change / upgrade / patch management etc		Is bidder expected to provide class room based handson traing. If yes then please share no. of participants for the same.		Training need to be provided in BOBCARD Office inperson for implemented solution.
737	8	2. Requirements Summary 2.1 Intent	Acceptance: A one-month test period will be used by BOBCARD to evaluate the implemented Solution. After the implemented solution has been successfully tested, BOBCARD and the Bidder shall agree on the Go-LIVE date.		We understand that during this one month period operation SLA are not applicable. Please confirm.		Yes, SLA is not applicable only for uptime.
738	8	2. Requirements Summary 2.1 Intent	The bidder shall assign dedicated Project Manager and associated support personnel for this project onsite.		We understand that Project Manager and associated personnel need to be onsite during project related activities, not all the time. Pls confirm.		The bidder shall assign dedicated Project Manager and associated support personnel for this project onsite during the implementation, support / training / change / upgrade / patch management etc
739	9	2. Requirements Summary 2.1 Intent	Bidder should provide 1year of hand holding support post Go-Live, this may extend to 2 years on mutual understanding.		Is bidder expected to deploy onsite resources for hand holding. Please confirm.		Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
740	9	2. Requirements Summary 2.1 Intent	Bidder should provide 1year of hand holding support post Go-Live, this may extend to 2 years on mutual understanding.		If its onside hand holding, please confirm the resource type to be deployed for the same i.e. L1, L2 or L3		Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
741	9	2. Requirements Summary 2.1 Intent	Bidder should provide 1year of hand holding support post Go-Live, this may extend to 2 years on mutual understanding.		If its onside hand holding, please confirm the number of hours the resource to be deployed per day.		Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
742	9	2. Requirements Summary 2.1 Intent	Bidder is expected to train the administrator/business users till the personnel gain enough expertise in the system and capable of taking over the operational function. The training should include features, facilities, operations, implementation, troubleshooting, system administration and DR elements if any.		Is bidder expected to provide class room based handson traing. If yes then please share no. of participants for the same.		Training need to be provided in BOBCARD Office inperson for implemented solution.
743	9	2. Requirements Summary 2.1 Intent	The tenure of the contract initially would be for 1 year from the date of the issuance of first purchase order. BOBCARD can further extend to 2 years at its at mutually agreed terms.		As per clause no. of the 17 under 3.1 Project Scope "The initial term of this contract shall be 3 years and may be extended to another 2 years subject to satisfactory performance by successful bidder and OEM(s).". Please confirm initial contract period i.e. 1 year or 2 Yeras.		Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
744	9	2. Requirements Summary 2.5 Training	The Bidder is required to provide training to the BOBCARD team on the proposed solution in RFP for Procurement of Servers, Network & Software components, provide a training schedule and furnish training details as per the RFP requirements for all major components.		Is bidder expected to provide class room based handson traing. If yes then please share no. of participants for the same.		Training need to be provided in BOBCARD Office inperson for implemented solution.
745	10	3.1 Project Scope	The successful bidder shall provide all necessary back-to-back support from OEM(s) for delivery, installation, configuration, testing, operationalisation and support of the respective Hardware and Software components (appliances, softwares etc.).		Is bidder expected to involve OEM for deployment of the proposed solution. Pls confirm.		Bidder to decide.
746	12	3.1 Project Scope	7. The successful bidder should also integrate existing infrastructure setup (like existing LAN, proxy, MFA, SIEM) with the new devices to be supplied.		Pls share make & model of proxy, MFA, SIEM		This will be market leading product only. Basis on compatibility Bidder has to integrate the existing infra setup with new setup. All the product will be share only with the final bidder

747	12	3.1 Project Scope	8. All required configuration to integrate with existing setup should be taken care of by bidder.		Pls share details of existing setup		This will be market leading product only. Basis on compatibility Bidder has to integrate the existing infra setup with new setup. All the product will be share only with the final bidder
748	13	3.1 Project Scope	16. L2 and L3 onsite support post implementation a. Software upgradation b. Hardware Upgradation c. Mass Changes for compliance d. Major, minor changes in feature/functionality roll out on the same infrastructure.		For how long L2 and L3 onsite support is required. Please confirm.		Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
749	15	3.1 Project Scope Knowledge Transfer (KT)	2. The KT should include the architecture, software, integration, customization, deployment guidelines, troubleshooting reporting and other aspects of the solution (if applicable). The Successful bidder should train BOBCARD personnel for independent operation, creation of policies/rules, generation of reports, and analysis of the reports, troubleshooting and familiarization of features, policy configuration etc. post implementation		Is bidder expected to provide class room based handson traing. If yes then please share no. of participants for the same.		One time Training need to be provided in BOBCARD Office inperson for implemented solution. Training can be given by OEM/Bidder, trainer must be certified resource.
750	15	3.1 Project Scope Go-Live	5. The successful bidder shall operate the deployed system for four weeks (after GO-Live) to fix all the implementation issues without any additional cost to BOBCARD.		Is bidder expected to operate the deployed system for four weeks (after GO-LIVE) with required resources in all three shifts (24x7 basis). Please confirm.		Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
751	17	4. Service Levels System Down	2hrs onwards to 8hrs During Business hours, in a single day - 2.5% of Quarterly Support Cost		As per RFP clause "SLA: The solution is expected to be available for 99.99% on 24x7 and up time / availability will be calculated on monthly basis.". Since solution uptime clause is addressing the RFP requirement, additional "System Down" clauseseems to be redundant. Request you remove the same.		No Change
752		Appendix 03 Bill of Material	Appendix 03 Bill of Material		We understand that Rack Space & passive cabling will be supplied by BOBCARD. Please confirm.		yes, Rack space & passive cabling will be supplied by BOBCARD
753		Appendix02 Techno Functional Requirements- Network components	The Router should support multi-core Processor, internal redundant field replaceable power supply (from Day1). The Router Should have capabilities of seamless field upgrade/replacement for PSU and Fan		Please share power cord type required i.e. Indian Standerd or ICE standerd		All devices must be compatible with Power cord for PDU with IEC-60320 C13-14 or C-19/20 cord ends
754		Appendix02 Techno Functional Requirements- Network components	Switch should be capable to support internal field replaceable and hot swappable redundant power supply		Please share power cord type required i.e. Indian Standerd or ICE standerd		All devices must be compatible with Power cord for PDU with IEC-60320 C13-14 or C-19/20 cord ends
755		Appendix02 Techno Functional Requirements- Network components	Switch should be provided with redundant power supply units		Please confirm which type of airflow is to be provisioned i.e. Port Side Intake or Port Side Exhaust		Port Side Intake
756		Appendix 03 Bill of Material	Core Switch: 12 Nos.		Please details of the appliances/Device to which proposed core switches will be uplinked.		This will be shared only with elected Bidder
757	8	2.1	The successful bidder will be expected to provide all the components mentioned in the RFP along with required necessary tools, hardware and software licenses to implement as complete cloud platform solution to run VMs on this setup. Provide training for all proposed Hardware and Software to BOBCARD IT Team and handover the solution.		Do we need to provide professional training from OEM or handover session will be provided to BOBCARD team.		Professional training from Bidder/OEM will be provided to BOBCARD team. Training need to be provided in BOBCARD Office inperson for implemented solution.
758			Do you need any migration P2V or V2V from OLD setup to New infra.				Yes, migration P2V or V2V from OLD setup to New infra is required and this Migration is in bidders scope.
759			Any third party software integration with new infra?		Backup, replication or orchestration software intrgration?		Yes
760			Does Guest OS deployment and configuration to be done by bidder or BOBCARD team on both Production and UAT clusters?				Yes, this will be part of 1 year manage service.

761			No. of VMs to be configured on Production and UAT servers?				As mentioned in this corrigendum
762			Guest OS licenses would be provided by BOBCARD.		(Yes/No)		Yes
763			Do you need hypervisor to be hardened while moved into production?				All the Devices & Software need to be harden before go live. (either BOBCARD Hardening policy or CIS bench mark)
764			Please share the workload compute requirement details to size virtualization nodes?				required node mentioned in BOM
765			What will be the IOPS requirement for the Prod and UAT solution?				This will be shared only with elected Bidder
766			What are the workload will be running on these virtualized nodes?				This will be shared only with elected Bidder
767			what will be the growth per year to be considered in Production and UAT workload?				This will be shared only with elected Bidder
768			Is there any integration with public cloud?		(Yes/No)		Yes
769	17	5.2 Price	IV. In case of any variation (upward or down ward) in Government levies / taxes / cess / excise / custom duty etc. which has been included as part of the price will be borne by the Vendor. Variation would also include the introduction of any new tax / cess/ excise, etc provided that the benefit or burden of other taxes quoted separately as part of the commercial bid like GST and any taxes introduced instead of Service tax, VAT and levies associated to Service Tax, VAT or any new taxes (other than excise, custom duties, other duties and associated government levies) introduced after the submission of vendor's proposal shall be passed on or adjusted to the Company. Local entry tax and octroi will be paid on actuals based on receipt provided. If the Vendor makes any conditional or vague offers, without conforming to these guidelines, the company will treat the prices quoted as in conformity with these guidelines and proceed accordingly. Local entry taxes / octroi whichever is applicable, if any, will be paid by the Bank on production of relative invoices / payment receipts / documents. Necessary documentary evidence should be produced for having paid the customs / excise duty, sales tax, if applicable, and or other applicable levies		The bidder does not have any control over Government levies / taxes / cess / excise / custom duty etc. Hence incase of any revision in these factors the bidder requests the prices to be revised to the extent of revision of these factors.		No Change
770	19	5.4 Bid Security and Performance Guarantee	Bidders are required to submit a Bid Security/ Earnest Money Deposit (EMD) for Rupees 5 Lac by way of RTGS/Online transfer (Appendix 06 – Bank Details for EMD & Tender Fees).		Kindly request BoB Cardto allow EMD submission in form of Bank Guarantee.		No Change
771	31	8. Payment Terms	The payment terms defined in RFP for product supply are as below: - Hardware Supply – 20% of Delivered Material - Software Supply – 20% of Delivered Material - Rack Mounting and Software Implementation – 30% Acceptance / Go-Live – 50%		Kindly request BOBCARD to revise the payment terms for product supply as per industry standard defined below: - Hardware Supply – 70% of Delivered Material - Software Supply – 70% of Delivered Material - Rack Mounting and Software Implementation – 20% - Acceptance / Go-Live – 10%		Supply of Servers & Network component as prescribed under hardware requirement Within 6-8 weeks from date of PO. Rest all clause remain same

772	42	9.22 Addition/Deletion of Qualified Offerings	2. The selected bidder shall agree that the price for incremental offering cannot exceed the original proposed cost and the Company reserves the right to re-negotiate the price. At the unit rates provided for TCO calculations, the Company has the right to order as much as it wants at those rates. However, this excludes the hardware to be provided by the Bidder at their cost due to under sizing.		The prices are dependant on Taxes, Duties (including Custom Duty), Levies, USD-INR exchange rate, OEM list prices, OEM discounting etc. These factors are not within bidder's control and hence request BOBCARD to allow for prices prevailing at the time of additional order. This prices can be higher than the contracted price due to the prevailing market conditions.		No Change
773	42	9.24 Liquidated Damages and penalty	The proposed rate of penalty would be 0.5% of the entire project cost/TCO per week of delay or non-compliance.		The RFP mentions two different penalty - 0.5% for per week of delay and 0.5% per month of delay. Kindly request BOBCARD to clarify whether penalty of 0.5% will be levied for every week of delay or every month of delay.		0.5% per month of delay basis on this penalty for every week delay will be calculated.
774	43	9.24 Liquidated Damages and penalty	V. The maximum amount that may be levied by way of penalty pursuant to clause above shall not exceed 10% of the Total Contract value.		The maximum penalty levy in RFP is mentioned as 5% as well as 10%. Kindly clarify on the maximum applicable penalty in RFP.		The maximum amount that may be levied by way of penalty pursuant to clause above shall not exceed 5% of the Total Contract value. All clauses remain same
775	32	9.1	Entire clause on Indemnity		Principle of Indemnity is used for providing a remeady where parties do not have a direct remeady against each other. For situations where there is a remeady availble at the disposal of the Parties, the due process of establishing a claim and dispute resolution shall be followed. Hence considering the scope of services, only Indemnity relevant is an Indemnity on 3rd party claims for breach of Intellectual Property RIghts	Indemnity across the document shall be restricted to only 3rd party claims arising out of breach of Intellectual Property Rights.	No Change
776	34	9.3	All employees engaged by the Service Provider shall be in sole employment of the Service Provider and the Service Provider shall be solely responsible for their salaries, wages, statutory payments etc. That under no circumstances shall company be liable for any payment or claim or compensation (including but not limited to compensation on account of injury/death/termination) of any nature to the employees and personnel of the Service Provider		Company cannot have an absolute disclaimer of liability. This means that Company shall not be liable for any claims of injury, etc. even if caused due to Company's fault.	All employees engaged by the Service Provider shall be in sole employment of the Service Provider and the Service Provider shall be solely responsible for their salaries, wages, statutory payments etc. That unless otherwise caused due to negligence or mis-conduct of the Company or it's personnel, Company shall not be liable for any payment or claim or compensation (including but not limited to compensation on account of injury/death/termination) of any nature to the employees and personnel of the Service Provider	No Change
777	35	9.5.4	IV. Any other reason.		Termination for cause as well an convenience is already covered. What does this envisage then. Notice period and cure period is also not specified for this sub clause. This this mean that without assigning any reason contract can be terminated at a days notice.	Clarification requested	No Change

#							
778	NA	NA	NA		Every commercial contract has a Limitation of Liability clause which is a fundamental clause in any commercial arrangement. We did not find any Limitation of Liability clause hence proposing a new one as mentioned in the Adjacent Column.	NOTWITHSTANDING ANYTHING ELSE CONTAINED HEREIN OR ANY OTHER DOCUMENT TO THE MAXIMUM EXTENT ALLOWED BY LOCAL LAWS, THE MAXIMUM AGGREGATE LIABILITY OF EITHER PARTY UNDER THIS AGREEMENT IRRESPECTIVE OF WHETHER IT ARISES UNDER CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY, INDEMNITY, OR OTHER LEGAL THEORY SHALL BE LIMITED TO PROVEN DIRECT DAMAGES AND SHALL NOT EXCEED CHARGES PAID OR PAYABLE BY THE COMPANY FOR SUCH GOODS AND/ OR IMPACTED SERVICES IN THE 12 MONTHS IMMEDIATELY PRECEDING THE DATE OF THE ACT OR OMISSION GIVING RISE TO THE CLAIM . THE FOREGOING SHALL NOT LIMIT A PARTY'S LIABILITY FOR BODILY INJURY OR DEATH ARISING FROM PARTY'S NEGLIGENCE. IN NO EVENT SHALL EITHER PARTY BE LIABLE TO THE OTHER FOR ANY INCIDENTAL, CONSEQUENTIAL, OR ANY OTHER INDIRECT LOSS OR DAMAGE (INCLUDING BUT NOT LIMITED TO LOST PROFITS OR REVENUES, WASTED TIME AND EXPENDITURE, LOSS OF ANTICIPATED PROFIT OR EARNING, LOSS OF OPPORTUNITY, LOSS OF USE, GOODWILL AND REPUTATION AND LOSS OF DATA), NOR FOR EXEMPLARY OR PUNITIVE DAMAGES. THESE	No Change
779	Annexure 1	4	The Bidder should be profitable organization for all three financial years mentioned in above.		The Bidder should be profitable organization in atleast 2 out of three financial years mentioned in above.	The Bidder should be profitable organization in atleast 2 out of three financial years mentioned in above and should have positive networth in all three years.	The Bidder should be profitable organization in atleast 2 out of 3 financial years mentioned in above. 2023-24 is mandatory
780		Virtual Platform / Pt 30	The proposed solution should be capable of adding additional combined server and storage components, seamlessly, with node owntime, to scale performance and capacity on demand.		There seems to be a typo in this point: Please confirm if the solution is expected to be capable of adding additional combined server compute and storage capacity with adding new nodes without any cluster downtime to scale the performance and capacity on demand Revised point: "The proposed solution should be capable of adding additional combined server and storage components, seamlessly, with no downtime, to scale performance and		The proposed solution should be capable of adding additional combined server and storage components, seamlessly, with no downtime, to scale performance and capacity on demand.
781		Virtual Platform / Pt 2	The Bidder should provide 1 Technical Resource from Software OEM for a period of 1 Year to provide timely health check, suggest OEM best practice, conduct timely health check of the deployed solution and submit a report indicating OEM best practices.		Please confirm if the Onsite resource which has been asked for needs to be a HCI Software OEM resource		Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
782		Appendix 03 Bill of Material / Optional commercial / Sr.no. 5	One year support cost of on site L3 resource (1 server & Virtual platform)		Please confirm if the Onsite resource which has been asked for needs to be a HCI Software OEM resource		Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
783	10	section 2.5	The Bidder is required to provide training to the BOBCARD team on the proposed solution in RFP for Procurement of Servers, Network & Software components, provide a training schedule and furnish training details as per the RFP requirements for all major components.		Please confirm the following - - Tranining to be done onsite, if yes please confirm the location and no of participants for the training - Is it a one time training or we need to provide yearly training		One time Training need to be provided in BOBCARD Office inperson for implemented solution. Training can be given by OEM/Bidder, trainer must be certified resource.

784	12	7		The successful bidder should also integrate existing infrastructure setup (like existing LAN, proxy, MFA, SIEM) with the new devices to be supplied.	Please clarify the use case for Firewall, IPS and WAF for integration with proxy as this will help us to understand if there is feasibility of integration available		This will be market leading product only. Basis on compatibility Bidder has to integrate the existing infra setup with new setup. All the product will be share only with the final bidder
785	12	7		The successful bidder should also integrate existing infrastructure setup (like existing LAN, proxy, MFA, SIEM) with the new devices to be supplied.	Please clarify which MFA solution is used by BOBCards and what is the use case for integration. This will help us to understand if there is feasibility of integration ith proposed Firewall, WAF and IPS		This will be market leading product only. Basis on compatibility Bidder has to integrate the existing infra setup with new setup. All the product will be share only with the final bidder
786	12	10		All the devices to be hosted should support both IPv4 and IPv6 Interlinks between the devices should be on minimum 10G/25G ports and there should be resiliency between the devices. All possible high availability scenarios should be considered.	Our understanding is for all proposed Firewall (perimeter and internal), WAF and IPS, we need to propose a appliance which has either 10G or 25G slot available for future expansion over and above the port requirement mentioned in "annexure 2 techno function requirement - network components". Card and transreceiver will be procured by BOBCard in future if required. Please confirm		Bidder has to comply with ask mentioned in Annexure 2
787	12	11		The resolution time for the hardware/software related issues should be 4 hours, there should be 24*7*365 support from the OEM for all the supplied products through this RFP.	Point 12 mentions hardware RMA should be within 24hrs. It will not be possible to resolve the issue within 4 hrs if RMA will take 24 hrs. Also, at time the issue ocuured would have dependency on OEM (eg - critical bug fix)	Hence request you to revise the clause as below - The resolution time for the hardware/software related issues should be 24 to 48 hours, there should be 24*7*365 support from the OEM for all the supplied products through this RFP.	No Change.
788	12	17		The initial term of this contract shall be 3 years and may be extended to another 2 years subject to satisfactory performance by successful bidder and OEM(s).	Page 9, section 2.2 mentions the contract tenure ill be for 1 year whwre this clause mentions for 3 years. Please clarify		Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
789		Appendix02 - Techno functional requirements - network components - WAF+LB - point no 11		The proposed WAF Solution should be deployed in minimun Five banks & NBFC in India in last three years having more than 200+ branches. The OEM/bidder should produce the completion certificate for the same	This clause should be part of eligibility or scoring rather than technical specification where the ASK can be for OEM reference to ensure OEM has sifficient experience of deploying and bidder reference of deploying in similar verticals	Request you to revise the clause as below - OEM Experience The proposed WAF Solution should be deployed in minimun Three Organizations in BFSI segment in last five years. The OEM should produce the completion certificate for the same Bidder Experience Bidder should have experience of depoying similar WAF solution in minimum Two Oragnizations in BFSI segment in India in last five years. Bidder should produce the completion certificate for the same	OEM Experience The proposed WAF Solution should be deployed in minimum Three Organizations in BFSI segment in last three years. The OEM should produce the completion certificate for the same Bidder Experience Bidder should have experience of deploying proposed WAF solution. rest will be consider as per evaluation criteria.
790		Appendix02 - Techno functional requirements - network components - internal firewall - section 6 - point 1		Shall support minimum 5 Gbps of NGFW throughput (Firewall + Application Visibility Control)	section 5- point 1 mentions to provide firewall, AVC, IPS and Anti-APT functionality from day 1 and also there is ask for URL filtering whereas this clause mentions to provide throughput by enabling only firewall and AVC. Hence please clarify what parameters needs to be considered for NGFW throughout		Shall support minimum 5 Gbps of NGFW throughput (Firewall + Application Visibility Control)
791		Appendix02 - Techno functional requirements - network components - internal firewall - section 5 - point 1		The solution should provide firewall, AVC, IPS and Anti-APT functionality in a single appliance from day one. The product licensing should be device-based and not user/IP based (should support unlimited users except for VPN).	There is a ASK for a dedicated IPS and also requirement for IPS in internal firewall and perimeter firewall. Our understanding is IPS is for the DMZ segment. Hence we can offload IPS functionality from perimeter firewall. Kindly clarify		No Change
792		Appendix02-Perimeter Firewall - point no 15		Solution should have minimum 450 GB SSD pair, system storage	Requesting change as "SSD's are by default high performance drives with inbuilt resiliencey" Request you to change the Point to "Solution should have minimum 450 GB SSD , system storage"	Request you to change the Point to "Solution should have minimum 450 GB SSD , system storage"	No Change

793		Appendix 2: Technical spec - point 6	The solution should support Load balancing and WAF features in same appliances and both the features should be from same OEM only.		Request to have WAF & Load balancer in separate appliances as load balancer impact the performance of the WAF if they are in same appliance.		No Change
794		Appendix 2: Technical spec - point 7	The proposed appliance shoulde provide minimum 1.2 Gbps of real world WAF throughput from day 1 and should be scalable to 2.2 Gbps with With all WAF functions enabled per intance in blocking mode SSL inspection.			Request to rephrase the clause as below - The proposed appliance shoulde provide minimum 1 1 GBPS of real world WAF throughput from day 1 and should be scalable to 2 Gbps with With all WAF functions enabled per intance in blocking mode SSL inspection.	No Change
795	11	3.1 Project Scope Point #1	The supplied Hardware and Software shall be of the latest versions and should not be end of life / end of support for the next 7 years.		Request the start Date for 7 Yrs mention in the clause be specified. Is it RFP Date or Date of PO Issuance/GoLive Date or something else?	Right tenure will help align the final BOM and any discrepency inpurs will impact pricing , so requesting clarification	The supplied Hardware and Software shall be of the latest versions and should not be end of life / end of support for the next 5 years from the date of delivery
796	12	3.1 Project Scope Point #4	All Software licenses effective date shall be effective as on Go-LIVE sign off or put in use for BOBCARD operations.		Contract Start period is mentioned as PO Issuance while the SW licenses effective date is mentioed as GoLive Sign off Dates as noticed. Request Bank to keep this synchronized if this is genuine or clarify the intent	Right tenure will help align the final BOM and any discrepent inpurs will impact pricing , so requesting clarification	License effectiveness should be start from the software is ready to use. License cost will not impact to BOBCARD due to implementation delay. No license activate without informing BOBCARD.
797	12	3.1 Project Scope Point #12	Hardware RMA (Return Merchandise Authorization) should be within 24 hours		Request this be modified as below Hardware RMA (Return Merchandise Authorization) should be within 24 hours or Next business Day Basis.	RMA for a request raised on Friday may be honored by Monday due to the wekend in between , so requesting to keep this clearly specified.	Hardware RMA (Return Merchandise Authorization) should be within 24 hours on Next business Day Basis.
798	19	5.3 Price Comparisons Point #c iv	End of Sales/ End of support: The Vendor has to ensure that any application, related software supplied / put to use as part of this RFP should not have reached end of support. In the event if any equipment supplied / put to use by the vendor reaches end of support, within the contract period from the date of use, the vendor has to replace the equipment/ software at no additional cost to the Company before		End of Life/End of Sale Clause here should specifiy the start date as to if PO issuance, RFP Date or any other . Further the tenure within which EOS/EOL should not happen must be mentioned like 7 years in clause Project Scope point #1	Right tenure will help align the final BOM and any discrepent inpurs will impact pricing , so requesting clarification	The supplied Hardware and Software shall be of the latest versions and should not be end of life / end of support for the next 5 years from the date of delivery
799	9	2.2 Tenure	The tenure of the contract initially would be for 1 year from the date of the issuance of first purchase order. BOBCARD can further extend to 2 years at its at mutually agreed terms.		Contract Tenure mentioend as 1 Year from PO Issuance here while its 3 years in clause 3.1 Point 17/ Pls clarify the right tenure?	Right tenure will help align the final BOM and any discrepent inpurs will impact pricing , so requesting clarification	Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
800	13	3.1 Project Scope Point #17	The initial term of this contract shall be 3 years and may be extended to another 2 years subject to satisfactory performance by successful bidder and OEM(s).		Mentioned here is 3 years of initial contract and in 2.2 section the contract mentioned is 1 Year/ pls clarify the right tenure	Right tenure will help align the final BOM and any discrepent inpurs will impact pricing , so requesting clarification	Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
801	30	7.2 Evaluation Methodology for Eligible Bidder Commercial Bid Evaluation	The key considerations of the TCO would be the total payouts for entire project through the contract period of 5 years.		Mentioned here is 5 years contract but in 2.2 the tenure of contrat is 1 Year, pls clarify the number to consider	Right tenure will help align the final BOM and any discrepent inpurs will impact pricing , so requesting clarification	Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
802	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Server Prod > HCI Rack Servers > 1	Total QTY is 14		Clarifictaion Needed: 1. Please provide split of quantity of servers / Nodes per location. 2. Kindly specify the number of clusters and nodes per cluster also.	clarifiction will help arrive at the boq rightly	This will be shared with only elected bidder

803	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Server Prod > HCI Rack Servers > 7	Each Rack Server Controller Cards / Controller Drive should be provided in HA mode in RAID -1.		Request Change: Each HCI Server should be configured with two BOOT drives with hardware RAID Controller. For NVMe storage drives: Provides as per Certifed HCI Node with NVMe configuration	From the HCI Rack server or Pre configured HCI NODE - RAID Controller card is not required for NVMe drives. Also, is this ask for Boot drive with RAID Controller?	Yes, we need boot drive for HCI hypervisor provided in HA mode in RAID -1
804	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Server UAT > HCI Rack Servers > 7	Each Rack Server Controller Cards / Controller Drive should be provided in HA mode in RAID -1.		Request Change: Each HCI Server should be configured with two BOOT drives with hardware RAID Controller. For NVMe storage drives: Provides as per Certifed HCI Node with NVMe configuration	From the HCI Rack server or Pre configured HCI NODE - RAID Controller card is not required for NVMe drives. Also, is this ask for Boot drive with RAID Controller?	Yes, we need boot drive for HCI hypervisor provided in HA mode in RAID -1
805	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Server Prod > HCI Rack Servers > 6	Each Rack servers should have minimum usable Storage Capacity of 10 TB of all caching SSD and other HDD. 20% disk slot on each node should be free for future expansion		Clarification needed: In virtualized environment, the storage (usable) capacity is calcluated across the cluster. Need clarification on the total capacity required across the number of nodes in a cluster.	clarifiction will help arrive at the boq rightly	as mentioned in RFP 10TB usable storage per node * no of node = total usable capacity
806	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Server UAT > HCI Rack Servers > 6	Each Rack servers should have minimum usable Storage Capacity of 10 TB of all caching SSD and other HDD. 20% disk slot on each node should be free for future expansion		Clarification needed: In virtualized environment, the storage (usable) capacity is calcluated across the cluster. Need clarification on the total capacity required across the number of nodes in a cluster.	clarifiction will help arrive at the boq rightly	as mentioned in RFP 10TB usable storage per node * no of node = total usable capacity
807	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Server Prod > HCI Rack Servers > 13 >Server Security	Request New Point to be added		Request to add the below point for security and management features for HCI Nodes Day2 operations and management of HCI Nodes for updates on Hardware and Software. HCI Node management tool should integrate with Virtual platform and Network switches. Should be able to do Firmware updates, Manage Cluster and deployment, Full stack visibility of HCI Node, TAC/Case Support, Continuous Health checks on Networking, Server, VMs , Anomalies detection, Security advisories, patch management etc.	HCI Node should integrate with Virtual platform and Network switches, Should have management software for a Firmware update, Manage Cluster and deployment, Full stack visibility HCI Node, TAC/Case Support, Continuous Health checks on Networking, Server, VMs , Anomalies detection, Security advisories, patch management,	No Change, additional feature will be consider as value add
808	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Server UAT > HCI Rack Servers > 13> Server Security	Request New Point to be added		Request to add the below point for security and management features for HCI Nodes Day2 operations and management of HCI Nodes for updates on Hardware and Software. HCI Node management tool should integrate with Virtual platform and Network switches. Should be able to do Firmware updates, Manage Cluster and deployment, Full stack visibility of HCI Node, TAC/Case Support, Continuous Health checks on Networking, Server, VMs , Anomalies detection, Security advisories, patch management etc.	HCI Node should integrate with Virtual platform and Network switches, Should have management software for a Firmware update, Manage Cluster and deployment, Full stack visibility HCI Node, TAC/Case Support, Continuous Health checks on Networking, Server, VMs , Anomalies detection, Security advisories, patch management,	No Change, additional feature will be consider as value add
809	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmentation > 1	The Solution should be capable of supporting major hardware OEMs like Juniper, Arista, Cisco, HPE and Dell. The proposed solution should be a purely software-based solution and should not be dependent on any hardware make and model.		Request below modified clause be considered: The Solution should be capable of supporting major hardware OEMs like Juniper, Arista, Cisco, HPE and Dell. The proposed solution should be a purely software-based solution and should not be dependent on any hardware make and model by creating overlay tunnels between the hosts.	The key benefits of no dependecy on hardware is by using software defined networking i.e overlay. Overlay is mandatory for network & Security automation as part of software defined data center.	No Change

#							
810	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmentation > 2	The solution should provide a distributed firewall such that the firewalling for Virtual Machines can be provided closest to the application within the server itself without traffic going to a Physical Firewall.		Request below modified clause be considered which includes additonal points The solution should provide a distributed firewall such that the application aware and identity based statefull firewalling for Virtual Machines can be provided closest to the application within the server itself without traffic going to a Physical Firewall or regardless of underlying L2 Netwrork topology. The solution should also provide an integrated networking solution (CNI implementations) as well as provide advance turnkey container networking & firewalling services. Solution should support for container networking plug-ins, support for pod to pod communication and support for ingress controllers. The micro-segmentation solution should have a capability for stateful firewalling and ALGs (Application Level Gateway) on a per-workload granularity regardless of the underlying L2 network topology (i.e. possible on either logical network overlays or underlying VLANs), embedded in the hypervisor kernel, distributed across entire environment with centralized policy and management	*As per security framework its recommended not to use standard ports for your applications and hence to have effective security on per VM basis an application/L7 firewalling is must.* Containers & Kubernetes are now part of all modern applications hence networking and security for container shall also be considered for end to end application security. there is App ID requirement is mentioned in RFP as part of "Internal Firewall" spec point # 23 hence same should be considered for mirosegmentation as well otherwise it will create non standard architecture.	No Change
811	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmenation >5	The proposed solution should provide the ability to define firewall rules at VM level for east-west traffic in order to implement Zero Trust Security		Request below modified clause be considered: The proposed solution should provide the ability to define Layer 7 application firewall rules at VM level for east-west traffic in order to implement Zero Trust Security alongwith URL Filtering and TLS inspection for encrypted traffic	Zero trust Security framework mandates TLS inspection for encrypted traffic, URL Filtering and Layer 7 application firewalling.	No Change, additional feature will be consider as value add
812	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmenation >4	The Proposed Solution including Hypervisor, SDS and Micro segmentation must be from the same OEM.		Request below modified clause be consideredL The Proposed Solution including Hypervisor, SDS, SDN and Micro segmentation must be from the same OEM.	SDN is missing in the spec, SDN will be mandatory to create complete automated Software Defined data center by creating an abstraction of the network enabling programming of network behavior in a centrally controlled manner through software applications.	No Change, SDN will be consider as value add
813	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmenation >6	The proposed solution should allow users to define granular firewall rules based on IP Addresses, Tags/Categories and Subnets to segment User Applications		Request below modified clause be considered which includes additonal points The proposed solution should allow users to define granular firewall rules for both VM and conatiners based on IP Addresses, VM Names, Tags/Categories and Subnets to segment User Applications by creating dynamic security groups. The solution should have capability to provide stateful micro-segmentation for virtual machines and Kubernetes workloads from a single console. The solution should also support enforcement of stateful distributed firewall for IPv6 VM workloads. These firewall rules can use IPv6 addresses, IPv6 CIDR, IP Sets that include both IPv4 and IPv6 addresses and security groups that can include logical ports that have both IPv4 and IPv6 addresses. IPv6 capability should be available both at management and data plane	Its necessary to have dynamic security group capability to ensure complete automation. Mentioned in the RFP page 8 -> 2.0 --> Requirement Summary--> 2.1 Intent--> mentions requirement for IPv6 "The proposed solution should support both IPv4 and IPv6."	No Change
814	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmenation >7	Solution should provide capability to create network segments by defining them entirely in software and avoid the need to re-architect your network or deploy physical appliances		Request below modified clause be accmodated: Solution should provide capability to create network segments and L2 Streching between DC and DR by defining them entirely in software and avoid the need to re-architect your network or deploy physical appliances	L2 Streching is required for better application availability considering RFP asks for 99.99 % availability on monthly basis. RFP Page 17 -> "4. Service Levels "-->"SLA: The solution is expected to be available for 99.99% on 24x7 and up time availability will be calculated on monthly basis."	No Change, L2 stretching implementation will be discuss with elected bidder.
815	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Container >2	The solution must be able to manage Kubernetes clusters. Licenses for managing Kubernetes clusters should be implemented from Day-1		Request below modified clause be accmodated: The solution must be able to manage Kubernetes clusters. Licenses for managing Kubernetes clusters along with components such as backup, container registry and monitoring alongwith Windows Container support should be implemented from Day-1	Kubernetes Cluster doesn't work in isloation but require other components such as container registry and backup solution. If not included than Bob Card will have procure them separately. And Not aving Windows Container support will block any windows based apps to be deployed on Kubernetes Platform.	Yes, BOBCARD will take care such requirement

					Request below modified clause be accmodated:		
816	NA	Appendix02 Techno Functional Requirements- Network components > internal FW NG Firewall Features NEW POINT	Must have provisioning, operations and lifecycle management of Kubernetes, automated deployment, scaling, and operation of Kubernetes clusters		Must have provisioning, operations and lifecycle management of Kubernetes, automated deployment, Auto scaling & Auto Healing, and operation of Kubernetes clusters	Complete Automation is not possible without Auto Scaling and Auto Healing of Kubernetes Clusters. One has to manually add nodes in case of failure or unprovisioned increase in load.	No Change
817	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Container >4	Container Platform should provide single pane of Glass for Lifecycle Management of all K8S clusters deployed on prem.		Request below modified clause be accmodated: Container Platform should provide single pane of Glass for Lifecycle Management of all K8S clusters alongwith ingress, backup and container registry deployed on prem.	Kubernetes Cluster doesn't work in isloation but require other components such as container registry and backup solution. These shall too be considered for life cycle management	Yes, BOBCARD will take care such requirement
818	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management >1	The solution should provide capability of generating reports for usage, performance, compliance, health, forecasting and capacity.		Request below modified clause be accmodated: The solution should provide capability of generating reports for health, Capacity Optmization - Right Sizing (Under sized, Oversized), Reclamation (Idle, Powered off , Snapshot, Orphaned Disk , Forecasting - Capacity Forecasting, Migration assessment, Migration Planning Usage - Process and service utlization Compliance - Regulatory Benchmark (PCIDSS and ISO) Security Guidelines for Infrastructure and Cloud Management	Bob Cards will need capacity optimization capabilities to identify over-provisioned & under-provisioned resources and provide recommendations, alerts and automated actions on right-sizing and resource consumption so they can be right-sized for adequate performance and avoid resource wastage. Should provide visibility of capacity and VMs which can be reclaimed and cost visibility of the reclaimed capacity and VMs.	No Change, additional feature will be consider as value add
819	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management >11	The solution should have intelligent operations with anomaly detection which will allow monitoring seasonal trends and automatically send email alert		The solution should have AI/ML driven intelligent operations & troubleshooting workbench with anomaly detection,third party infra (Server, Storage , Network, database and Application) along with parent child relatiohship mapping, service and process monitoring which will allow monitoring seasonal trends and automatically send email alert. The solution should also have log management capability for infrastructure and applications . log management solution should delivers intuitive, actionable dashboards, sophisticated analytics, and broad third-party extensibility across physical, virtual, and cloud environments.	BoB Cards will not be able to manage the infrastructure without comprhesive log management capability. Its also mandatory for from regulation/compliance perspective to have log stored for given period of time for audit. BoB Card would need apps (database and Application) to infra (Server, Storage , Network) level visibility for toublesshooting and performance monitoring.	No Change, additional feature will be consider as value add
820	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management >7	The solution must have an approval process to review, reject or approve the deployment requests from the marketplace.		Request below modified clause be considered: The Solution must support multiple levels of approval with E-mail notifications with ability to automate manual provisioning and de-provisioning of the tasks and policies embedded in each layer of their application including auto - approve and auto-reject capability based on application criticality	The solution must have an approval process to review, multi level & auto reject or approve the deployment requests from the marketplace.	No Change, additional feature will be consider as value add
821	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 6	Hypervisor should support container and opensource integration for cloud native application from day-1. Must be a Kubernetes ready from day-1.		Request below modified clause be accmodated: Hypervisor should support container both Linux and Windows along with other kubernetes ecosystems such as container registry, backup, ingress & monitoring and opensource integration for cloud native application from day-1. Must be a Kubernetes ready from day-1.	Kubernetes does't work in isolation and requires multiple components for production setup.	Yes, BOBCARD will take care such requirement
822	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 16	Virtualization Manager should provide feature which can perform quick, as-needed deployment of additional virtualized hosts. When the service is running, it can push out update images, eliminating patching and update without impacting production.		Please clarify the scenario and expected outcome out of the below point in this clause: "When the service is running, it can push out update images, eliminating patching and update without impacting production."		Virtualization manager should allow addition of new nodes and patching/upgrade of hypervisor running on the node without any VM downtime.
823	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 22	Unlimited VM replication from DC to DR (No restriction on VM replication and DR orchestration) with the capability to define Recovery Plans		Request to provide the number of VMs to be orchestrated for automated recovery and not keep open as unlimited since this approach is OEM specific . The VMs to be protected/orchestrated are limited to what can be provisioned on these 14 servers of production. Furehr pls clarify the need for Recovery Plans		No Change, can not predict the exact number of VMs for next 5 Years which need to be replicated.
824	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 23	Proposed solution should have a self-service restore feature on a per-VM basis to allow trusted application administrators to recover their own files with the ability to mount snapshots as a drive in Windows VMs		Request this be modified as below or clarify the requriement: Proposed solution should have a self-service restore feature on a per-VM basis to allow trusted application administrators to recover their own VMs from the snapshot	Please clarify this requirement, this looks like back and restore requirements so the modified clause	This will help BOBCARD to recover file without losing current state of virtual machine.

825	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 24	Hypervisor should provide Visibility for Running VM and their connectivity co-relationship with Network Ports on attached Physical TOR / Core Direct which Include Network RX/TX Bytes.		Request below modified clause with additional inputs be considered : Hypervisor should provide Visibility for Running VM and their connectivity co-relationship with Network Ports on attached Physical TOR / Core Direct which Include Network RX/TX Bytes.Solution Should provide end to end visibility across physical firewall, switch and storage, Flow Analysis and Security Planning,Guided Troubleshooting, Microsegmentation planning, RCA (Connectivity Problem, Packet Loss, N/W latency), Application Discovery, Service Monitoring , Application Dependency Mapping and monitoring of non compliant ports	Monitoring is not considering all components of the stack. Unless end to end visibility is provided as part of this solution BoB Card has to spend separately on monitoring.	Yes, BOBCARD will take care such requirement. However Hypervisor should provide Visibility for Running VM and their connectivity co-relationship with Network Ports on attached Physical Port which Include Network RX/TX Bytes.
826	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 30	Virtualization software or the solution should provide Cluster level encryption protects unauthorized data access at-rest.		Request below modified clause be considered : Virtualization software or the solution should provide Cluster level, VM Level encryption protects unauthorized data access at-rest and in transit.	Having capability to do the enscryption at app VM level and in transit is required to complete solution.	No Change, additional feature will be consider as value add
827	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Software Defined Storage > 1	Maintain primary working set copy of active data on the Local Node as VM's are hosted to provide high IOPS and low latency. Proposed solution must be proposed for faster reads and write for Business-critical Apps.		Request below additional point be added in theis clause : Proposed solution must be proposed for faster reads and write for Business-critical Apps.	Architecture is specific to one vendor, request BoB Cards to consider on outcome than specific architecture. There is no specific latency requirements mentioned in the spec.	No Change.
828	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Software Defined Storage >2	The solution must have De-duplication and Compression features licensed and implemented from day one (Should not have dependency on any proprietary hardware device).		Request below modified clause be considered: The solution must have De-duplication/Compression features licensed and implemented from day one (Should not have dependency on any proprietary hardware device).	Solution should have flexibility to implement either compression and de-duplication. BoB Cards should conisder overhead while deciding on both.	No Change
829	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Software Defined Storage >24	The proposed solution should support 1 min RPO & 1 hour RTO for critical workload in case BOB Cards wants to have this capability replication for Future use. The proposed solution should have native Replication and DR Orchestration from Day-1		What is the use case for 1 min RPO and 1 Hour RTO? is this linked with some regulatory requirement?	Replication is best handled at application level as having additional solution for infrastructure will complexity and cost for BoB Cards Its best to use extends the existing DR orchestration solution for this environment as well.	This is required for BOBCARD mission critical application. The solution should capable to support 1min RPO. The propose replication solution should be same OEM as the virtualization solution to provide seamless integration.
830	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Software Defined Storage >25	The solution provided should function even after one node failure.		Request below modified clause be considered: The solution provided should function even after two node failure.	RFP asks for 99.99 % availability SLA for the proposed solution. It will require minimum N+2 configuration for required resiliency and uptime.	No Change, additional feature will be consider as value add
831	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Software Defined Storage >31	The solution should provide enterprise data services such as compression completely in software. Software Defined Storage solution must have de-duplication and compression features Licensed and implemented from day one. These functionalities should be part of the proposed solution. The solution must have functionality to support compression and or deduplication online on data container without any downtime and data loss as per business requirement.		Request below modified clause be considered: The solution should provide enterprise data services such as compression completely in software. Software Defined Storage solution must have de-duplication or compression features Licensed and implemented from day one. These functionalities should be part of the proposed solution. The solution must have functionality to support compression and or deduplication online on data container without any downtime and data loss as per business requirement.	Solution should have flexibility to implement either compression and de-duplication. BoB Cards should conisder overhead while deciding on both.	No Change
832	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmentation > new point	Additional Point for consideration		The solution must ensure that there is not alteration in the IP address of the Virtual machine, by blocking the traffic from or to the VM inherited as a feature in the Solution.	IP/MAC spoofing is major security concern for organizations like BoB Cards handing customers data.	No Change, additional feature will be consider as value add
833	NA				The solution should support multi-tenancy to isolate networking/security for different departments/function within BoB Cards upto a minimum of 4 tenants and 5 VPCs	VPC will enable Bob Cards to create isolation from access , resources, network and security.	ange, additional feature will be consider as value
834	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Container > 6	Should support cluster scale out i.e addition of worker nodes as and when required.		Request below modified clause be considered: Should support Automated cluster scale out i.e addition of worker nodes as and when required.	Complete Automation is not possible without Auto Scaling and Auto Healing of Kubernetes Clusters. One has to manually add nodes in case of failure or unprovisioned increase in load.	No Change

835	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > 3	The solution shall provide a single pane of glass for automated provisioning with model-based orchestration of compute, network and storage through a unified multi-tenant self-service catalog.		Request below modified clause be consiered The solution shall provide a single pane of glass for automated provisioning with model-based orchestration of compute, network , storage and Kubernetes through a unified multi-tenant self-service catalog .	All modern applications are combination of both container and VM form factor.	No Change, additional feature will be consider as value add
836	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > 5	The solution must provide a self-service portal to allow user to consume the creation of infrastructure easily.		Request below modified clause be considered: The solution must provide a self-service portal to allow user to consume the creation of infrastructure easily for both VM and Kubernetes	All modern applications are combination of both container and VM form factor.	No Change, additional feature will be consider as value add
837	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > 8	The software must allow the designer to use shell script, PowerShell script to code the automation.		Request below modified clause be considered: The software must allow the designer to use shell script, PowerShell script, Python and node JS to code the automation.	Python and nodeJs are very popular language for scrpting in terms resource availability and community support	No Change, additional scripting will be value add
838	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > 9	The software must allow the designer to design VM blueprints.		Request below modified clause be considered: The software must allow the designer to design Multi VM & Kubernetes blueprints.	All modern applications are combination of both container and VM form factor.	No Change, additional feature will be consider as value add
839	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > 12	The solution should have simple low-code, no-code automation engine which allows automating day-to-day routine tasks		Request below modified clause and adidtoinal inpurs on the clause be considered: The solution should have simple low-code, no-code automation engine which allows automating day-to-day routine tasks such as Snapshot creation, Addition of Disk, Power Cycle (Suspend , Shutdown, Reboot, reset), Resize, Rebuild, Additional of Network, VM Unregister , Delete,connect remote console, Change Security Group with capability to create additional resource actions as out of the box capability.	All modern applications are combination of both container and VM form factor.	No Change, additional feature will be consider as value add
840	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > New Point	New Point		Solution should provide capability to define and showcase cost to create cloud like experience to the business unit with the overall cost spend on the infrastructure [server hardware, storage, licenses, application, maintenance, labor, network, facilities , etc.	Bob Cards will need Cost transparency (Showback and Chargeback capability) across private, hybrid to optimize planning and prioritization of VM/ Server/Application onboarding/provisioning	No Change, additional feature will be consider as value add
841	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF & IPS	New Point		We request BoB Card to allow for both software and hardware based solution for Load Balancer, WAF, IPS/IDS. As these components are dynamic as per application consumption requirements and considering bob card is directly managing customer data, its very crítcal that these components are added as part of sofwate defined stack.	Modern applications increasingly require software-defined networking (SDN) and security solutions due to their need for greater flexibility, agility, and scalability. Traditional networking and security methods often lack the adaptability to support the dynamic nature of modern application environments, especially in cloud	No Change
842	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF C.Solution Capabilites Pont #5	The solution must support and integrate the web application vulnurability tools (Web application scanners) being proposed by bidder as part of this RFP at minimum to virtually patch web application vulnurabilies or else solution should have ready plug-ins to integrate banks VAPT tool.		Requesting you to modify the clause as below: The solution must support and integrate the web application vulnurability tools (Web application scanners) being proposed by bidder as part of this RFP, solution should have ready plug-ins to integrate banks VAPT tool.	Solution should be capable to protect against zero-day vulnerability using positive security model without being dependent on virtual patching. Virtual patch can even lead to false positive.	No Change
843	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #2	Appliance/Chassis based Hardware should support scalability with license upgrade. -18 vCPU from day 1 | Scalable to 32 vCPU -128 GB DDR RAM from day 1 -1 TB X 1 SSD M.2 SSD (in Raid) from Day 1		This clause will limit the participation of other OEMs in this RFP. Hence request you to relax the clause to allow healthy participation of other OEMs		No Change
844	NA	7/B.Hardware & InAppendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #7	The proposed appliance shoulde provide minimum 1.2 Gbps of real world WAF throughput from day 1 and should be scalable to 2.2 Gbps with license upgrade on the same hardware or additional blades in case of a chassis based solution. The WAF throughput mentioned should be inclusive after enabling the below mentioned features: With all WAF functions enabled per intance in blocking mode SSL inspection.		This clause will limit the participation of other OEMs in this RFP. Hence request you to relax the clause to allow healthy participation of other OEMs		No Change

845	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #8	The appliance should support the layer 7 throughput should be at least 58 Gbps scalable to 92 Gbps on same hardware with license upgrade. (Data rerernces for above should be verified from publicly available datasheet)		This clause will limit the participation of other OEMs in this RFP. Hence request you to relax the clause to allow healthy participation of other OEMs	No Change
846	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #9	The proposed appliance must have minimum hardware compression of 34 Gbps for HTTP traffic form day 1 and scalable upto 48 Gbps with add on license on same hardware. (Data rerernces for above should be verified from publicly available datasheet)		This clause will limit the participation of other OEMs in this RFP. Hence request you to relax the clause to allow healthy participation of other OEMs	No Change
847	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #10	The proposed appliance should support minimum hardware based SSL offloading from day 1 up to : 34 Gbps Scalable upto 48 Gbps on same hardware with license upgrade. (The SSL encryption & decryption process must be hardware-based proccessor for acceleration) (Data rerernces for above should be verified from publicly available datasheet)		This clause will limit the participation of other OEMs in this RFP. Hence request you to relax the clause to allow healthy participation of other OEMs	No Change
848	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #11	The solution must support minimum SSL TPS/CPS: -29 K ECDSA P-256-bit keys from day 1 -58 K RSA 2048-bit keys from day 1 scalable to minimum SSL TPS/CPS -68 K ECDSA P-256-bit keys -98 K of RSA 2048-bit Keys (Data rerernces for above should be verified from publicly available datasheet with SSL)		This clause will limit the participation of other OEMs in this RFP. Hence request you to relax the clause to allow healthy participation of other OEMs	No Change
849	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #12	The proposed appliance should support minimum 74 million L4 concurrent connections from day one and scalable upto 99 Million on same hardware with license upgrade.		This clause will limit the participation of other OEMs in this RFP. Hence request you to relax the clause to allow healthy participation of other OEMs	No Change
850	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #13	The proposed appliance should support minimum 2.4 million L7 requests per seconds from day 1 and scalable upto 4.2 Million on same hardware with with license upgrade.		This clause will limit the participation of other OEMs in this RFP. Hence request you to relax the clause to allow healthy participation of other OEMs	No Change
851	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF General Requirement Point #13	The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide traffic performance statistics for last 30 days including Active Connections, Active Sessions, CPU Usage By Core, HTTP Requests, Memory Used, RAM Cache Utilization, Rewrite Transaction, Data Rewrite Transactions, SSL Transactions, Throughput(bits), Throughput(packets), & Total New Connections	The clause should mention the functionality should be achieved without being dependent on tools.	This clause will limit the participation of other OEMs in this RFP. Hence request you to relax the clause to allow healthy participation of other OEMs	No Change
852	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #14	The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide a security event timeline dashboard where critical events like Audit logs, Pool status change, Failover status change, DOS attacks etc. must be shown for ease of troubleshooting with last 20 Failed logins details	The clause should mention the functionality should be achieved without being dependent on tools.	This clause will limit the participation of other OEMs in this RFP. Hence request you to relax the clause to allow healthy participation of other OEMs	No Change
853	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #15	The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide a Bug tracker option, where an admin can login and find any bugs affecting the devices	The clause should mention the functionality should be achieved without being dependent on tools.	This clause will limit the participation of other OEMs in this RFP. Hence request you to relax the clause to allow healthy participation of other OEMs	No Change

854	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #16	The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide an upgrade Options suggestions for next hotfix and stability release for ease of day-2 operations with single click access to release notes a nd EOS dates		The clause should mention the functionality should be achieved without being dependent on tools.	This clause will limit the participation of other OEMs in this RFP. Hence request you to relax the clause to allow healthy participation of other OEMs	No Change
855	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #17	The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide an ability to execute CLI commands which are essential for diagnostics which will show historic data or data at the time of file captured. E.g show history of all executed commands on the CLI		Request you to remove this clause	Database Load Balancer is provided as inbuilt feature from database solution provider and hence not needed from SLB solution	No Change
856	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF C.Solution Capabilities Point #23	Solution should have the capability to highlight (In red / any color code) only malicious payload from the entire attack payload on the event analysis dashboard for detailed fornsics analysis. This is extermly critical when our incident response teams are in combat with the attackers during wartime.

This feature/functionality has to be live demonstrated by the bidder after the prebid query meeting, by setting up a lab in the cloud/on-premises | | Forensics are not required for LB or WAF kind of solution. This is required for DDoS kind of solution and it is not recommended to have DDoS solution within WAF+LB as DDoS should be a stateless technology and it's placement should be at perimeter level above firewall to protect complete infrastruture | | No Change |
| 857 | NA | Appendix02 Techno Functional Requirements- Network components > LB+WAF C.Solution Capabilities Point #36 | The Proposed WAF Solution should provide built-in L7 layer DDoS detection and mitigation features based on machine learning and behavioral analytics and dynamic signatures. It should have CAPTCHA support or other mechanism to avoid distributed attack.

This feature/functionality has to be live demonstrated by the bidder after the prebid query meeting, by setting up a lab in the cloud/on-premises | | Request to remove this point | DDoS should be a stateless device and it's placement should be at perimeter level above firewall. This ensures protection to network from any advanced DDoS attacks. Hence, it should not be expected to be part of other security solutions within the network. | No Change |
| 858 | NA | Appendix02 Techno Functional Requirements- Network components > LB+WAF C.Solution Capabilities Point #58 | The Solution should have IPSEC tunneling capabiltiies | | Request to remove this point | VPN is recommended to be a dedicated solution since it relies on TLS protocol. It is also recommended to terminate the traffic on Firewall or before Firewall as it will check for security parameters on the same.

If this is done on ADC, there won't be any security check and can possess threat or security flaw | No Change |
| 859 | NA | Appendix02 Techno Functional Requirements- Network components > LB+WAF C.Solution Capabilities Point #59 | The proposed solution should support a comprehensive list of ways in which LB can monitor the backend services including Daimeter, DNS, FTP, Gateway ICMP, HTTP, HTTPS, TCP half open, TCP , LDAP, MSSQL, MYSQL, MQTT , POSTGRESQL, POP3 , IMAP, NNTP, Radius , SIP and custom external scripts | | Request to modify the clause as below:

The proposed solution should support a comprehensive list of ways in which LB can monitor the backend services including DNS, FTP, Gateway ICMP, HTTP, HTTPS, TCP half open, TCP , LDAP, MSSQL, MYSQL , POSTGRESQL, POP3 , IMAP, NNTP, Radius and custom external scripts | SIP, Diameter & MQTT Traffic are used in Service Provider environment and are not relevant and used in any Enterprise environment like BOB Cards. | No Change |
| 860 | NA | Appendix02 Techno Functional Requirements- Network components > LB+WAF C.Solution Capabilities Point #61 | The proposed solution should support various types of LB config for handling traffic, including standard reverse proxy, forwarding in L2 , Forwarding in IP, High performance mode, Stateless mode , Reject mode, DHCP relay, and Message routing for SIP, Daimeter and MQTT traffic | | Request this clause be modified as below:

The proposed solution should support various types of LB config for handling traffic, including standard reverse proxy, forwarding in L2 , Forwarding in IP, High performance mode, Stateless mode , Reject mode, DHCP relay | SIP, Diameter & MQTT Traffic are used in Service Provider environment and are not relevant and used in any Enterprise environment like BOB Cards. | No Change |

861	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF C.Solution Capabilities Point #70	The proposed solution should support native integration with kubernetes based platforms hosting microservices e.g. Openshift, TKG cluster etc. Solution should update the configuration of LB automatically by observing events within kubernetes clusters form day 1 without add on license.		Solution should be able to support by means of same solution.		No Change
862	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF C.Solution Capabilities Point #81	The proposed LB solution should also support secure remote access to admin users (concurrency of not more than 10); where the solution can do endpoint checks for the admins and establist a secure tunnel with autentication against AD/OAUTH/Radius and MFA via Google authenticator. The system should allow per user basis a login schedule ?(e.g night shift employee cannot login during working hours)		This clause will limit the participation of other OEMs in this RFP. Hence request you to relax the clause to allow healthy participation of other OEMs		No Change
863	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF D.Availability #2	The solution should support SQL-based querying for the following databases for the health checks: for Oracle, MSSQL, MySQL, PostgresSQL and other databases if required in future.		Request this clause be removed	Database Load Balancer is provided as inbuilt feature from database solution provider and this is proprietary load balancing feature of Database solution provider and hence not needed from ADC solution.	No Change
864	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #7	The Firewall appliance should have certifications like ICSA /EAL4/CCNDPP		Request this be modified as below: The Firewall solution should have certifications like ICSA /EAL4/CCNDPP	Every OEM has its own solution offering and certification ask may align to the approach solution is provided rather than mandating it on the appliance	No Change
865	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #9	OEM/Bidder should provide below transceivers from Day-1. Firewall and SFP should be from same OEM. Below mentioned SFP quantity is required per appliance. 4 X 10GE SR SFP+ 4 X 1G SFP 4 x 25G SFP28		OEM/Bidder should provide below transceivers from Day-1. Firewall and SFP should be from same OEM. Below mentioned SFP quantity is required per appliance. 4 X 1G RJ 45 4 X 10G SFP+ 4 x 25G SFP28	Requesting if 1G can be considered using Copper Links and not SFP	No Change
866	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #15	Solution should have minimum 450 GB SSD pair, system storage		Request to modify this as below Solution should have minimum 900 GB SSD pair, system storage	Perimeter Firewall needs high storage deployments for storing logs considering 3/6 months retention in case the remote Management device is impacted , so good to ask for more	No Change, additional feature will consider as value add
867	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #16	Solution should have minimum 32 GB		Request clause to be modifiedL Solution should have minimum 128 GB RAM	Perimeter Firewall has to have good RAM and such baselining will help with operations of critical banking infra	No Change, additional feature will consider as value add

| 868 | NA | Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #19 | "The proposed firewall must provide minimum 10 Gbps of Threat prevention throughput with Real world traffic. (Throughput must be derived from Appmix traffic and not Video/JPEG based traffic) (enterprise testing condition). The throughput must remain 10 Gbps even after enabling NGFW + IPS/IDS + Antivirus + Anti Spyware + Anti Bot + DoS/DDOS + All signature enabled + Logging enabled + Bidirectional inspection + File Blocking. OEM to provide publicly available The Test methodology and result should be compliant to the benchmark testing methodology for the above parameters provided in the Internet Engineering Task Force (IETF)- 'Benchmarking Methodology for Network Security Device Performance document mentioning throughput with transaction size, traffic mix. enabled on day 1. No cluster based solution should be quoted to meet the above requirement. | | Request below modified clause be considered , instead of Appmix traffic , real world traffic should be mentioned for deriving throughput

"The proposed firewall must provide minimum 10 Gbps of Threat prevention throughput with Real world traffic. (Throughput must be derived from real world traffic and not Video/JPEG based traffic) (enterprise testing condition). The throughput must remain 10 Gbps even after enabling NGFW + IPS/IDS + Antivirus + Anti Spyware + Anti Bot + DoS/DDOS + All signature enabled + Logging enabled + Bidirectional inspection + File Blocking. OEM to provide publicly available The Test methodology and result should be compliant to the benchmark testing methodology for the above parameters provided in the Internet Engineering Task Force (IETF)- 'Benchmarking Methodology for Network Security Device Performance document mentioning throughput with transaction size, traffic mix. enabled on day 1. No cluster based solution should be quoted to meet the above requirement. | instead of appmix traffic real world traffic will be rifht measure of throuhgput , so requesting the change | No Change |
| 869 | NA | Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #21 | NGFW appliance must be capable of handling minimum 2 M concurrent sessions utilizing HTTP transactions with all Security feature Turned ON and not based on UDP / Lab environment / ideal testing environment, this claim has to be supported with declaration of concurrent connections claim from OEM | | Request below modified clause to accomodate support for 5M concurrent sessions

NGFW appliance must be capable of handling minimum 5 M concurrent sessions utilizing HTTP transactions with all Security feature Turned ON and not based on UDP / Lab environment / ideal testing environment, this claim has to be supported with declaration of concurrent connections claim from OEM | Mid/Large scale deployments need higher concurrent session support and baselining this to 50 Lakh concurrent sessions will be in the interest of the Bank , so the requested change | No Change, additional feature will consider as value add |
| 870 | NA | Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #49 | Solution should support creation of minimum 1 virtual context / instance from Day-1 without any compromise on system performance and network bandwidth. | | Solution should support creation of minimum 5 virtual context /instance from Day-1 without any compromise on system performance and network bandwidth. | Support for only 1 Virtual context may not be scalable for the DC design and min support for 5 instances is the need for any DC infra Perimeter Firewall understanding furture state architecure and growing needs. | No Change, additional feature will consider as value add |
| 871 | NA | Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #54 | The proposed NGFW solution architecture should have Control Plane separated from the Data Plane in the Firewall appliance architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup, QoS, NAT etc). Control plane must have dedicated resources such as CPU, RAM etc. This is to ensure Bank always has management access to NGFW irrespective of Firewall load / Traffic Spike / Cyber Attack driving higher CPU utilization. Bank should able to login to the firewall and carry out reporting / management / packet capture etc to identify the root cause and ccordingly take necessary action to remediate it. | | Request below modified clause be considered

The proposed NGFW solution architecture should have Control Plane separated from the Data Plane in the Firewall solution architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup, QoS, NAT etc). Control plane must have dedicated resources such as CPU, RAM etc. This is to ensure Bank always has management access to NGFW irrespective of Firewall load / Traffic Spike / Cyber Attack driving higher CPU utilization. Bank should able to login to the firewall and carry out reporting / management / packet capture etc to identify the root cause and accordingly take necessary action to remediate it. | OEMs have different approaches to achieving the use case and instead of the ask on the appliance itself , the Firewall Solution will be a generic term to use in requirements so this suggestion | No Change |

872	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #72	IPS should provide detailed information on each protection, including: Vulnerability and threat descriptions, Threat severity, Performance impact, Release date, Industry Reference, Confidence level etc.		Request below changed clause : IPS should provide detailed information on each protection, including: Vulnerability and threat descriptions, Threat severity, Release date, etc	Performance impact, industry reference and confidence level are subject to configuration and infrastructure in the bank.	No Change
873	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #76	Should have more than 60+ predefined Categories based on Urls, Application types, Security Risk level etc. However solution should be able to create custom categories for URL and application.		Request below modified clause with increased number of categories: Should have more than 80+ predefined Categories based on Urls, Application types, Security Risk level etc. However solution should be able to create custom categories for URL and application.	Having more predefined categories support would help bank with improved threat detection and better granular policy control with less manual effort.	No Change, additional feature will consider as value add
874	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #89	Solution should give information related to Performance impact and confidence level of protections while creating profiles.		Request this clause be deleted	performance can be subject to policy configurations and existing infra at bank.	No Change
875	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #114	"Management server should support the following for rule optimization: • Unused Rules Calculation for specific time-period based on Firewall Traffic Logs. • Analysis on Covered/Shadow/Hidden Rules • Analysis on Rules Consolidation (Merging of similar kind of rules) • Analysis on Redundant Rules • Tightening of Overly Permissive Rules (Any-Any) • Analysis on Unattached/Unused Objects to simplify objects management • Analysis on Rule-Reordering to improve the performance of the Firewall • Analysis on Disabled/Expired Rules for enhanced visibility on the Firewall Rules sets"		"Management server should support the following for rule optimization: • Unused Rules Calculation for specific time-period based on Firewall Traffic Logs / HIt count • Analysis on Covered/Shadow/Hidden Rules • Analysis on Redundant Rules • Analysis on Unattached/Unused Objects to simplify objects management • Analysis on Disabled/Expired Rules for enhanced visibility on the Firewall Rules sets"	OEMs could be handling the use case suggested for removal differently or have no dependency on the performance of the Firewall , so requesting these be removed from the ask	No Change
876	NA	Appendix02 Techno Functional Requirements- Network components > IPS Features Point #15	Should support more than 3000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness		Should support more than 5000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness	Increasing number of signature support is beneficial for the Bank's operations and for Effective Security reasons	No Change
877	NA	Appendix02 Techno Functional Requirements- Network components > internal FW Point #11	The Firewall solution Should support more than 4000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness and should be able to create 40 or more application categories for operational efficiency. Dedicated IPS solution shall be in corporated by the bidder to achive this scale of IPS AVC signatures in this solution.		Request this clause be modfied as below: The Firewall solution Should support more than 6000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness and should be able to create 40 or more application categories for operational efficiency. Dedicated IPS solution shall be in corporated by the bidder to achive this scale of IPS AVC signatures in this solution.	Increasing number of signature support is Beneficial for the Bank's operations and for Effective Security reasons	No Change, additional feature will consider as value add
878	NA	Appendix02 Techno Functional Requirements- Network components > internal FW NG Firewall Features NEW POINT	New Point to be added		The solution should provide Change Management capability for the organizations needs to implement more formal processes for configuration changes, including audit tracking and official approval before changes are deployed.	By leveraging these features and integrating with external change management tools, organizations can implement a robust change management process that includes formal approval, audit tracking, and compliance reporting within Cisco FMC.	No Change
879	NA				The solution should provide traffic hit count, Rule Conflict Detection (Redundant & Shadowed) and policy warning for streamlining firewall policies.	These features are crucial for optimizing firewall policies, ensuring efficient traffic flow, and maintaining security posture.	No Change, additional feature will be consider as value add
880	NA	Appendix02 Techno Functional Requirements- Network components > internal FW Hardware Architecture Point #3	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 8x64 GB of RAM.		Request below modified clause be considered as correction on the ask which seems typo: 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.		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.

#		Reference	Clause		Query		Response
881	NA	Appendix02 Techno Functional Requirements- Network components > Mngmt Switch 6 Product Support Point #2	The OEM support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support		Request below modified clause be considered The OEM/OEM certified partner support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support	OEM Certified partner has thorough experience of OS version upgrades and maintaining network operations troubleshooting issues and it will be cost effective to include this in the ask	The OEM/OEM certified partner support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support
882	NA	Appendix02 Techno Functional Requirements- Network components > Mngmt Switch 9 Miscellaneous Points Point #1	Console cable and power cable (As per Indian standards) as per customer requirement to be provided. All Cables shall be factory-terminated.		Since Console Cables are common for all devices per OEM , Request Bank to clarify the count of console cables to be provided , is it one each with each Switch or one per DC and DR Each ?.		No Change
883	NA	Appendix02 Techno Functional Requirements- Network components > Mngmt Switch 10 Product Support Point #2	The OEM support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support		Request below modified clause be considered The OEM/OEM certified partner support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support	OEM Certified partner has thorough experience of OS version upgrades and maintaining network operations troubleshooting issues and it will be cost effective to include this in the ask	The OEM/OEM certified partner support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support
884	NA	Appendix02 Techno Functional Requirements- Network components > Core Swtich >9 Manageability > Appliance point 9.4	Switch Anomolies related with Advisories , PSIRT and Field Notices		Request this clause be removed from the telemetry asks	This feature is not requireed for the design at the BOB DataCenter and may be removed	No Change
885	NA	Appendix02 Techno Functional Requirements- Network components > Core Swtich >13 Fabric Management > Appliance point 13.1	Solution must provide Centralized Management Appliance – Single pane of glass for managing, monitoring and provisioning the entire Solution within Data Center & across all Data Centers		Request BOBCards to provide VM compute resources for spinning up the VMs to provide this functionality while we can provide the necessary sw and support.		Requested product functionality should be comply, BOBCards will provide VM compute resources for spinning up the VMs to provide this functionality however bidder should provide the necessary sw and support.
886	NA	Appendix02 Techno Functional Requirements- Network components > Core Swtich >5 Layer 2 Features > Appliance point 5.11	Switch Hardware should have capability to support BGP EVPN Route Type 1, Type 2, Type 3, Type 4, Route Type 5, Type 6/Type 7/Equivalent routes		Request this point be removed	BOBCards design doesn't have Fabric so this is not applicable	No Change
887	NA	Appendix02 Techno Functional Requirements- Network components > Core Swtich >13 Fabric Management > Appliance point 13.36	Solution should provides reports using predefined templates, including inventory, use, and health reports.		Request below modified clause be considered: Solution should provides reports including inventory, use, and health reports.		No Change
888	13	16	L2 and L3 onsite support post implementation a. Software upgradation b. Hardware Upgradation c. Mass Changes for compliance d. Major, minor changes in feature/functionality roll out on the same infrastructure.		The activities mentioned in this clause is a part of the Managed Services (Day 2 Operations) deliverables. This clause needs to be changed.		Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
889	32	Support for the day-to-day operations	Payment shall be released on half yearly basis; i.e., 50% of invoice Cost shall be paid on completion 06 month & balance 50% on completion of 12 months of the respective year subjected to acceptance of Tax Invoice by BOBCARD		This clause is related to Day 2 support (Managed Services) which is not a part of this RFP scope. Please clarify.		Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
890	15	Pt. 5: Go-live	The successful bidder shall operate the deployed system for four weeks (after GO-Live) to fix all the implementation issues without any additional cost to BOBCARD.		Does the bidder need to operate the deployed system for four weeks utilizing the project/implementation resources only, please confirm? Also, this 4 weeks operations should be run only during business hours, please confirm?		Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
891	NA	Annexure 2	The bidder should have supplied and installed similar to proposed hardware in last three (3) financial years, i.e. 2021-2022, 2022-23, 2023-24 (Bidder to provide details in Annexure K and submit PO / Contract details)		Need Clarification on " installed HW similar to proposed HW " whether the reference PO's for the HW i.e. Switches,Servers,Firewall, WAF+ Loadbalancer, IPS & IDS, Router can be from one PO or multiple PO's	In case of Single PO we hereby request BOB Cards to consider 3 out of 6 technologies in a single PO.	We will consider multiple PO
892	NA	Annexure 2				We hereby request BOB Cards to consider" The bidder should have supplied and installed similar to proposed hardware in last Five (5) financial years, i.e.2019-2020,2020-2021, 2021-2022, 2022-23, 2023-24 (Bidder to provide details in Annexure K and submit PO / Contract details)	The bidder should have deployed and configured proposed software as per OEM certified and standard hardware in last three (3) financial years, i.e. 2021-2022, 2022-23, 2023-24 (Bidder to provide details / submit PO / Contract details)

893	NA	Annexure 2	The bidder should have deployed and configured proposed software as per OEM standard on proposed hardware in last three (3) financial years, i.e. 2021-2022, 2022-23, 2023-24 (Bidder to provide details / submit PO / Contract details)			The bidder should have deployed and configured proposed Cloud software as per OEM standard on similar hardware in last Five (5) financial years, i.e.2019-2020,2020-2021, 2021-2022, 2022-23, 2023-24 (Bidder to provide details in Annexure K and submit PO / Contract details)	The bidder should have deployed and configured proposed software as per OEM certified and standard hardware in last three (3) financial years, i.e. 2021-2022, 2022-23, 2023-24 (Bidder to provide details / submit PO / Contract details)
894	9	2. Requirements Summary 2.1 Intent	• Bidder should provide 1year of hand holding support post Go-Live, this may extend to 2 years on mutual understanding.		Query We request BOBCARD to provide number of days per week when the bidder engineer should attend for providing hand holding support. Also, for which all solution should the support be factored	The reason for this query is to identify skills required and estimate manpower to deploy, factor costs.	Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
895	9	2. Requirements Summary 2.1 Intent	Generic		Query We understand, the project scope does not include any VM migration, data migration etc. If these activities are required, please provide details to so we can confirm interoperability, and make estimate of time and manpower efforts.		The project scope does not include any VM migration, data migration
896	9	2. Requirements Summary 2.1 Intent	Generic		Query Considering that there is no migration, we understand that BOBCARD has confirmed interoperability of current setup with new setup at different level (e.g. Application on new Windows OS)		Migration of existing setup to implemented solution is under bidders scope
897	9	2. Requirements Summary 2.1 Intent	Generic		Clarification Sought We understand, the location of deployment is only primary DC. There is no DR site.		The location of deployment of this solution are DC (Mumbai/New Mumbai) and DR (Bangalore) exact location address will be shared only with elected bidder
898	9	2. Requirements Summary 2.1 Intent	BOBCARD at its discretion reserves the right to change the scope of the RFP considering the size and variety of the requirements and the changing business conditions.		Clarification Sought We understand, the change in scope will based on mutual discussion and will have limited impact on timelines, manpower efforts. The change in scope will have no impact on the products supplied. Kindly confirm if our understanding is right.		No Change
899	10	2.5 Training	The Bidder is required to provide training to the BOBCARD team on the proposed solution in RFP for Procurement of Servers, Network & Software components, provide a training schedule and furnish training details as per the RFP requirements for all major components.		Query We request BOBCARD to provide number of attendees and count of days for which the training is to be provided.	The RFP includes many different technologies. This information will be useful to identify resources required to impart training and the mandays required.	One time Training need to be provided in BOBCARD Office in person for implemented solution. Training can be given by OEM/Bidder, trainer must be certified resource.
900	10	2.5 Training	The Bidder is required to provide training to the BOBCARD team on the proposed solution in RFP for Procurement of Servers, Network & Software components, provide a training schedule and furnish training details as per the RFP requirements for all major components.		Clarification Sought We understand, the sign-off will be provided before the training. The payment, warranty period will not be related to the training.	The RFP includes many different technologies. The training will require a lot of coordination based on free time slots available from BOBCARD team and may take many days to complete. Hence this request.	Training is a part of scop of project. Hence final payment will be release after training only
901	12	3.1 Project Scope	7. The successful bidder should also integrate existing infrastructure setup (like existing LAN, proxy, MFA, SIEM) with the new devices to be supplied. 8. All required configuration to integrate with existing setup should be taken care of by bidder		Query We request BOBCARD to provide details of these integration requirements such as make, model, version, configuration etc.	This information will be used 1) to confirm on the interoperability 2) identify skills and estimate manpower efforts required to complete the integration	This will be market leading product only. Basis on compatibility Bidder has to integrate the existing infra setup with new setup. All the product will be share only with the final bidder
902	12	3.1 Project Scope	7. The successful bidder should also integrate existing infrastructure setup (like existing LAN, proxy, MFA, SIEM) with the new devices to be supplied. 8. All required configuration to integrate with existing setup should be taken care of by bidder		Clarification Sought Many integrations will require efforts from the existing technology vendor / OEM. We understand, BOBCARD will extend such support. For instance, these OEM will need to provide APIs for new solution or consume APIs provided by new solution.	The objective of highlighting this point is to conduct the project smoothly and on time.	This will be market leading product only. Basis on compatibility Bidder has to integrate the existing infra setup with new setup. All the product will be share only with the final bidder
903	12	3.1 Project Scope	10. All the devices to be hosted should support both IPv4 and IPv6 Interlinks between the devices should be on minimum 10G/25G ports and there should be resiliency between the devices. All possible high availability scenarios should be considered.		Query We understand, the requirement is for ports which auto-negotiate between 10G and 25G. And the requirement is not for either 10G or 25G ports.		the requirement is for ports which auto-negotiate between 10G and 25G.

904	14	3.1 Project Scope	24. The successful bidder should provide test cases for UAT for BOBCARD review. Upon finalization of test cases, user acceptance testing will be started by the BOBCARD Team		Query We request BOBCARD to elaborate the clause " provide test cases for UAT" and the activity to be performed by the bidder.		UAT test cases will be performed by BOBCARD with the help of Bidder
905	14	3.1 Project Scope 32. Security Requirements	The Successful bidder shall abide by the access level agreement to ensure safeguards of the confidentiality, integrity, and availability of the information systems.		Query We request BOBCARD to elaborate the clause " access level agreement" and the activity to be performed by the bidder.		This is clauses mentioned in BOBCARD NDA and will be shared with final Bidder
906	16	3.5 Business Process Definition (BPD)/ Parameterization	1. The selected bidder is also expected to carry out and document a detailed current assessment for all business activities, and services performed by the Company to gain understanding of the Company's existing business and operations. 2. The selected bidder is expected to help the Company to parameterize the product and provide valuable inputs at the time of system parameterization based on the current state assessment undertaken by the selected bidder. Also, the core team training conducted by the selected bidder should reflect the understanding of the Company's current processes as a result of conducting the current assessment. 3. The selected bidder would be responsible for ensuring that the BPD/Parameterization exercise is as per the plan		Clarification Sought We understand, if FRSM is conducted and agreed upon by the bidder and BOBCARD, BPD parameterization is not required. Kindly confirm.		No Change
907	16	3.6 Customization	2. The Bidder needs to provide all statutory and regulatory reports as required by the regulatory institutions. The Company will not pay any additional customization costs either for gaps observed and/or gaps observed for statutory or regulatory reports as required by the Company. 3. The Bidder will have to provide all the MIS reports as per the requirements of the Company.		Clarification Sought We understand, the reports here implies reports as available from various solution components deployed. Kindly confirm.		Point 2 remain as is. For point no.3 yes your understanding is correct
908	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform	2. The Bidder should provide 1 Technical Resource from Software OEM for a period of 1 Year to provide timely health check, suggest OEM best practice, conduct timely health check of the deployed solution and submit a report indicating OEM best practices. 3. The Bidder should provide 1 Technical Resource Certified by the Software OEM for the period of the contract to provide operations support, work on day-to day activities of managing the infrastructure, perform infrastructure updates and upgrades.		Change Request We request BOBCARD to add suitable lines to the Annexure 3, BoM to capture cost of Resident Engineer rendering these services.		Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
909	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform	Unlimited VM replication from DC to DR (No restriction on VM replication and DR orchestration) with the capability to define Recovery Plans The proposed solution should support 1 min RPO & 1 hour RTO for critical workload in case BOB Cards wants to have this capability replication for Future use. The proposed solution should have native Replication and DR Orchestration from Day-1		Clarification Sought We understand, current deployment is only at one site. The replication or DR orchestration is not to be configured as part of deployment. Kindly confirm or clarify		No Change, can not predict the exact number of VMs for next 5 Years which need to be replicated.

910	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform	The proposed solution should support 1 min RPO & 1 hour RTO for critical workload in case BOB Cards wants to have this capability replication for Future use. The proposed solution should have native Replication and DR Orchestration from Day-1		Clarification Sought We understand, any licence for DR orchestration is not required as part of the BOM. addl. These licences are available in pack of 25 and BOBCARD is requested to provide the count if licences are to be supplied. Kindly confirm.		This is required for BOBCARD mission critical application. The solution should capable to support 1min RPO. The propose replication solution should be same OEM as the virtualization solution to provide seamless integration.
911	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform	Micro segmentation		Query We request BOBCARD to provide information if micro segmentation is required for UAT servers as well		Yes
912	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform	Container		Query We request BOBCARD to provide count of servers on which Container will be running		This will be share with elected bidder
913	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform	Cloud Management		Query We request BOBCARD to provide information if the nodes for cloud management will be allocated from the 14 Prod Nodes.		The nodes for cloud management will be allocated from quantity of nodes mentioned in RFP
914	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform	Server Prod, Server UAT 9. NIC - Minimum 6 Ports 10/25GbE NIC cards with Transceivers		Query We understand, the requirement is for ports which auto-negotiate between 10G and 25G. And the requirement is not for either 10G or 25G ports.		The proposed port should be 25G
915	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform	Disks Slots Configuration Each Rack servers should have minimum usable Storage Capacity of 10 TB of all caching SSD and other HDD.		Query We request BOBCARD to provide usable capacity required across the cluster, node count failure to tolerate and desired replication factor OR Raw capacity per node	The technology chosen is software defined storage. Hence we seek this information.	as mentioned in RFP 10TB usable storage per node * no of node = total usable capacity
916	NA	Appendix03 Bill Of Material			Query Many of the components mentioned (Firewall, WAF, Switches, Routers....) may require additional compute / storage to run system management. We request BOBCARD to provide information if the bidder has to factor infrastructure for this purpose.		Yes, Bidder can
917	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 1	The proposed solution should be a Hyperconverged infrastructure (HCI) with 5 years comprehensive warranty		Not having the option to use external storage limits customer's ability from leveraging existing/external storage for specific application requirement which may come in future or on going setup. These application then will have to be hosted in separate infrastructure adding to cost and will create separate silo to manage along with migration effort of existing data	The proposed solution should be a Hyperconverged infrastructure (HCI) with option to use external storage with 5 years comprehensive warranty	The proposed solution should be a Hyperconverged infrastructure (HCI) with an option to use as external storage
918	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Software Defined Storage > 14	The proposed solution should support Replication factor RF-2 (1 Node failure). Proposed Solution must be planned with N+1 without considering Dedup, compression, erasure coding at both DC and DR location.		RFP asks for 99.99 % availability SLA for the proposed solution. It will require minimum N+2 configuration. 99.99 % SLA would also require BoB Cards to consider four site (DC, DR , NDC and NDR) architecture along with stretched cluster (both Infrastructure & Kubernetes) between DC and NDC . Request Bob Cards to clarify the business impact of missing 99.99 % availability SLA. Is current setup also has 99.99 % availability ?	The proposed solution should support Replication factor RF-3 (2 Node failure). Proposed Solution must be planned with N+2 without considering Dedup, compression at both DC and DR location.	No Change, additional feature will be consider as value add
919	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Micro segmentation > 1	The Solution should be capable of supporting major hardware OEMs like Juniper, Arista, Cisco, HPE and Dell. The proposed solution should be a purely software-based solution and should not be dependent on any hardware make and model.		The key benefits of no dependency on hardware is by using software defined networking i.e. overlay. Overlay is mandatory for network & Security automation as part of software defined data center.	The Solution should be capable of supporting major hardware OEMs like Juniper, Arista, Cisco, HPE and Dell. The proposed solution should be a purely software-based solution and should not be dependent on any hardware make and model by creating overlay tunnels between the hosts.	No Change, additional feature will be consider as value add

920	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Micro segmentation > 2	The solution should provide a distributed firewall such that the firewalling for Virtual Machines can be provided closest to the application within the server itself without traffic going to a Physical Firewall.		As per security framework its recommended not to use standard ports for your applications and hence to have effective security on per VM basis an application/L7 firewalling is must. Containers & Kubernetes are now part of all modern applications hence networking and security for container shall also be considered for end to end application security. there is App ID requirement is mentioned in RFP as part of "Internal Firewall" spec point # 23 hence same should be considered for miscegenation as well otherwise it will create non standard architecture.	The solution should provide a distributed firewall such that the application aware and identity based stateful firewalling for Virtual Machines can be provided closest to the application within the server itself without traffic going to a Physical Firewall or regardless of underlying L2 Network topology. The solution should also provide an integrated networking solution (CNI implementations) as well as provide advance turnkey container networking & firewalling services. Solution should support for container networking plug-ins, support for pod to pod communication and support for ingress controllers. The micro-segmentation solution should have a capability for stateful firewalling and ALGs (Application Level Gateway) on a per-workload granularity regardless of the underlying L2 network topology (i.e. possible on either logical network overlays or underlying VLANs), embedded in the hypervisor kernel, distributed across entire environment with centralized policy and management	No Change
921	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Microvegetation >5	The proposed solution should provide the ability to define firewall rules at VM level for east-west traffic in order to implement Zero Trust Security		Zero trust Security framework mandates TLS inspection for encrypted traffic, URL Filtering and Layer 7 application firewalling.	The proposed solution should provide the ability to define Layer 7 application firewall rules at VM level for east-west traffic in order to implement Zero Trust Security along with URL Filtering and TLS inspection for encrypted traffic	No Change, additional feature will be consider as value add
922	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Microvegetation >4	The Proposed Solution including Hypervisor, SDS, SDN and Micro segmentation must be from the same OEM.		SDN is missing in the spec, SDN will be mandatory to create complete automated Software Defined data center by creating an abstraction of the network enabling programming of network behaviour in a centrally controlled manner through software applications.	The Proposed Solution including Hypervisor, SDS, SDN and Micro segmentation must be from the same OEM.	No Change, additional feature will be consider as value add
923	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Microvegetation >6	The proposed solution should allow users to define granular firewall rules based on IP Addresses, Tags/Categories and Subnets to segment User Applications		Its necessary to have dynamic security group capability to ensure complete automation. RFP page 8 -> 2.0 --> Requirement Summary--> 2.1 Intent--> mentions requirement for IPv6 "The proposed solution should support both IPv4 and IPv6."	The proposed solution should allow users to define granular firewall rules for both VM and containers based on IP Addresses, VM Names, Tags/Categories and Subnets to segment User Applications by creating dynamic security groups. The solution should have capability to provide stateful micro-segmentation for virtual machines and Kubernetes workloads from a single console. The solution should also support enforcement of stateful distributed firewall for IPv6 VM workloads. These firewall rules can use IPv6 addresses, IPv6 CIDR, IP Sets that include both IPv4 and IPv6 addresses and security groups that can include logical ports that have both IPv4 and IPv6 addresses. IPv6 capability should be available both at management and data plane	No Change
924	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Microvegetation >7	Solution should provide capability to create network segments by defining them entirely in software and avoid the need to re-architect your network or deploy physical appliances		L2 Stretching is required for better application availability considering RFP asks for 99.99 % availability on monthly basis. RFP Page 17 -> "4. Service Levels "-->"SLA: The solution is expected to be available for 99.99% on 24x7 and up time availability will be calculated on monthly basis."	Solution should provide capability to create network segments and L2 Stretching between DC and DR by defining them entirely in software and avoid the need to re-architect your network or deploy physical appliances	No Change, L2 stretching implementation will be discuss with elected bidder.

925	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Container >2	The solution must be able to manage Kubernetes clusters. Licenses for managing Kubernetes clusters should be implemented from Day-1		Kubernetes Cluster doesn't work in isolation but require other components such as container registry and backup solution. If not included than Bob Card will have procure them separately. And Not aving Windows Container support will block any windows based apps to be deployed on Kubernetes Platform.	The solution must be able to manage Kubernetes clusters. Licenses for managing Kubernetes clusters along with components such as backup, container registry and monitoring along with Windows Container support should be implemented from Day-1	Yes, BOBCARD will take care such requirement
926	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Container >3	Must have provisioning, operations and lifecycle management of Kubernetes, automated deployment, scaling, and operation of Kubernetes clusters		Complete Automation is not possible without Auto Scaling and Auto Healing of Kubernetes Clusters. One has to manually add nodes in case of failure or unprovisioned increase in load.	Must have provisioning, operations and lifecycle management of Kubernetes, automated deployment, Auto scaling & Auto Healing, and operation of Kubernetes clusters	Must have provisioning, operations and lifecycle management of Kubernetes, automated deployment, Auto scaling & Auto Healing, and operation of Kubernetes clusters
927	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Container >4	Container Platform should provide single pane of Glass for Lifecycle Management of all K8S clusters deployed on prem.		Kubernetes Cluster doesn't work in isolation but require other components such as container registry and backup solution. These shall too be considered for life cycle management	Container Platform should provide single pane of Glass for Lifecycle Management of all K8S clusters along with ingress, backup and container registry deployed on prem.	No Change, additional feature will be consider as value add
928	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management >1	The solution should provide capability of generating reports for usage, performance, compliance, health, forecasting and capacity.		Bob Cards will need capacity optimization capabilities to identify over-provisioned & under-provisioned resources and provide recommendations, alerts and automated actions on right-sizing and resource consumption so they can be right-sized for adequate performance and avoid resource wastage. Should provide visibility of capacity and VMs which can be reclaimed and cost visibility of the reclaimed capacity and VMs.	The solution should provide capability of generating reports for health, Capacity Optimization - Right Sizing (Under sized, Oversized), Reclamation (Idle, Powered off , Snapshot, Orphaned Disk , Forecasting - Capacity Forecasting, Migration assessment, Migration Planning Usage - Process and service utilization Compliance - Regulatory Benchmark (PCIDSS and ISO) Security Guidelines for Infrastructure and Cloud Management	No Change, additional feature will be consider as value add
929	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management >11	The solution should have intelligent operations with anomaly detection which will allow monitoring seasonal trends and automatically send email alert		BoB Cards will not be able to manage the infrastructure without compressive log management capability. Its also mandatory for from regulation/compliance perspective to have log stored for given period of time for audit. BoB Card would need apps (database and Application) to infra (Server, Storage , Network) level visibility for troubleshooting and performance monitoring.	The solution should have AI/ML driven intelligent operations & troubleshooting workbench with anomaly detection, third party infra (Server, Storage , Network, database and Application) along with parent child relationship mapping, service and process monitoring which will allow monitoring seasonal trends and automatically send email alert. The solution should also have log management capability for infrastructure and applications . log management solution should delivers intuitive, actionable dashboards, sophisticated analytics, and broad third-party extensibility across physical, virtual, and cloud environments.	No Change, additional feature will be consider as value add
930	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management >7	The solution must have an approval process to review, reject or approve the deployment requests from the marketplace.		The solution must have an approval process to review, multi level & auto reject or approve the deployment requests from the marketplace.	Bob Cards would need multiple levels of approval with E-mail notifications with ability to automate manual provisioning and de-provisioning of the tasks and policies embedded in each layer of their application including auto -approve and auto-reject capability based on application criticality	No Change, additional feature will be consider as value add
931	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 6	Hypervisor should support container and opensource integration for cloud native application from day-1. Must be a Kubernetes ready from day-1.		Kubernetes does't work in isolation and requires multiple components for production setup.	Hypervisor should support container both Linux and Windows along with other Kubernetes ecosystems such as container registry, backup, ingress & monitoring and opensource integration for cloud native application from day-1. Must be a Kubernetes ready from day-1.	Yes, BOBCARD will take care such requirement
932	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 16	Virtualization Manager should provide feature which can perform quick, as-needed deployment of additional virtualized hosts. When the service is running, it can push out update images, eliminating patching and update without impacting production.		Please clarify the scenario "When the service is running, it can push out update images, eliminating patching and update without impacting production." Its not clear from the language as what is the expected outcome.	Virtualization Manager should provide feature which can perform quick, as-needed deployment of additional virtualized hosts. When the service is running, it can push out update images, eliminating patching and update without impacting production. Proposed solution should allow live patching of select critical security patches.	Virtualization manager should allow addition of new nodes and patching/upgrade of hypervisor running on the node without any VM downtime.

933	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 22	Unlimited VM replication from DC to DR (No restriction on VM replication and DR orchestration) with the capability to define Recovery Plans		Unlimited is open terms, request you to provide the number of VMs to orchestrated for automated recovery. As unlimited is relevant for one specific vendor . The VMs to be protected/orchestrated are limited to what can be provisioned on these 14 servers of production.	Request BoB cards to Clarify the need for Recovery Plans- We do provide unlimited Replication from DC to DR which is orchestrated. In Terms of Recovery Plans (which is automation) We request bank to consider defining specific number of Virtual Machines. Its however best to use extends the existing DR orchestration solution fot this environment as well.	No Change, can not predict the exact number of VMs for next 5 Years which need to be replicated.
934	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 23	Proposed solution should have a self-service restore feature on a per-VM basis to allow trusted application administrators to recover their own files with the ability to mount snapshots as a drive in Windows VMs		Please clarify this requirement, this looks like back and restore requirements	Proposed solution should have a self-service restore feature on a per-VM basis to allow trusted application administrators to recover their own VMs from the snapshot	This will help BOBCARD to recover file without losing current state of virtual machine.
935	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 24	Hypervisor should provide Visibility for Running VM and their connectivity co-relationship with Network Ports on attached Physical TOR / Core Direct which Include Network RX/TX Bytes.		Monitoring is not considering all components of the stack. Unless end to end visibility is provided as part of this solution BoB Card has to spend separately on monitoring.	Hypervisor should provide Visibility for Running VM and their connectivity co-relationship with Network Ports on attached Physical TOR / Core Direct which Include Network RX/TX Bytes.Solution Should provide end to end visibility across physical firewall, switch and storage, Flow Analysis and Security Planning,Guided Troubleshooting, Micro segmentation planning, RCA (Connectivity Problem, Packet Loss, N/W latency), Application Discovery, Service Monitoring , Application Dependency Mapping and monitoring of non compliant ports	Yes, BOBCARD will take care such requirement. However Hypervisor should provide Visibility for Running VM and their connectivity co-relationship with Network Ports on attached Physical Port which Include Network RX/TX Bytes.
936	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 30	Virtualization software or the solution should provide Cluster level encryption protects unauthorized data access at-rest.		Having capability to do the encryption at app VM level and in transit is required to complete solution.	Virtualization software or the solution should provide Cluster level, VM Level encryption protects unauthorized data access at-rest and in transit.	No Change, additional feature will be consider as value add
937	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Software Defined Storage > 1	Maintain primary working set copy of active data on the Local Node as VM's are hosted to provide high IOPS and low latency. Proposed solution must be proposed for faster reads and write for Business-critical Apps.		Architecture is specific to one vendor, request BoB Cards to consider on outcome than specific architecture. There is no specific latency requirements mentioned in the spec.	Proposed solution must be proposed for faster reads and write for Business-critical Apps.	No Change
938	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Software Defined Storage >2	The solution must have De-duplication and Compression features licensed and implemented from day one (Should not have dependency on any proprietary hardware device).		Solution should have flexibility to implement either compression and de-duplication. BoB Cards should consider overhead while deciding on both.	The solution must have De-duplication/Compression features licensed and implemented from day one (Should not have dependency on any proprietary hardware device).	No Change
939	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Software Defined Storage >24	The proposed solution should support 1 min RPO & 1 hour RTO for critical workload in case BOB Cards wants to have this capability replication for Future use. The proposed solution should have native Replication and DR Orchestration from Day-1		What is the use case for 1 min RPO and 1 Hour RTO? is this linked with some regulatory requirement? Replication is best handled at application level as having additional solution for infrastructure will complexity and cost for BoB Cards Its best to use extends the existing DR orchestration solution for this environment as well.	What is the use case for 1 min RPO and 1 Hour RTO? is this linked with some regulatory requirement? Replication is best handled at application level as having additional solution for infrastructure will complexity and cost for BoB Cards Its best to use extends the existing DR orchestration solution for this environment as well.	This is required for BOBCARD mission critical application. The solution should capable to support 1min RPO. The propose replication solution should be same OEM as the virtualization solution to provide seamless integration.
940	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Software Defined Storage >25	The solution provided should function even after one node failure.		RFP asks for 99.99 % availability SLA for the proposed solution. It will require minimum N+2 configuration for required resiliency and uptime.	The solution provided should function even after two node failure.	No Change, additional feature will be consider as value add
941	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Software Defined Storage >31	The solution should provide enterprise data services such as compression completely in software. Software Defined Storage solution must have de-duplication and compression features Licensed and implemented from day one. These functionalities should be part of the proposed solution. The solution must have functionality to support compression and or deduplication online on data container without any downtime and data loss as per business requirement.		Solution should have flexibility to implement either compression and de-duplication. BoB Cards should consider overhead while deciding on both.	The solution should provide enterprise data services such as compression completely in software. Software Defined Storage solution must have de-duplication or compression features Licensed and implemented from day one. These functionalities should be part of the proposed solution. The solution must have functionality to support compression and or deduplication online on data container without any downtime and data loss as per business requirement.	No Change

942	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Micro segmentation > new point	New Point		IP/MAC spoofing is major security concern for organizations like BoB Cards handing customers data.	The solution must ensure that there is not alteration in the IP address of the Virtual machine, by blocking the traffic from or to the VM inherited as a feature in the Solution.	No Change
943	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Micro segmentation > new point			VPC will enable Bob Cards to create isolation from access , resources, network and security.	The solution should support multi-tenancy to isolate networking/security for different departments/function within BoB Cards upto a minimum of 4 tenants and 5 VPCs	No Change, additional feature will be consider as value add
944	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Container > 6	Should support cluster scale out i.e. addition of worker nodes as and when required.		Complete Automation is not possible without Auto Scaling and Auto Healing of Kubernetes Clusters. One has to manually add nodes in case of failure or unprovisioned increase in load.	Should support Automated cluster scale out i.e. addition of worker nodes as and when required.	No Change
945	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > 3	The solution shall provide a single pane of glass for automated provisioning with model-based orchestration of compute, network and storage through a unified multi-tenant self-service catalog.		All modern applications are combination of both container and VM form factor.	The solution shall provide a single pane of glass for automated provisioning with model-based orchestration of compute, network , storage and Kubernetes through a unified multi-tenant self-service catalog .	No Change, additional feature will be consider as value add
946	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > 5	The solution must provide a self-service portal to allow user to consume the creation of infrastructure easily.		All modern applications are combination of both container and VM form factor.	The solution must provide a self-service portal to allow user to consume the creation of infrastructure easily for both VM and Kubernetes.	No Change, additional feature will be consider as value add
947	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > 8	The software must allow the designer to use shell script, PowerShell script to code the automation.		Python and nodeJs are very popular language for scrpting in terms resource availability and community support	The software must allow the designer to use shell script, PowerShell script, Python and node JS to code the automation.	No Change, additional scripting will be value add
948	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > 9	The software must allow the designer to design VM blueprints.		All modern applications are combination of both container and VM form factor.	The software must allow the designer to design Multi VM & Kubernetes blueprints.	No Change, additional feature will be consider as value add
949	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > 12	The solution should have simple low-code, no-code automation engine which allows automating day-to-day routine tasks		All modern applications are combination of both container and VM form factor.	The solution should have simple low-code, no-code automation engine which allows automating day-to-day routine tasks such as Snapshot creation, Addition of Disk, Power Cycle (Suspend , Shutdown, Reboot, reset), Resize, Rebuild, Additional of Network, VM Unregister , Delete,connect remote console, Change Security Group with capability to create additional resource actions as out of the box capability.	No Change, additional feature will be consider as value add
950	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > New Point	New Point	...ed Cost transparency (Showback and Chargeback capability) across private, hybrid to optimize planning and p...		Solution should provide capability to define and showcase cost to create cloud like experience to the business unit with the overall cost spend on the infrastructure [server hardware, storage, licenses, application, maintenance, labor, network, facilities , etc.	No Change, additional feature will be consider as value add
951	NA	Appendix02 Techno Functional Requirements- Network components > LB/WAF & IPS	New Point		Modern applications increasingly require software-defined networking (SDN) and security solutions due to their need for greater flexibility, agility, and scalability. Traditional networking and security methods often lack the adaptability to support the dynamic nature of modern application environments, especially in cloud	We request BoB Card to allow for both software and hardware based solution for Load Balancer, WAF, IPS/IDS. As these components are dynamic as per application consumption requirements and considering bob card is directly managing customer data, its very critcal that these components are added as part of sofwate defined stack.	No Change
952	11	3.1 Project Scope Point #1	The supplied Hardware and Software shall be of the latest versions and should not be end of life / end of support for the next 7 years.		Request the start Date for 7 Yrs mention in the clause be specified. Is it RFP Date or Date of PO Issuance/GoLive Date or something else?	Right tenure will help align the final BOM and any discrepent inpurs will impact pricing , so requesting clarification	The supplied Hardware and Software shall be of the latest versions and should not be end of life / end of support for the next 5 years from the date of delivery
953	12	3.1 Project Scope Point #4	All Software licenses effective date shall be effective as on Go-LIVE sign off or put in use for BOBCARD operations.		Contract Start period is mentioned as PO Issuance while the SW licenses effective date is mentioed as GoLive Sign off Dates as noticed. Request Bank to keep this synchronized if this is genuine or clarify the intent	Right tenure will help align the final BOM and any discrepent inpurs will impact pricing , so requesting clarification	License effectiveness should be start from the software is ready to use. License cost will not impact to BOBCARD due to implementation delay. No license activate without informing BOBCARD.

954	12	3.1 Project Scope Point #12	Hardware RMA (Return Merchandise Authorization) should be within 24 hours		Request this be modified as below Hardware RMA (Return Merchandise Authorization) should be within 24 hours on Next business Day Basis.	RMA for a request raised on Friday may be honored by Monday due to the wekend in between , so requesting to keep this clearly specified.	Hardware RMA (Return Merchandise Authorization) should be within 24 hours on Next business Day Basis.
955	19	5.3 Price Comparisons Point #c iv	End of Sales/ End of support: The Vendor has to ensure that any application, related software supplied / put to use as part of this RFP should not have reached end of support. In the event if any equipment supplied / put to use by the vendor reaches end of support, within the contract period from the date of use, the vendor has to replace the equipment/ software at no additional cost to the Company before end of support.		End of Life/End of Sale Clause here should specifiy the start date as to if PO issuance, RFP Date or any other . Further the tenure within which EOS/EOL should not happen must be mentioned like 7 years in clause Project Scope point #1	Right tenure will help align the final BOM and any discrepnt inpurs will impact pricing , so requesting clarification	The supplied Hardware and Software shall be of the latest versions and should not be end of life / end of support for the next 5 years from the date of delivery
956	9	2.2 Tenure	The tenure of the contract initially would be for 1 year from the date of the issuance of first purchase order. BOBCARD can further extend to 2 years at its at mutually agreed terms.		Contract Tenure mentioend as 1 Year from PO Issuance here while its 3 years in clause 3.1 Point 17/ Pls clarify the right tenure?	Right tenure will help align the final BOM and any discrepnt inpurs will impact pricing , so requesting clarification	Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
957	13	3.1 Project Scope Point #17	The initial term of this contract shall be 3 years and may be extended to another 2 years subject to satisfactory performance by successful bidder and OEM(s).		Mentioned here is 3 years of initial contract and in 2.2 section the contract mentioned is 1 Year/ pls clarify the right tenure	Right tenure will help align the final BOM and any discrepnt inpurs will impact pricing , so requesting clarification	Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
958	30	7.2 Evaluation Methodology for Eligible Bidder Commercial Bid Evaluation	The key considerations of the TCO would be the total payouts for entire project through the contract period of 5 years.		Mentioned here is 5 years contract but in 2.2 the tenure of contrat is 1 Year, pls clarify the number to consider	Right tenure will help align the final BOM and any discrepnt inpurs will impact pricing , so requesting clarification	Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
959	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Server Prod > HCI Rack Servers > 1	Total QTY is 14		Clarifictaion Needed: 1. Please provide split of quantity of servers / Nodes per location. 2. Kindly specify the number of clusters and nodes per cluster also.	clarifiction will help arrive at the boq rightly	This will be shared with only elected bidder
960	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Server Prod > HCI Rack Servers > 7	Each Rack Server Controller Cards / Controller Drive should be provided in HA mode in RAID -1.		Request Change: Each HCI Server should be configured with two BOOT drives with hardware RAID Controller. For NVMe storage drives: Provides as per Certifed HCI Node with NVMe configuration	From the HCI Rack server or Pre configured HCI NODE - RAID Controller card is not required for NVMe drives. Also, is this ask for Boot drive with RAID Controller?	Yes, we need boot drive for HCI hypervisor provided in HA mode in RAID -1
961	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Server UAT > HCI Rack Servers > 7	Each Rack Server Controller Cards / Controller Drive should be provided in HA mode in RAID -1.		Request Change: Each HCI Server should be configured with two BOOT drives with hardware RAID Controller. For NVMe storage drives: Provides as per Certifed HCI Node with NVMe configuration	From the HCI Rack server or Pre configured HCI NODE - RAID Controller card is not required for NVMe drives. Also, is this ask for Boot drive with RAID Controller?	Yes, we need boot drive for HCI hypervisor provided in HA mode in RAID -1
962	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Server Prod > HCI Rack Servers > 6	Each Rack servers should have minimum usable Storage Capacity of 10 TB of all caching SSD and other HDD. 20% disk slot on each node should be free for future expansion		Clarification needed: In virtualized environment, the storage (usable) capacity is calcluated across the cluster. Need clarification on the total capacity required across the number of nodes in a cluster.	clarifiction will help arrive at the boq rightly	as mentioned in RFP 10TB usable storage per node * no of node = total usable capacity
963	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Server UAT > HCI Rack Servers > 6	Each Rack servers should have minimum usable Storage Capacity of 10 TB of all caching SSD and other HDD. 20% disk slot on each node should be free for future expansion		Clarification needed: In virtualized environment, the storage (usable) capacity is calcluated across the cluster. Need clarification on the total capacity required across the number of nodes in a cluster.	clarifiction will help arrive at the boq rightly	as mentioned in RFP 10TB usable storage per node * no of node = total usable capacity
964	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Server Prod > HCI Rack Servers > 13 >Server Security	Request New Point to be added		Request to add the below point for security and management features for HCI Nodes Day2 operations and management of HCI Nodes for updates on Hardware and Software. HCI Node management tool should integrate with Virtual platform and Network switches. Should be able to do Firmware updates, Manage Cluster and deployment, Full stack visibility of HCI Node, TAC/Case Support, Continuous Health checks on Networking, Server, VMs , Anomalies detection, Security advisories, patch management etc.	HCI Node should integrate with Virtual platform and Network switches, Should have management software for a Firmware update, Manage Cluster and deployment, Full stack visibility HCI Node, TAC/Case Support, Continuous Health checks on Networking, Server, VMs , Anomalies detection, Security advisories, patch management,	No Change, additional feature will be consider as value add

965	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Server UAT > HCI Rack Servers > 13> Server Security	Request New Point to be added		Request to add the below point for security and management features for HCI Nodes Day2 operations and management of HCI Nodes for updates on Hardware and Software. HCI Node management tool should integrate with Virtual platform and Network switches. Should be able to do Firmware updates, Manage Cluster and deployment, Full stack visibility of HCI Node, TAC/Case Support, Continuous Health checks on Networking, Server, VMs , Anomalies detection, Security advisories, patch management etc.	HCI Node should integrate with Virtual platform and Network switches, Should have management software for a Firmware update, Manage Cluster and deployment, Full stack visibility HCI Node, TAC/Case Support, Continuous Health checks on Networking, Server, VMs , Anomalies detection, Security advisories, patch management,	No Change, additional feature will be consider as value add
966	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmentation > 1	The Solution should be capable of supporting major hardware OEMs like Juniper, Arista, Cisco, HPE and Dell. The proposed solution should be a purely software-based solution and should not be dependent on any hardware make and model.		Request below modified clause be considered: The Solution should be capable of supporting major hardware OEMs like Juniper, Arista, Cisco, HPE and Dell. The proposed solution should be a purely software-based solution and should not be dependent on any hardware make and model by creating overlay tunnels between the hosts.	The key benefits of no dependecy on hardware is by using software defined networking i.e overlay. Overlay is mandatory for network & Security automation as part of software defined data center.	No Change
967	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmentation > 2	The solution should provide a distributed firewall such that the firewalling for Virtual Machines can be provided closest to the application within the server itself without traffic going to a Physical Firewall.		Request below modified clause be considered which includes additonal points The solution should provide a distributed firewall such that the application aware and identity based statefull firewalling for Virtual Machines can be provided closest to the application within the server itself without traffic going to a Physical Firewall or regardless of underlying L2 Netwrork topology. The solution should also provide an integrated networking solution (CNI implementations) as well as provide advance turnkey container networking & firewalling services. Solution should support for container networking plug-ins, support for pod to pod communication and support for ingress controllers. The micro-segmentation solution should have a capability for stateful firewalling and ALGs (Application Level Gateway) on a per-workload granularity regardless of the underlying L2 network topology (i.e. possible on either logical network overlays or underlying VLANs), embedded in the hypervisor kernel, distributed across entire environment with centralized policy and management	*As per security framework its recommended not to use standard ports for your applications and hence to have effective security on per VM basis an application/L7 firewalling is must.* *Containers & Kubernetes are now part of all modern applications hence netwroing and security for container shall also be considered for end to end application security.* *there is App ID requirement is mentioned in RFP as part of "Internal Firewall" spec point # 23 hence same should be considered for mirosegmenation as well otherwise it will create non standard architecture.*	No Change
968	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmenation >5	The proposed solution should provide the ability to define firewall rules at VM level for east-west traffic in order to implement Zero Trust Security		Request below modified clause be considered: The proposed solution should provide the ability to define Layer 7 application firewall rules at VM level for east-west traffic in order to implement Zero Trust Security alongwith URL Filtering and TLS inspection for encrypted traffic	Zero trust Security framework mandates TLS inspection for encrypted traffic, URL Filtering and Layer 7 application firewalling.	No Change, additional feature will be consider as value add
969	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmenation >4	The Proposed Solution including Hypervisor, SDS and Micro segmentation must be from the same OEM.		Request below modified clause be consideredL The Proposed Solution including Hypervisor, SDS, SDN and Micro segmentation must be from the same OEM.	SDN is missing in the spec, SDN will be mandatory to create complete automated Software Defined data center by creating an abstraction of the network enabling programming of network behavior in a centrally controlled manner through software applications.	No Change, SDN will be consider as value add

970	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmenation >6	The proposed solution should allow users to define granular firewall rules based on IP Addresses, Tags/Categories and Subnets to segment User Applications		Request below modified clause be considered which includes additonal points The proposed solution should allow users to define granular firewall rules for both VM and conatiners based on IP Addresses, VM Names, Tags/Categories and Subnets to segment User Applications by creating dynamic security groups. The solution should have capability to provide stateful micro-segmentation for virtual machines and Kubernetes workloads from a single console. The solution should also support enforcement of stateful distributed firewall for IPv6 VM workloads. These firewall rules can use IPv6 addresses, IPv6 CIDR, IP Sets that include both IPv4 and IPv6 addresses and security groups that can include logical ports that have both IPv4 and IPv6 addresses. IPv6 capability should be available both at management and data plane	Its necessary to have dynamic security group capability to ensure complete automation. Mentioned in the RFP page 8 -> 2.0 --> Requirement Summary--> 2.1 Intent--> mentions requirement for IPv6 "The proposed solution should support both IPv4 and IPv6."	No Change
971	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmenation >7	Solution should provide capability to create network segments by defining them entirely in software and avoid the need to re-architect your network or deploy physical appliances		Request below modified clause be accmodated: Solution should provide capability to create network segments and L2 Streching between DC and DR by defining them entirely in software and avoid the need to re-architect your network or deploy physical appliances	L2 Streching is required for better application availability considering RFP asks for 99.99 % availability on monthly basis. RFP Page 17 -> "4. Service Levels "-->"SLA: The solution is expected to be available for 99.99% on 24x7 and up time availability will be calculated on monthly basis."	No Change, L2 stretching implementation will be discuss with elected bidder.
972	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Container >2	The solution must be able to manage Kubernetes clusters. Licenses for managing Kubernetes clusters should be implemented from Day-1		Request below modified clause be accmodated: The solution must be able to manage Kubernetes clusters. Licenses for managing Kubernetes clusters along with components such as backup, container registry and monitoring alongwith Windows Container support should be implemented from Day-1	Kubernetes Cluster doesn't work in isloation but require other components such as container registry and backup solution. If not included than Bob Card will have procure them separately. And Not aving Windows Container support will block any windows based apps to be deployed on Kubernetes Platform.	Yes, BOBCARD will take care such requirement
973	NA	Appendix02 Techno Functional Requirements- Network components > internal FW NG Firewall Features NEW POINT	Must have provisioning, operations and lifecycle management of Kubernetes, automated deployment, scaling, and operation of Kubernetes clusters		Request below modified clause be accmodated: Must have provisioning, operations and lifecycle management of Kubernetes, automated deployment, Auto scaling & Auto Healing, and operation of Kubernetes clusters	Complete Automation is not possible without Auto Scaling and Auto Healing of Kubernetes Clusters. One has to manually add nodes in case of failure or unprovisioned increase in load.	No Change
974	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Container >4	Container Platform should provide single pane of Glass for Lifecycle Management of all K8S clusters deployed on prem.		Request below modified clause be accmodated: Container Platform should provide single pane of Glass for Lifecycle Management of all K8S clusters alongwith ingress, backup and container registry deployed on prem.	Kubernetes Cluster doesn't work in isloation but require other components such as container registry and backup solution. These shall too be considered for life cycle management	Yes, BOBCARD will take care such requirement
975	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management >1	The solution should provide capability of generating reports for usage, performance, compliance, health, forecasting and capacity.		Request below modified clause be accmodated: The solution should provide capability of generating reports for health, Capacity Optmization - Right Sizing (Under sized, Oversized), Reclamation (Idle, Powered off , Snapshot, Orphaned Disk , Forecasting - Capacity Forecasting, Migration assessment, Migration Planning Usage - Process and service utlization Compliance - Regulatory Benchmark (PCIDSS and ISO) Security Guidelines for Infrastructure and Cloud Management	Bob Cards will need capacity optimization capabilities to identify over-provisioned & under-provisioned resources and provide recommendations, alerts and automated actions on right-sizing and resource consumption so they can be right-sized for adequate performance and avoid resource wastage. Should provide visibility of capacity and VMs which can be reclaimed and cost visibility of the reclaimed capacity and VMs.	No Change, additional feature will be consider as value add
976	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management >11	The solution should have intelligent operations with anomaly detection which will allow monitoring seasonal trends and automatically send email alert		The solution should have AI/ML driven intelligent operations & troubleshooting workbench with anomaly detection,third party infra (Server, Storage , Network, database and Application) along with parent child relatiohship mapping, service and process monitoring which will allow monitoring seasonal trends and automatically send email alert. The solution should also have log management capability for infrastructure and applications . log management solution should delivers intuitive, actionable dashboards, sophisticated analytics, and broad third-party extensibility across physical, virtual, and cloud environments.	BoB Cards will not be able to manage the infrastructure without comprehsive log management capability. Its also mandatory for from regulation/compliance perspective to have log stored for given period of time for audit. BoB Card would need apps (database and Application) to infra (Server, Storage , Network) level visibility for toubleshooting and performance monitoring.	No Change, additional feature will be consider as value add

977	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management >7	The solution must have an approval process to review, reject or approve the deployment requests from the marketplace.		Request below modified clause be considered: The Solution must support multiple levels of approval with E-mail notifications with ability to automate manual provisioning and de-provisioning of the tasks and policies embedded in each layer of their application including auto -approve and auto-reject capability based on application criticality	The solution must have an approval process to review, multi level & auto reject or approve the deployment requests from the marketplace.	No Change, additional feature will be consider as value add
978	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 6	Hypervisor should support container and opensource integration for cloud native application from day-1. Must be a Kubernetes ready from day-1.		Request below modified clause be accmodated: Hypervisor should support container both Linux and Windows along with other kubernetes ecosystems such as container registry, backup, ingress & monitoring and opensource integration for cloud native application from day-1. Must be a Kubernetes ready from day-1.	Kubernetes does't work in isolation and requires multiple components for production setup.	Yes, BOBCARD will take care such requirement
979	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 16	Virtualization Manager should provide feature which can perform quick, as-needed deployment of additional virtualized hosts. When the service is running, it can push out update images, eliminating patching and update without impacting production.		Please clarify the scenario and expected outcome out of the below point in this clause: "When the service is running, it can push out update images, eliminating patching and update without impacting production."		Virtualization manager should allow addition of new nodes and patching/upgrade of hypervisor running on the node without any VM downtime.
980	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 22	Unlimited VM replication from DC to DR (No restriction on VM replication and DR orchestration) with the capability to define Recovery Plans		Request to provide the number of VMs to be orchestrated for automated recovery and not keep open as unlimited since this approach is OEM specific . The VMs to be protected/orchestrated are limited to what can be provisioned on these 14 servers of production. Furehr pls clarify the need for Recovery Plans		No Change, can not predict the exact number of VMs for next 5 Years which need to be replicated.
981	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 23	Proposed solution should have a self-service restore feature on a per-VM basis to allow trusted application administrators to recover their own files with the ability to mount snapshots as a drive in Windows VMs		Request this be modified as below or clarify the requriement: Proposed solution should have a self-service restore feature on a per-VM basis to allow trusted application administrators to recover their own VMs from the snapshot	Please clarify this requirement, this looks like back and restore requirements so the modified clause	This will help BOBCARD to recover file without losing current state of virtual machine.
982	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 24	Hypervisor should provide Visibility for Running VM and their connectivity co-relationship with Network Ports on attached Physical TOR / Core Direct which Include Network RX/TX Bytes.		Request below modified clause with additional inputs be considered : Hypervisor should provide Visibility for Running VM and their connectivity co-relationship with Network Ports on attached Physical TOR / Core Direct which Include Network RX/TX Bytes.Solution Should provide end to end visibility across physical firewall, switch and storage, Flow Analysis and Security Planning,Guided Troubleshooting, Microsegmentation planning, RCA (Connectivity Problem, Packet Loss, N/W latency), Application Discovery, Service Monitoring , Application Dependency Mapping and monitoring of non compliant ports	Monitoring is not considering all components of the stack. Unless end to end visibility is provided as part of this solution BoB Card has to spend separately on monitoring.	Yes, BOBCARD will take care such requirement. However Hypervisor should provide Visibility for Running VM and their connectivity co-relationship with Network Ports on attached Physical Port which Include Network RX/TX Bytes.
983	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 30	Virtualization software or the solution should provide Cluster level encryption protects unauthorized data access at-rest.		Request below modified clause be considered : Virtualization software or the solution should provide Cluster level, VM Level encryption protects unauthorized data access at-rest and in transit.	Having capability to do the enscryption at app VM level and in transit is required to complete solution.	No Change, additional feature will be consider as value add
984	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Software Defined Storage > 1	Maintain primary working set copy of active data on the Local Node as VM's are hosted to provide high IOPS and low latency. Proposed solution must be proposed for faster reads and write for Business-critical Apps.		Request below additional point be added in theis clause : Proposed solution must be proposed for faster reads and write for Business-critical Apps.	Architecture is specific to one vendor, request BoB Cards to consider on outcome than specific architecture. There is no specific latency requirements mentioned in the spec.	No Change.
985	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Software Defined Storage >2	The solution must have De-duplication and Compression features licensed and implemented from day one (Should not have dependency on any proprietary hardware device).		Request below modified clause be considered: The solution must have De-duplication/Compression features licensed and implemented from day one (Should not have dependency on any proprietary hardware device).	Solution should have flexibility to implement either compression and de-duplication. BoB Cards should conisder overhead while deciding on both.	No Change

986	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Software Defined Storage >24	The proposed solution should support 1 min RPO & 1 hour RTO for critical workload in case BOB Cards wants to have this capability replication for Future use. The proposed solution should have native Replication and DR Orchestration from Day-1		What is the use case for 1 min RPO and 1 Hour RTO? is this linked with some regulatory requirement?	Replication is best handled at application level as having additional solution for infrastructure will complexity and cost for BoB Cards Its best to use extends the existing DR orchestration solution for this environment as well.	This is required for BOBCARD mission critical application. The solution should capable to support 1min RPO. The propose replication solution should be same OEM as the virtualization solution to provide seamless integration.
987	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Software Defined Storage >25	The solution provided should function even after one node failure.		Request below modified clause be considered: The solution provided should function even after two node failure.	RFP asks for 99.99 % availability SLA for the proposed solution. It will require minimum N+2 configuration for required resiliency and uptime.	No Change, additional feature will be consider as value add
988	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Software Defined Storage >31	The solution should provide enterprise data services such as compression completely in software. Software Defined Storage solution must have de-duplication and compression features Licensed and implemented from day one. These functionalities should be part of the proposed solution. The solution must have functionality to support compression and or deduplication online on data container without any downtime and data loss as per business requirement.		Request below modified clause be considered: The solution should provide enterprise data services such as compression completely in software. Software Defined Storage solution must have de-duplication or compression features Licensed and implemented from day one. These functionalities should be part of the proposed solution. The solution must have functionality to support compression and or deduplication online on data container without any downtime and data loss as per business requirement.	Solution should have flexibility to implement either compression and de-duplication. BoB Cards should conisder overhead while deciding on both.	No Change
989	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmentation > new point	Additional Point for consideration		The solution must ensure that there is not alteration in the IP address of the Virtual machine, by blocking the traffic from or to the VM inherited as a feature in the Solution.	IP/MAC spoofing is major security concern for organizations like BoB Cards handing customers data.	No Change, additional feature will be consider as value add
990	NA				The solution should support multi-tenancy to isolate networking/security for different departments/function within BoB Cards upto a minimum of 4 tenants and 5 VPCs	VPC will enable Bob Cards to create isolation from access , resources, network and security.	ange, additional feature will be consider as valu
991	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Container > 6	Should support cluster scale out i.e addition of worker nodes as and when required.		Request below modified clause be considered: Should support Automated cluster scale out i.e addition of worker nodes as and when required.	Complete Automation is not possible without Auto Scaling and Auto Healing of Kubernetes Clusters. One has to manually add nodes in case of failure or unprovisioned increase in load.	No Change
992	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > 3	The solution shall provide a single pane of glass for automated provisioning with model-based orchestration of compute, network and storage through a unified multi-tenant self-service catalog.		Request below modified clause be consiered The solution shall provide a single pane of glass for automated provisioning with model-based orchestration of compute, network , storage and Kubernetes through a unified multi-tenant self-service catalog .	All modern applications are combination of both container and VM form factor.	No Change, additional feature will be consider as value add
993	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > 5	The solution must provide a self-service portal to allow user to consume the creation of infrastructure easily.		Request below modified clause be considered: The solution must provide a self-service portal to allow user to consume the creation of infrastructure easily for both VM and Kubernetes	All modern applications are combination of both container and VM form factor.	No Change, additional feature will be consider as value add
994	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > 8	The software must allow the designer to use shell script, PowerShell script to code the automation.		Request below modified clause be considered: The software must allow the designer to use shell script, PowerShell script, Python and node JS to code the automation.	Python and nodeJs are very popular language for scrpting in terms resource availability and community support	No Change, additional scripting will be value add
995	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > 9	The software must allow the designer to design VM blueprints.		Request below modified clause be considered: The software must allow the designer to design Multi VM & Kubernetes blueprints.	All modern applications are combination of both container and VM form factor.	No Change, additional feature will be consider as value add
996	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > 12	The solution should have simple low-code, no-code automation engine which allows automating day-to-day routine tasks		Request below modified clause and adidtoinal inpurs on the clause be considered: The solution should have simple low-code, no-code automation engine which allows automating day-to-day routine tasks such as Snapshot creation, Addition of Disk, Power Cycle (Suspend , Shutdown, Reboot, reset), Resize, Rebuild, Additional of Network, VM Unregister , Delete,connect remote console, Change Security Group with capability to create additional resource actions as out of the box capability.	All modern applications are combination of both container and VM form factor.	No Change, additional feature will be consider as value add

997	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > New Point	New Point		Solution should provide capability to define and showcase cost to create cloud like experience to the business unit with the overall cost spend on the infrastructure [server hardware, storage, licenses, application, maintenance, labor, network, facilities , etc.	Bob Cards will need Cost transparency (Showback and Chargeback capability) across private, hybrid to optimize planning and prioritization of VM/ Server/Application onboarding/provisioning	No Change, additional feature will be consider as value add
998	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF & IPS	New Point		We request BoB Card to allow for both software and hardware based solution for Load Balancer, WAF, IPS/IDS. As these components are dynamic as per application consumption requirements and considering bob card is directly managing customer data, its very critcal that these components are added as part of sofwate defined stack.	Modern applications increasingly require software-defined networking (SDN) and security solutions due to their need for greater flexibility, agility, and scalability. Traditional networking and security methods often lack the adaptability to support the dynamic nature of modern application environments, especially in cloud	No Change
999	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF C.Solution Capabilites Pont #5	The solution must support and integrate the web application vulnurability tools (Web application scanners) being proposed by bidder as part of this RFP at minimum to virtually patch web application vulnurabilies or else solution should have ready plug-ins to integrate banks VAPT tool.		Requesting you to modify the clause as below: The solution must support and integrate the web application vulnurability tools (Web application scanners) being proposed by bidder as part of this RFP, solution should have ready plug-ins to integrate banks VAPT tool.	Solution should be capable to protect against zero-day vulnerability using positive security model without being dependent on virtual patching. Virtual patch can even lead to false positive.	No Change
1000	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #2	Appliance/Chassis based Hardware should support scalability with license upgrade. -18 vCPU from day 1 | Scalable to 32 vCPU -128 GB DDR RAM from day 1 -1 TB X 1 SSD M.2 SSD (in Raid) from Day 1		The clause represents single OEM offering for sizing		No Change
1001	NA	7/B.Hardware & InAppendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #7	The proposed appliance shoulde provide minimum 1.2 Gbps of real world WAF throughput from day 1 and should be scalable to 2.2 Gbps with license upgrade on the same hardware or additional blades in case of a chassis based solution. The WAF throughput mentioned should be inclusive after enabling the below mentioned features: With all WAF functions enabled per intance in blocking mode SSL inspection.		The clause represents single OEM offering for sizing		No Change
1002	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #8	The appliance should support the layer 7 throughput should be at least 58 Gbps scalable to 92 Gbps on same hardware with license upgrade. (Data rerernces for above should be verified from publicly available datasheet)		The clause represents single OEM offering for sizing		No Change
1003	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #9	The proposed appliance must have minimum hardware compression of 34 Gbps for HTTP traffic form day 1 and scalable upto 48 Gbps with add on license on same hardware. (Data rerernces for above should be verified from publicly available datasheet)		The clause represents single OEM offering for sizing		No Change
1004	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #10	The proposed appliance should support minimum hardware based SSL offloading from day 1 up to : 34 Gbps Scalable upto 48 Gbps on same hardware with license upgrade. (The SSL encryption & decryption process must be hardware-based proccessor for acceleration) (Data rerernces for above should be verified from publicly available datasheet)		The clause represents single OEM offering for sizing		No Change

1005	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #11	The solution must support minimum SSL TPS/CPS: -29 K ECDSA P-256-bit keys from day 1 -58 K RSA 2048-bit keys from day 1 scalable to minimum SSL TPS/CPS -68 K ECDSA P-256-bit keys -98 K of RSA 2048-bit Keys (Data rerernces for above should be verified from publicly available datasheet with SSL)		The clause represents single OEM offering for sizing		No Change
1006	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #12	The proposed appliance should support minimum 74 million L4 concurrent connections from day one and scalable upto 99 Million on same hardware with license upgrade.		The clause represents single OEM offering for sizing		No Change
1007	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #13	The proposed appliance should support minimum 2.4 million L7 requests per seconds from day 1 and scalable upto 4.2 Million on same hardware with with license upgrade.		The clause represents single OEM offering for sizing		No Change
1008	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF General Requirement Point #13	The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide traffic performance statistics for last 30 days including Active Connections, Active Sessions, CPU Usage By Core, HTTP Requests, Memory Used, RAM Cache Utilization, Rewrite Transaction, Data Rewrite Transactions, SSL Transactions, Throughput(bits), Throughput(packets), & Total New Connections		The clause should mention the functionality should be achieved without being dependent on tools.	The clause represents single OEM offering.	No Change
1009	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #14	The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide a security event timeline dashboard where critical events like Audit logs, Pool status change, Failover status change, DOS attacks etc. must be shown for ease of troubleshooting with last 20 Failed logins details		The clause should mention the functionality should be achieved without being dependent on tools.	The clause represents single OEM offering.	No Change
1010	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #15	The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide a Bug tracker option, where an admin can login and find any bugs affecting the devices		The clause should mention the functionality should be achieved without being dependent on tools.	The clause represents single OEM offering.	No Change
1011	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #16	The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide an upgrade Options suggestions for next hotfix and stability release for ease of day-2 operations with single click access to release notes a nd EOS dates		The clause should mention the functionality should be achieved without being dependent on tools.	The clause represents single OEM offering.	No Change
1012	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #17	The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide an ability to execute CLI commands which are essential for diagnostics which will show historic data or data at the time of file captured. E.g show history of all executed commands on the CLI		Request you to remove this clause	Database Load Balancer is provided as inbuilt feature from database solution provider and hence not needed from SLB solution	No Change
1013	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF C.Solution Capabilities Point #23	Solution should have the capability to highlight (In red / any color code) only malicious payload from the entire attack payload on the event analysis dashboard for detailed fornsics analysis. This is extermly critical when our incident response teams are in combat with the attackers during wartime. This feature/functionality has to be live demonstrated by the bidder after the prebid query meeting, by setting up a lab in the cloud/on-premises		Forensics are not required for LB or WAF kind of solution. This is required for DDoS kind of solution and it is not recommended to have DDoS solution within WAF+LB as DDoS should be a stateless technology and it's placement should be at perimeter level above firewall to protect complete infrastructure		No Change

1014	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF C.Solution Capabilities Point #36	The Proposed WAF Solution should provide built-in L7 layer DDoS detection and mitigation features based on machine learning and behavioral analytics and dynamic signatures. It should have CAPTCHA support or other mechanism to avoid distributed attack. This feature/functionality has to be live demonstrated by the bidder after the prebid query meeting, by setting up a lab in the cloud/on-premises.		Request to remove this point	DDoS should be a stateless device and it's placement should be at perimeter level above firewall. This ensures protection to network from any advanced DDoS attacks. Hence, it should not be expected to be part of other security solutions within the network.	No Change
1015	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF C.Solution Capabilities Point #58	The Solution should have IPSEC tunneling capabiltiies		Request to remove this point	VPN is recommended to be a dedicated solution since it relies on TLS protocol. It is also recommended to terminate the traffic on Firewall or before Firewall as it will check for security parameters on the same. If this is done on ADC, there won't be any security check and can possess threat or security flaw.	No Change
1016	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF C.Solution Capabilities Point #59	The proposed solution should support a comprehensive list of ways in which LB can monitor the backend services including Daimeter, DNS, FTP, Gateway ICMP, HTTP, HTTPS, TCP half open, TCP , LDAP, MSSQL, MYSQL, MQTT , POSTGRESQL, POP3 , IMAP, NNTP, Radius , SIP and custom external scripts		Request to modify the clause as below: The proposed solution should support a comprehensive list of ways in which LB can monitor the backend services including DNS, FTP, Gateway ICMP, HTTP, HTTPS, TCP half open, TCP , LDAP, MSSQL, MYSQL , POSTGRESQL, POP3 , IMAP, NNTP, Radius and custom external scripts	SIP, Diameter & MQTT Traffic are used in Service Provider environment and are not relevant and used in any Enterprise environment like BOB Cards.	No Change
1017	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF C.Solution Capabilities Point #61	The proposed solution should support various types of LB config for handling traffic, including standard reverse proxy, forwarding in L2 , Forwarding in IP, High performance mode, Stateless mode , Reject mode, DHCP relay, and Message routing for SIP, Daimeter and MQTT traffic		Request this clause be modified as below: The proposed solution should support various types of LB config for handling traffic, including standard reverse proxy, forwarding in L2 , Forwarding in IP, High performance mode, Stateless mode , Reject mode, DHCP relay	SIP, Diameter & MQTT Traffic are used in Service Provider environment and are not relevant and used in any Enterprise environment like BOB Cards.	No Change
1018	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF C.Solution Capabilities Point #70	The proposed solution should support native integration with kubernetes based platforms hosting microservices e.g. Openshift, TKG cluster etc. Solution should update the configuration of LB automatically by observing events within kubernetes clusters form day 1 without add on license.		Solution should be able to support by means of same solution.		No Change
1019	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF C.Solution Capabilities Point #81	The proposed LB solution should also support secure remote access to admin users (concurrency of not more than 10); where the solution can do endpoint checks for the admins and establist a secure tunnel with autentication against AD/OAUTH/Radius and MFA via Google authenticator. The system should allow per user basis a login schedule ?(e.g night shift employee cannot login during working hours)		The clause represents single OEM offering.		No Change
1020	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF D.Availability #2	The solution should support SQL-based querying for the following databases for the health checks: for Oracle, MSSQL, MySQL, PostgresSQL and other databases if required in future.		Request this clause be removed	Database Load Balancer is provided as inbuilt feature from database solution provider and this is proprietary load balancing feature of Database solution provider and hence not needed from ADC solution.	No Change
1021	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #7	The Firewall appliance should have certifications like ICSA /EAL4/CCNDPP		Request this be modified as below: The Firewall solution should have certifications like ICSA /EAL4/CCNDPP	Every OEM has its own solution offering and certification ask may align to the approach solution is provided rather than mandating it on the appliance inline to a particular OEM	No Change

1022	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #9	OEM/Bidder should provide below transceivers from Day-1. Firewall and SFP should be from same OEM. Below mentioned SFP quantity is required per appliance. 4 X 10GE SR SFP+ 4 X 1G SFP 4 x 25G SFP28		OEM/Bidder should provide below transceivers from Day-1. Firewall and SFP should be from same OEM. Below mentioned SFP quantity is required per appliance. 4 X 1G RJ 45 4 X 10G SFP+ 4 x 25G SFP28	Requesting if 1G can be considered using Copper Links and not SFP	No Change
1023	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #15	Solution should have minimum 450 GB SSD pair, system storage		Request to modify this as below Solution should have minimum 900 GB SSD pair, system storage	Perimeter Firewall needs high storage numbers as visible with mid/large scale deployments for storing logs considering 3/6 months retention in case the remote Management device is impacted , so good to ask for more	No Change, additional feature will consider as value add
1024	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #16	Solution should have minimum 32 GB		Request clause to be modifiedL Solution should have minimum 128 GB RAM	Perimeter Firewall has to have good RAM and such baselining will help with operations of critical banking infra	No Change, additional feature will consider as value add
1025	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #19	"The proposed firewall must provide minimum 10 Gbps of Threat prevention throughput with Real world traffic. (Throughput must be derived from Appmix traffic and not Video/JPEG based traffic) (enterprise testing condition). The throughput must remain 10 Gbps even after enabling NGFW + IPS/IDS + Antivirus + Anti Spyware + Anti Bot + DoS/DDOS + All signature enabled + Logging enabled + Bidirectional inspection + File Blocking. OEM to provide publicly available The Test methodology and result should be compliant to the benchmark testing methodology for the above parameters provided in the Internet Engineering Task Force (IETF)- 'Benchmarking Methodology for Network Security Device Performance document mentioning throughput with transaction size, traffic mix. enabled on day 1. No cluster based solution should be quoted to meet the above requirement.		Request below modified clause be considered , instead of Appmix traffic , real world traffic should be mentioned for deriving throughput "The proposed firewall must provide minimum 10 Gbps of Threat prevention throughput with Real world traffic. (Throughput must be derived from real world traffic and not Video/JPEG based traffic) (enterprise testing condition). The throughput must remain 10 Gbps even after enabling NGFW + IPS/IDS + Antivirus + Anti Spyware + Anti Bot + DoS/DDOS + All signature enabled + Logging enabled + Bidirectional inspection + File Blocking. OEM to provide publicly available The Test methodology and result should be compliant to the benchmark testing methodology for the above parameters provided in the Internet Engineering Task Force (IETF)- 'Benchmarking Methodology for Network Security Device Performance document mentioning throughput with transaction size, traffic mix. enabled on day 1. No cluster based solution should be quoted to meet the above requirement.	instead of appmix traffic real world traffic will be rifht measure of throuhput , so requesting the change	No Change
1026	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #21	NGFW appliance must be capable of handling minimum 2 M concurrent sessions utilizing HTTP transactions with all Security feature Turned ON and not based on UDP / Lab environment / ideal testing environment, this claim has to be supported with declaration of concurrent connections claim from OEM		Request below modified clause to accomodate support for 5M concurrent sessions NGFW appliance must be capable of handling minimum 5 M concurrent sessions utilizing HTTP transactions with all Security feature Turned ON and not based on UDP / Lab environment / ideal testing environment, this claim has to be supported with declaration of concurrent connections claim from OEM	Mid/Large scale deployments need higher concurrent session support and baselining this to 50 Lakh concurrent sessions will be in the interest of the Bank , so the requested change	No Change, additional feature will consider as value add
1027	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #49	Solution should support creation of minimum 1 virtual context / instance from Day-1 without any compromise on system performance and network bandwidth.		Solution should support creation of minimum 5 virtual context /instance from Day-1 without any compromise on system performance and network bandwidth.	Support for only 1 Virtual context may not be scalable for the DC design and min support for 5 instances is the need for any DC infra Perimeter Firewall understanding furture state architecure and growing needs.	No Change, additional feature will consider as value add

1028	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #54	The proposed NGFW solution architecture should have Control Plane separated from the Data Plane in the Firewall appliance architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup, QoS, NAT etc). Control plane must have dedicated resources such as CPU, RAM etc. This is to ensure Bank always has management access to NGFW irrespective of Firewall load / Traffic Spike / Cyber Attack driving higher CPU utilization. Bank should able to login to the firewall and carry out reporting / management / packet capture etc to identify the root cause and ccordingly take necessary action to remediate it.		Request below modified clause be considered

The proposed NGFW solution architecture should have Control Plane separated from the Data Plane in the Firewall solution architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup, QoS, NAT etc). Control plane must have dedicated resources such as CPU, RAM etc. This is to ensure Bank always has management access to NGFW irrespective of Firewall load / Traffic Spike / Cyber Attack driving higher CPU utilization. Bank should able to login to the firewall and carry out reporting / management / packet capture etc to identify the root cause and accordingly take necessary action to remediate it. | OEMs have different approaches to achieving the use case and instead of the ask on the appliance itself , the Firewall Solution will be a generic term to use in requirements so this suggestion | No Change |
| 1029 | NA | Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #72 | IPS should provide detailed information on each protection, including: Vulnerability and threat descriptions, Threat severity, Performance impact, Release date, Industry Reference, Confidence level etc. | | Request below changed clause :

IPS should provide detailed information on each protection, including: Vulnerability and threat descriptions, Threat severity, Release date, etc | Performance impact, industry reference and confidence level are subject to configuration and infrastructure in the bank. | No Change |
| 1030 | NA | Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #76 | Should have more than 60+ predefined Categories based on Urls, Application types, Security Risk level etc. However solution should be able to create custom categories for URL and application. | | Request below modified clause with increased number of categories:

Should have more than 80+ predefined Categories based on Urls, Application types, Security Risk level etc. However solution should be able to create custom categories for URL and application. | Having more predefined categories support would help bank with improved threat detection and better granular policy control with less manual effort. | No Change, additional feature will consider as value add |
| 1031 | NA | Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #89 | Solution should give information related to Performance impact and confidence level of protections while creating profiles. | | Request this clause be deleted | performance can be subject to policy configurations and existing infra at bank. | No Change |
| 1032 | NA | Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #114 | "Management server should support the following for rule optimization:
• Unused Rules Calculation for specific time-period based on Firewall Traffic Logs.
• Analysis on Covered/Shadow/Hidden Rules
• Analysis on Rules Consolidation (Merging of similar kind of rules)
• Analysis on Redundant Rules
• Tightening of Overly Permissive Rules (Any-Any)
• Analysis on Unattached/Unused Objects to simplify objects management
• Analysis on Rule-Reordering to improve the performance of the Firewall
• Analysis on Disabled/Expired Rules for enhanced visibility on the Firewall Rules sets" | | "Management server should support the following for rule optimization:
• Unused Rules Calculation for specific time-period based on Firewall Traffic Logs / HIt count
• Analysis on Covered/Shadow/Hidden Rules
• Analysis on Redundant Rules
• Analysis on Unattached/Unused Objects to simplify objects management
• Analysis on Disabled/Expired Rules for enhanced visibility on the Firewall Rules sets" | OEMs could be handling the use case suggested for removal differently or have no dependency on the performance of the Firewall , so requesting these be removed from the ask | No Change |
| 1033 | NA | Appendix02 Techno Functional Requirements- Network components > IPS Features Point #15 | Should support more than 3000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness | | Should support more than 5000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness | Increasing number of signature support is beneficial for the Bank's operations and for Effective Security reasons | No Change |

1034	NA	Appendix02 Techno Functional Requirements- Network components > internal FW Point #11	The Firewall solution Should support more than 4000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness and should be able to create 40 or more application categories for operational efficiency. Dedicated IPS solution shall be in corporated by the bidder to achive this scale of IPS AVC signatures in this solution.	Request this clause be modfied as below: The Firewall solution Should support more than 6000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness and should be able to create 40 or more application categories for operational efficiency. Dedicated IPS solution shall be in corporated by the bidder to achive this scale of IPS AVC signatures in this solution.	Increasing number of signature support is Beneficial for the Bank's operations and for Effective Security reasons	No Change, additional feature will consider as value add
1035	NA	Appendix02 Techno Functional Requirements- Network components > internal FW NG Firewall Features NEW POINT	New Point to be added	The solution should provide Change Management capability for the organizations needs to implement more formal processes for configuration changes, including audit tracking and official approval before changes are deployed.	By leveraging these features and integrating with external change management tools, organizations can implement a robust change management process that includes formal approval, audit tracking, and compliance reporting within Cisco FMC.	No Change
1036	NA			The solution should provide traffic hit count, Rule Conflict Detection (Redundant & Shadowed) and policy warning for streamlining firewall policies.	These features are crucial for optimizing firewall policies, ensuring efficient traffic flow, and maintaining security posture.	No Change, additional feature will be consider as value add
1037	NA	Appendix02 Techno Functional Requirements- Network components > internal FW Hardware Architecture Point #3	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 8x64 GB of RAM.	Request below modified clause be considered as correction on the ask which seems typo: 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.		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.
1038	NA	Appendix02 Techno Functional Requirements- Network components > Mngmt Switch 6 Product Support Point #2	The OEM support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support	Request below modified clause be considered The OEM/OEM certified partner support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support	OEM Certified partner has thorough experience of OS version upgrades and maintaining network operations troubleshooting issues and it will be cost effective to include this in the ask	The OEM/OEM certified partner support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support
1039	NA	Appendix02 Techno Functional Requirements- Network components > Mngmt Switch 9 Miscellaneous Points Point #1	Console cable and power cable (As per Indian standards) as per customer requirement to be provided. All Cables shall be factory-terminated.	Since Console Cables are common for all devices per OEM , Request Bank to clarify the count of console cables to be provided , is it one each with each Switch or one per DC and DR Each ?.		No Change
1040	NA	Appendix02 Techno Functional Requirements- Network components > Mngmt Switch 10 Product Support Point #2	The OEM support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support	Request below modified clause be considered The OEM/OEM certified partner support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support	OEM Certified partner has thorough experience of OS version upgrades and maintaining network operations troubleshooting issues and it will be cost effective to include this in the ask	The OEM/OEM certified partner support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support
1041	NA	Appendix02 Techno Functional Requirements- Network components > Core Swtich >9 Manageability > Appliance point 9.4	Switch Anomolies related with Advisories , PSIRT and Field Notices	Request this clause be removed from the telemetry asks	This feature is not requireed for the design at the BOB DataCenter and may be removed	No Change
1042	NA	Appendix02 Techno Functional Requirements- Network components > Core Swtich >13 Fabric Management > Appliance point 13.1	Solution must provide Centralized Management Appliance – Single pane of glass for managing, monitoring and provisioning the entire Solution within Data Center & across all Data Centers	Request BOBCards to provide VM compute resources for spinning up the VMs to provide this functionality while we can provide the necessary sw and support.		Requested product functionality should be comply, BOBCards will provide VM compute resources for spinning up the VMs to provide this functionality however bidder should provide the necessary sw and support.
1043	NA	Appendix02 Techno Functional Requirements- Network components > Core Swtich >5 Layer 2 Features > Appliance point 5.11	Switch Hardware should have capability to support BGP EVPN Route Type 1, Type 2, Type 3, Type 4, Route Type 5, Type 6/Type 7/Equivalent routes	Request this point be removed	BOBCards design doesn't have Fabric so this is not applicable	No Change
1044	NA	Appendix02 Techno Functional Requirements- Network components > Core Swtich >13 Fabric Management > Appliance point 13.36	Solution should provides reports using predefined templates, including inventory, use, and health reports.	Request below modified clause be considered: Solution should provides reports including inventory, use, and health reports.		No Change

1045		Appendix02 Techno Functional Requirements- Network components > LB+WAF C.Solution Capabilites Pont #5	The solution must support and integrate the web application vulnurability tools (Web application scanners) being proposed by bidder as part of this RFP at minimum to virtually patch web application vulnurabilies or else solution should have ready plug-ins to integrate banks VAPT tool.		Hence, requesting you to modify the clause as below: The solution must support and integrate the web application vulnurability tools (Web application scanners) being proposed by bidder as part of this RFP, solution should have ready plug-ins to integrate banks VAPT tool.	Suggestion: Solution should be capable to protect against zero-day vulnerability using positive security model without being dependent on virtual patching. Virtual patch can even lead to false positive.	No Change
1046		Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #2	Appliance/Chassis based Hardware should support scalability with license upgrade. -18 vCPU from day 1 | Scalable to 32 vCPU -128 GB DDR RAM from day 1 -1 TB X 1 SSD M.2 SSD (in Raid) from Day 1		Hence requesting you to kindly mention no. of cores for processor required in the appliance	The clause represents single OEM offering for sizing.	No Change
1047		7/B.Hardware & InAppendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #7	The proposed appliance shoulde provide minimum 1.2 Gbps of real world WAF throughput from day 1 and should be scalable to 2.2 Gbps with license upgrade on the same hardware or additional blades in case of a chassis based solution. The WAF throughput mentioned should be inclusive after enabling the below mentioned features: With all WAF functions enabled per intance in blocking mode SSL inspection			The clause represents single OEM offering for sizing	No Change
1048		Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #8	The appliance should support the layer 7 throughput should be at least 58 Gbps scalable to 92 Gbps on same hardware with license upgrade. (Data rerernces for above should be verified from publicly available datasheet)		Hence requeting you to	The clause represents single OEM offering for sizing	No Change
1049		Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #9	The proposed appliance must have minimum hardware compression of 34 Gbps for HTTP traffic form day 1 and scalable upto 48 Gbps with add on license on same hardware. (Data rerernces for above should be verified from publicly available datasheet)			The clause represents single OEM offering for sizing	No Change
1050		Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #10	The proposed appliance should support minimum hardware based SSL offloading from day 1 up to : 34 Gbps Scalable upto 48 Gbps on same hardware with license upgrade. (The SSL encryption & decryption process must be hardware-based proccessor for acceleration) (Data rerernces for above should be verified from publicly available datasheet)			The clause represents single OEM offering for sizing	WAF/LB:
1051		Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #11	The solution must support minimum SSL TPS/CPS: -29 K ECDSA P-256-bit keys from day 1 -58 K RSA 2048-bit keys from day 1 scalable to minimum SSL TPS/CPS -68 K ECDSA P-256-bit keys -98 K of RSA 2048-bit Keys (Data rerernces for above should be verified from publicly available datasheet with SSL)			The clause represents single OEM offering for sizing	No Change

1052		Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #12	The proposed appliance should support minimum 74 million L4 concurrent connections from day one and scalable upto 99 Million on same hardware with license upgrade.		The clause represents single OEM offering for sizing	No Change
1053		Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #13	The proposed appliance should support minimum 2.4 million L7 requests per seconds from day 1 and scalable upto 4.2 Million on same hardware with with license upgrade.	Hence requesting you to kindly change this point as below: The proposed appliance should support minimum 2.4 million L7 requests per seconds from day 1 and scalable upto 3.8 Million on same hardware with with license upgrade.	The clause represents single OEM offering for sizing	No Change
1054		Appendix02 Techno Functional Requirements- Network components > LB+WAF General Requirement Point #13	The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide traffic performance statistics for last 30 days including Active Connections, Active Sessions, CPU Usage By Core, HTTP Requests, Memory Used, RAM Cache Utilization, Rewrite Transaction, Data Rewrite Transactions, SSL Transactions, Throughput(bits), Throughput(packets), & Total New Connections	Hence requesting you to kindly change this point as below: Solution should provide traffic performance statistics for last 30 days including Active Connections, Active Sessions, CPU Usage By Core, HTTP Requests, Memory Used, RAM Cache Utilization, Rewrite Transaction, Data Rewrite Transactions, SSL Transactions, Throughput(bits), Throughput(packets), & Total New Connections	The clause represents single OEM offering. The clause should mention the functionality should be achieved without being dependent on tools.	No Change
1055		Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #14	The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide a security event timeline dashboard where critical events like Audit logs, Pool status change, Failover status change, DOS attacks etc. must be shown for ease of troubleshooting with last 20 Failed logins details	Hence requesting you to kindly change this point as below: Solution should provide a security event timeline dashboard where critical events like Audit logs, Pool status change, Failover status change, DOS attacks etc. must be shown for ease of troubleshooting with last 20 Failed logins details	The clause represents single OEM offering. The clause should mention the functionality should be achieved without being dependent on tools.	No Change
1056		Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #15	The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide a Bug tracker option, where an admin can login and find any bugs affecting the devices	Hence requesting you to kindly change this point as below: Solution should provide a Bug tracker option, where an admin can login and find any bugs affecting the devices	The clause represents single OEM offering. The clause should mention the functionality should be achieved without being dependent on tools.	No Change
1057		Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #16	The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide an upgrade Options suggestions for next hotfix and stability release for ease of day-2 operations with single click access to release notes a nd EOS dates	Hence requesting you to kindly change this point as below: Solution should provide an upgrade Options suggestions for next hotfix and stability release for ease of day-2 operations with single click access to release notes a nd EOS dates	The clause represents single OEM offering. The clause should mention the functionality should be achieved without being dependent on tools.	No Change
1058		Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #17	The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide an ability to execute CLI commands which are essential for diagnostics which will show historic data or data at the time of file captured. E.g show history of all executed commands on the CLI	Request this clause be removed	Suggestion: Database Load Balancer is provided as inbuilt feature from database solution provider and hence not needed from SLB solution	No Change
1059		Appendix02 Techno Functional Requirements- Network components > LB+WAF C.Solution Capabilities Point #23	Solution should have the capability to highlight (In red / any color code) only malicious payload from the entire attack payload on the event analysis dashboard for detailed fornsics analysis. This is extermly critical when our incident response teams are in combat with the attackers during wartime. This feature/functionality has to be live demonstrated by the bidder after the prebid query meeting, by setting up a lab in the cloud/on-premises	Request this clause be removed	Suggestion: Forensics are not required for LB or WAF kind of solution. This is required for DDoS kind of solution and it is not recommended to have DDoS solution within WAF+LB as DDoS should be a stateless technology and it's placement should be at perimeter level above firewall to protect complete infrastructure	No Change

1060		Appendix02 Techno Functional Requirements- Network components > LB+WAF C.Solution Capabilities Point #36	The Proposed WAF Solution should provide built-in L7 layer DDoS detection and mitigation features based on machine learning and behavioral analytics and dynamic signatures. It should have CAPTCHA support or other mechanism to avoid distributed attack. This feature/functionality has to be live demonstrated by the bidder after the prebid query meeting, by setting up a lab in the cloud/on-premises		Request this clause be removed	Suggestion: DDoS should be a stateless device and it's placement should be at perimeter level above firewall. This ensures protection to network from any advanced DDoS attacks. Hence, it should not be expected to be part of other security solutions within the network.	No Change
1061		Appendix02 Techno Functional Requirements- Network components > LB+WAF C.Solution Capabilities Point #58	The Solution should have IPSEC tunneling capabiltiies		Request this clause be removed	VPN is recommended to be a dedicated solution since it relies on TLS protocol. It is also recommended to terminate the traffic on Firewall or before Firewall as it will check for security parameters on the same. If this is done on ADC, there won't be any security check and can possess threat or security flaw.	No Change
1062		Appendix02 Techno Functional Requirements- Network components > LB+WAF C.Solution Capabilities Point #59	The proposed solution should support a comprehensive list of ways in which LB can monitor the backend services including Daimeter, DNS, FTP, Gateway ICMP, HTTP, HTTPS, TCP half open, TCP , LDAP, MSSQL, MYSQL, MQTT , POSTGRESQL, POP3 , IMAP, NNTP, Radius , SIP and custom external scripts		Request to modify the clause as below: The proposed solution should support a comprehensive list of ways in which LB can monitor the backend services including DNS, FTP, Gateway ICMP, HTTP, HTTPS, TCP half open, TCP , LDAP, MSSQL, MYSQL , POSTGRESQL, POP3 , IMAP, NNTP, Radius and custom external scripts	Suggestion: SIP, Diameter & MQTT Traffic are used in Service Provider environment and are not relevant and used in any Enterprise environment like BOB Cards.	No Change
1063		Appendix02 Techno Functional Requirements- Network components > LB+WAF C.Solution Capabilities Point #61	The proposed solution should support various types of LB config for handling traffic, including standard reverse proxy, forwarding in L2 , Forwarding in IP, High performance mode, Stateless mode , Reject mode, DHCP relay, and Message routing for SIP, Daimeter and MQTT traffic		Request this clause be modified as below: The proposed solution should support various types of LB config for handling traffic, including standard reverse proxy, forwarding in L2 , Forwarding in IP, High performance mode, Stateless mode , Reject mode, DHCP relay	Suggestion: SIP, Diameter & MQTT Traffic are used in Service Provider environment and are not relevant and used in any Enterprise environment like BOB Cards.	No Change
1064		Appendix02 Techno Functional Requirements- Network components > LB+WAF C.Solution Capabilities Point #70	The proposed solution should support native integration with kubernetes based platforms hosting microservices e.g. Openshift, TKG cluster etc. Solution should update the configuration of LB automatically by observing events within kubernetes clusters form day 1 without add on license.		Request this clause be modified as below: The proposed solution should support native integration with kubernetes based platforms hosting microservices e.g. Openshift, TKG cluster etc. Solution should update the configuration of LB automatically by observing events within kubernetes clusters form day 1 with/without add on license.	Suggestion: Solution should be able to support by means of same solution.	No Change
1065		Appendix02 Techno Functional Requirements- Network components > LB+WAF C.Solution Capabilities Point #81	The proposed LB solution should also support secure remote access to admin users (concurrency of not more than 10); where the solution can do endpoint checks for the admins and establist a secure tunnel with autentication against AD/OAUTH/Radius and MFA via Google authenticator. The system should allow per user basis a login schedule ?(e.g night shift employee cannot login during working hours)		Request this clause be removed	The clause represents single OEM offering.	No Change

1066			Appendix02 Techno Functional Requirements- Network components > LB+WAF D.Availability #2	The solution should support SQL-based querying for the following databases for the health checks: for Oracle, MSSQL, MySQL, PostgresSQL and other databases if required in future.	Request this clause be removed	Suggestion: Database Load Balancer is provided as inbuilt feature from database solution provider nd this is proprietary load balancing feature of Database solution provider and hence not needed from ADC solution.	No Change
1067	9	2.2		The tenure of the contract initially would be for 1 year from the date of the issuance of first purchase order. BOBCARD can further extend to 2 years at its at mutually agreed terms.	Contradict statement mentioned in RFP page number 13, 17 clause. Kindly clarify. Mentioned initial contract will be for 3years	The tenure of the contract should be 3years,it will be commercially viable for both entity in case of subscription/services.	Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
1068	31	8		Network components delivery timeline 5-6 weeks		In case of Cisco Network components delivery period will be 8-10 weeks.So requesting waiver on LD cluase if cisco lies in final procurement stage	Supply of Servers & Network component as prescribed under hardware requirement Within 6-8 weeks from date of PO. Rest all clause remain same
1069	Appendix 03	optimal commercial (sheet2)		Windows latest OS datacentre edition - Qty 06	Clarification on number of Microsoft license consideration		As mentioned in the RFP quote for total core of each server for 6 nodes.
1070	8	2-2.1		Intent	The price quoted by the bidder should cover all the support to the solution including any updates/upgrades and fixing any issues faced. Bidder should provide onsite support to fix the issues for the period of 1 Year.Remote access would not be permitted for any support / training / change / upgrade / patch management etc	Please revise to: " Bidder should provide onsite support to fix the issues for the period of 1 Year after implemenation/signoff.Remote access would not be permitted for any support / training / change / upgrade / patch management etc"	The price quoted by the bidder should cover all the support to the solution including any updates/upgrades and fixing any issues faced. Bidder should provide onsite support to fix the issues for the period of 1 Year after declared the project Go-Live. Remote access would not be permitted for any support / training / change / upgrade / patch management etc
1071	8	2-2.1		Intent	Bidder should provide 1year of hand holding support post Go-Live, this may extend to 2 years on mutual understanding.	Please confirm if the SLA/contract terms for 2nd Year will remain the same.	This will be decided basis on the 1st year performance.
1072	9	2-2.1		Intent	Bidder is expected to train the administrator/business users till the personnel gain enough expertise in the system and capable of taking over the operational function. The training should include features, facilities, operations, implementation, troubleshooting, system administration and DR elements if any.	Please confirm if training is only to be extended till the onsite support period.	This will be one time training. Training need to be provided in BOBCARD Office inperson for implemented solution.
1073	11	3.1-2		Project Scope	Considering the extensive nature of the assignment and the envisaged relationship with the Bidder, any service, which forms a part of facilities management that is not explicitly mentioned in this RFP as excluded would form part of this RFP, and the Bidder is expected to provide the same at no additional costs to the Company. The Bidder has to envisage all necessary services to be provided and ensure the same is delivered to the Company. The Company will not accept any plea of the Bidder at a later date for omission of critical services on the pretext that the same was not explicitly mentioned in the RFP.	Please elaborate on the other facilities management requirement apart from the RFP SOW	No Change.

1074	12	3.1-5	Project Scope		Successful bidder should allocate a network architect to design the network architecture	Please provide the current network architecture	Successful bidder should allocate a network architect to design the network architecture for propose solution during implementation.
1075	12	3.1-7	Project Scope		The successful bidder should also integrate existing infrastructure setup (like existing LAN, proxy, MFA, SIEM) with the new devices to be supplied.	Please provide the current network architecture	This will be market leading product only. Basis on compatibility Bidder has to integrate the existing infra setup with new setup. All the product will be share only with the final bidder
1076	12	3.1-11	Project Scope		The resolution time for the hardware/software related issues should be 4 hours, there should be 24*7*365 support from the OEM for all the supplied products through this RFP.	Please revise to "The resolution time for the hardware/software related issues should be 6 hours"	No Change.
1077	14	3.1-21	Project Scope		The successful bidder 's resources will be required onsite during the testing phase.	Please specify the testing duration	Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
1078	14	3.1-28	Project Scope		The testing also includes testing to ascertain whether the response time, the bandwidth usage & performance of the solution are as per the expectations of BOBCARD and would involve an error free dry run of the customized solution and end-run simulation.	Please provide the details of accepted value of : 1. existing response time 2. bandwidth usage 3. performance	Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
1079	23	5.6-16	Other RFP Requirements		However, the selected Bidder shall install and commission the solution, in terms of this RFP, at locations designated by Company or at such Centers as Company may deem fit and the changes, if any, in the locations will be intimated to the Bidder.	Please provide the details of the designated locations	Datacentre location will be Mumbai/ New Mumbai and Bangalore/Hyderabad.
1080	24	5.6-21	Other RFP Requirements		The Bidder shall ensure that the solution provided and sized by the Bidder is capable of meeting Company's current and terminal year transaction and business volumes.	Please provide the current workload details for correct sizing	This clause stands removed
1081	NA	NA	Annexure-BOM		Core Switch -12 qty and Management Switch- 4 qty.	Please confirm the numbers or it is reverse i.e. Core Switch -12 qty and Management Switch- 4 qty	It is clearly mentioned in BOM
1082	12	3.1-4	Project Scope		The Bidder is required to note the following points: All Software licenses effective date shall be effective as on Go-LIVE sign off or put in use for BOBCARD operations.	Please change it to "All Software licenses effective date shall be effective as on order loading date to OEM"	License effectiveness should be start from the software is ready to use. License cost will not impact to BOBCARD due to implementation delay. No license activate without informing BOBCARD.
1083	13	3.1-8	Project Scope		All required configuration to integrate with existing setup should be taken care of by bidder.	Please share existing solutions which needs to integrate with new setup	This will be market leading product only. Basis on compatibility Bidder has to integrate the existing infra setup with new setup. All the product will be share only with the final bidder
1084		Memory slots- 4	Appendix01 (server Prod & Server UAT Sheet)		64 DDR5 DIMM slots to be provided. Memory to be provided with 4400MT/s or higher modules.	Please Change it " 32 DIMM slots to be provided"	No Change
1085	NA	Software Defined Storage- 1	Appendix01 (virtual platform Sheet)		Maintain primary working set copy of active data on the Local Node as VM's are hosted to provide high IOPS and low latency. Proposed solution must be proposed for faster reads and write for Business-critical Apps.	Please change it to "Proposed solution must be proposed for faster reads and write for Business-critical Apps." only	No Change

1086	NA	Software Defined Storage-7	Appendix01 (virtual platform Sheet)		The proposed solution should support HCI nodes with different models (same OEM) / different CPU & Memory / Disks configurations in the same cluster without any impact on enterprise-class storage services/ functionalities	Change it to "The proposed solution should support HCI nodes with different models	No Change
1087	NA	Software Defined Storage-24	Appendix01 (virtual platform Sheet)		The proposed solution should support 1 min RPO & 1 hour RTO for critical workload in case BOB Cards wants to have this capability replication for Future use. The proposed solution should have native Replication and DR Orchestration from Day-1	Change it to below one option: Option1: The proposed solution should support 1 min RPO & 1 hour RTO for critical workload in case BOB Cards wants to have this capability replication for Future use. Option2: The proposed solution should support 15 min RPO & 1 hour RTO for critical workload in case BOB Cards wants to have this capability replication for Future use. The proposed solution should have native Replication and DR Orchestration from Day-1	This is required for BOBCARD mission critical application. The solution should capable to support 1min RPO. The propose replication solution should be same OEM as the virtualization solution to provide seamless integration.
1088	NA	15	Appendix 02-Perimeter Firewall		Solution should have minimum 450 GB SSD pair, system storage	Please change to "Solution should have minimum 450 GB SSD , system storage"	No Change
1089		5/C.Solution Capabilites	General		The solution must support and integrate the web application vulnurability tools (Web application scanners) being proposed by bidder as part of this RFP at minimum to virtually patch web application vulnurabilies or else solution should have ready plug-ins to integrate banks VAPT tool.	Suggestion: Solution should be capable to protect against zero-day vulnerability using positive security model without being dependent on virtual patching. Virtual patch can even lead to false positive. Hence, requesting you to modify the clause as below: The solution must support and integrate the web application vulnurability tools (Web application scanners) being proposed by bidder as part of this RFP, solution should have ready plug-ins to integrate banks VAPT tool.	No Change
1090		2/B.Hardware & Interfaces requirement	General		Appliance/Chassis based Hardware should support scalability with license upgrade. -18 vCPU from day 1 | Scalable to 32 vCPU -128 GB DDR RAM from day 1 -1 TB X 1 SSD M.2 SSD (in Raid) from Day 1	The clause represents single OEM offering for sizing	WAF/LB: This the requirement in view of future growth of organization

1091		7/B.Hardware & Interfaces requirement	General		The proposed appliance shoulde provide minimum 1.2 Gbps of real world WAF throughput from day 1 and should be scalable to 2.2 Gbps with license upgrade on the same hardware or additional blades in case of a chassis based solution. The WAF throughput mentioned should be inclusive after enabling the below mentioned features: With all WAF functions enabled per intance in blocking mode SSL inspection.	The clause represents single OEM offering for sizing	No Change
1092		8/B.Hardware & Interfaces requirement	General		The appliance should support the layer 7 throughput should be at least 58 Gbps scalable to 92 Gbps on same hardware with license upgrade. (Data rerernces for above should be verified from publicly available datasheet)	The clause represents single OEM offering for sizing	No Change
1093		9/B.Hardware & Interfaces requirement	General		The proposed appliance must have minimum hardware compression of 34 Gbps for HTTP traffic form day 1 and scalable upto 48 Gbps with add on license on same hardware. (Data rerernces for above should be verified from publicly available datasheet)	The clause represents single OEM offering for sizing	No Change
1094		10/B.Hardware & Interfaces requirement	General		The proposed appliance should support minimum hardware based SSL offloading from day 1 up to : 34 Gbps Scalable upto 48 Gbps on same hardware with license upgrade. (The SSL encryption & decryption process must be hardware-based proccessor for acceleration) (Data rerernces for above should be verified from publicly available datasheet)	The clause represents single OEM offering for sizing	WAF/LB: This the requirement in view of future growth of organization
1095		11/B.Hardware & Interfaces requirement	General		The solution must support minimum SSL TPS/CPS: -29 K ECDSA P-256-bit keys from day 1 -58 K RSA 2048-bit keys from day 1 scalable to minimum SSL TPS/CPS -68 K ECDSA P-256-bit keys -98 K of RSA 2048-bit Keys (Data rerernces for above should be verified from publicly available datasheet with SSL)	The clause represents single OEM offering for sizing	WAF/LB: This the requirement in view of future growth of organization
1096		12/B.Hardware & Interfaces requirement	General		The proposed appliance should support minimum 74 million L4 concurrent connections from day one and scalable upto 99 Million on same hardware with license upgrade.	The clause represents single OEM offering for sizing	WAF/LB: This the requirement in view of future growth of organization
1097		13/B.Hardware & Interfaces requirement	General		The proposed appliance should support minimum 2.4 million L7 requests per seconds from day 1 and scalable upto 4.2 Million on same hardware with with license upgrade.	The clause represents single OEM offering for sizing	WAF/LB: This the requirement in view of future growth of organization
1098		13	General		The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide traffic performance statistics for last 30 days including Active Connections, Active Sessions, CPU Usage By Core, HTTP Requests, Memory Used, RAM Cache Utilization, Rewrite Transaction, Data Rewrite Transactions, SSL Transactions, Throughput(bits), Throughput(packets), & Total New Connections	The clause represents single OEM offering. The clause should mention the functionality should be achieved without being dependent on tools.	No Change

1099		14	General		The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide a security event timeline dashboard where critical events like Audit logs, Pool status change, Failover status change, DOS attacks etc. must be shown for ease of troubleshooting with last 20 Failed logins details	The clause represents single OEM offering. The clause should mention the functionality should be achieved without being dependent on tools.	No Change
1100		15	General		The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide a Bug tracker option, where an admin can login and find any bugs affecting the devices	The clause represents single OEM offering. The clause should mention the functionality should be achieved without being dependent on tools.	No Change
1101		16	General		The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide an upgrade Options suggestions for next hotfix and stability release for ease of day-2 operations with single click access to release notes a nd EOS dates	The clause represents single OEM offering. The clause should mention the functionality should be achieved without being dependent on tools.	No Change
1102		17	General		The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide an ability to execute CLI commands which are essential for diagnostics which will show historic data or data at the time of file captured. E.g show history of all executed commands on the CLI	Suggestion: Database Load Balancer is provided as inbuilt feature from database solution provider and hence not needed from SLB solution Hence requesting you to remove this point	No Change
1103		23/C.Solution Capabilites	General		Solution should have the capability to highlight (In red / any color code) only malicious payload from the entire attack payload on the event analysis dashboard for detailed fornsics analysis. This is extermly critical when our incident response teams are in combat with the attackers during wartime. This feature/functionality has to be live demonstrated by the bidder after the prebid query meeting, by setting up a lab in the cloud/on-premises	Suggestion: Forensics are not required for LB or WAF kind of solution. This is required for DDoS kind of solution and it is not recommended to have DDoS solution within WAF+LB as DDoS should be a stateless technology and it's placement should be at perimeter level above firewall to protect complete infrastruture	No Change
1104		36/C.Solution Capabilites	General		The Proposed WAF Solution should provide built-in L7 layer DDoS detection and mitigation features based on machine learning and behavioral analytics and dynamic signatures. It should have CAPTCHA support or other mechanism to avoid distributed attack. This feature/functionality has to be live demonstrated by the bidder after the prebid query meeting, by setting up a lab in the cloud/on-premises	Suggestion: DDoS should be a stateless device and it's placement should be at perimeter level above firewall. This ensures protection to network from any advanced DDoS attacks. Hence, it should not be expected to be part of other security solutions within the network.	No Change

1105		58/C.Solution Capabilites	General		The Solution should have IPSEC tunneling capabiltiies	VPN is recommended to be a dedicated solution since it relies on TLS protocol. It is also recommended to terminate the traffic on Firewall or before Firewall as it will check for security parameters on the same. If this is done on ADC, there won't be any security check and can possess threat or security flaw. Hence requesting you to remove this point	No Change
1106		59/C.Solution Capabilites	General		The proposed solution should support a comprehensive list of ways in which LB can monitor the backend services including Daimeter, DNS, FTP, Gateway ICMP, HTTP, HTTPS, TCP half open, TCP , LDAP, MSSQL, MYSQL, MQTT , POSTGRESQL, POP3 , IMAP, NNTP, Radius , SIP and custom external scripts	Suggestion: SIP, Diameter & MQTT Traffic are used in Service Provider environment and are not relevant and used in any Enterprise environment like BOB Cards. Hence requesting you to modify this point accordingly.	No Change
1107		61/C.Solution Capabilites	General		The proposed solution should support various types of LB config for handling traffic, including standard reverse proxy, forwarding in L2 , Forwarding in IP, High performance mode, Stateless mode , Reject mode, DHCP relay, and Message routing for SIP, Daimeter and MQTT traffic	Suggestion: SIP, Diameter & MQTT Traffic are used in Service Provider environment and are not relevant and used in any Enterprise environment like BOB Cards. Hence requesting you to modify this point accordingly.	No Change
1108		70/C.Solution Capabilites	General		The proposed solution should support native integration with kubernetes based platforms hosting microservices e.g. Openshift, TKG cluster etc. Solution should update the configuration of LB automatically by observing events within kubernetes clusters form day 1 without add on license.	Suggestion: Solution should be able to support by means of same solution.	No Change
1109		81/C.Solution Capabilites	General		The proposed LB solution should also support secure remote access to admin users (concurrency of not more than 10); where the solution can do endpoint checks for the admins and establist a secure tunnel with autentication against AD/OAUTH/Radius and MFA via Google authenticator. The system should allow per user basis a login schedule ?(e.g night shift employee cannot login during working hours)	The clause represents single OEM offering.	No Change

1110		2/D. Availability	General		The solution should support SQL-based querying for the following databases for the health checks: for Oracle, MSSQL, MySQL, PostgresSQL and other databases if required in future.	Suggestion: Database Load Balancer is provided as inbuilt feature from database solution provider nd this is proprietary load balancing feature of Database solution provider and hence not needed from ADC solution. Hence requesting you to remove this point.	This will consider as good to have
1111	11	3.1 Project Scope Point #1	The supplied Hardware and Software shall be of the latest versions and should not be end of life / end of support for the next 7 years.		Request the start Date for 7 Yrs mention in the clause be specified. Is it RFP Date or Date of PO Issuance/GoLive Date or something else?	Right tenure will help align the final BOM and any discrepent inpurs will impact pricing , so requesting clarification	The supplied Hardware and Software shall be of the latest versions and should not be end of life / end of support for the next 5 years from the date of delivery
1112	12	3.1 Project Scope Point #4	All Software licenses effective date shall be effective as on Go-LIVE sign off or put in use for BOBCARD operations.		Contract Start period is mentioned as PO Issuance while the SW licenses effective date is mentioed as GoLive Sign off Dates as noticed. Request Bank to keep this synchronized if this is genuine or clarify the intent	Right tenure will help align the final BOM and any discrepent inpurs will impact pricing , so requesting clarification	License effectiveness should be start from the software is ready to use. License cost will not impact to BOBCARD due to implementation delay. No license activate without informing BOBCARD.
1113	12	3.1 Project Scope Point #12	Hardware RMA (Return Merchandise Authorization) should be within 24 hours		Request this be modified as below Hardware RMA (Return Merchandise Authorization) should be within 24 hours on Next business Day Basis.	RMA for a request raised on Friday may be honored by Monday due to the wekend in between , so requesting to keep this clearly specified.	Hardware RMA (Return Merchandise Authorization) should be within 24 hours on Next business Day Basis.
1114	19	5.3 Price Comparisons Point #c iv	End of Sales/ End of support: The Vendor has to ensure that any application, related software supplied / put to use as part of this RFP should not have reached end of support. In the event if any equipment supplied / put to use by the vendor reaches end of support, within the contract period from the date of use, the vendor has to replace the equipment/ software at no additional cost to the Company before end of support.		End of Life/End of Sale Clause here should specifiy the start date as to if PO issuance, RFP Date or any other . Further the tenure within which EOS/EOL should not happen must be mentioned like 7 years in clause Project Scope point #1	Right tenure will help align the final BOM and any discrepent inpurs will impact pricing , so requesting clarification	The supplied Hardware and Software shall be of the latest versions and should not be end of life / end of support for the next 5 years from the date of delivery
1115	9	2.2 Tenure	The tenure of the contract initially would be for 1 year from the date of the issuance of first purchase order. BOBCARD can further extend to 2 years at its at mutually agreed terms.		Contract Tenure mentioend as 1 Year from PO Issuance here while its 3 years in clause 3.1 Point 17/ Pls clarify the right tenure?	Right tenure will help align the final BOM and any discrepent inpurs will impact pricing , so requesting clarification	Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live

1116	13	3.1 Project Scope Point #17	The initial term of this contract shall be 3 years and may be extended to another 2 years subject to satisfactory performance by successful bidder and OEM(s).		Mentioned here is 3 years of initial contract and in 2.2 section the contract mentioned is 1 Year/ pls clarify the right tenure	Right tenure will help align the final BOM and any discrepent inpurs will impact pricing , so requesting clarification	Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
1117	30	7.2 Evaluation Methodology for Eligible Bidder Commercial Bid Evaluation	The key considerations of the TCO would be the total payouts for entire project through the contract period of 5 years.		Mentioned here is 5 years contract but in 2.2 the tenure of contrat is 1 Year, pls clarify the number to consider	Right tenure will help align the final BOM and any discrepent inpurs will impact pricing , so requesting clarification	Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
1118	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Server Prod > HCI Rack Servers > 1	Total QTY is 14		Clarifictaion Needed: 1. Please provide split of quantity of servers / Nodes per location. 2. Kindly specify the number of clusters and nodes per cluster also.	clarifiction will help arrive at the boq rightly	This will be shared with only elected bidder
1119	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Server Prod > HCI Rack Servers > 7	Each Rack Server Controller Cards / Controller Drive should be provided in HA mode in RAID -1.		Request Change: Each HCI Server should be configured with two BOOT drives with hardware RAID Controller. For NVMe storage drives: Provides as per Certifed HCI Node with NVMe configuration	From the HCI Rack server or Pre configured HCI NODE - RAID Controller card is not required for NVMe drives. Also, is this ask for Boot drive with RAID Controller?	Yes, we need boot drive for HCI hypervisor provided in HA mode in RAID -1
1120	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Server UAT > HCI Rack Servers > 7	Each Rack Server Controller Cards / Controller Drive should be provided in HA mode in RAID -1.		Request Change: Each HCI Server should be configured with two BOOT drives with hardware RAID Controller. For NVMe storage drives: Provides as per Certifed HCI Node with NVMe configuration	From the HCI Rack server or Pre configured HCI NODE - RAID Controller card is not required for NVMe drives. Also, is this ask for Boot drive with RAID Controller?	Yes, we need boot drive for HCI hypervisor provided in HA mode in RAID -1
1121	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Server Prod > HCI Rack Servers > 6	Each Rack servers should have minimum usable Storage Capacity of 10 TB of all caching SSD and other HDD. 20% disk slot on each node should be free for future expansion		Clarification needed: In virtualized environment, the storage (usable) capacity is calcluated across the cluster. Need clarification on the total capacity required across the number of nodes in a cluster.	clarifiction will help arrive at the boq rightly	as mentioned in RFP 10TB usable storage per node * no of node = total usable capacity
1122	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Server UAT > HCI Rack Servers > 6	Each Rack servers should have minimum usable Storage Capacity of 10 TB of all caching SSD and other HDD. 20% disk slot on each node should be free for future expansion		Clarification needed: In virtualized environment, the storage (usable) capacity is calcluated across the cluster. Need clarification on the total capacity required across the number of nodes in a cluster.	clarifiction will help arrive at the boq rightly	as mentioned in RFP 10TB usable storage per node * no of node = total usable capacity
1123	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Server Prod > HCI Rack Servers > 13 >Server Security	Request New Point to be added		Request to add the below point for security and management features for HCI Nodes Day2 operations and management of HCI Nodes for updates on Hardware and Software. HCI Node management tool should integrate with Virtual platform and Network switches. Should be able to do Firmware updates, Manage Cluster and deployment, Full stack visibility of HCI Node, TAC/Case Support, Continuous Health checks on Networking, Server, VMs , Anomalies detection, Security advisories, patch management etc.	HCI Node should integrate with Virtual platform and Network switches, Should have management software for a Firmware update, Manage Cluster and deployment, Full stack visibility HCI Node, TAC/Case Support, Continuous Health checks on Networking, Server, VMs , Anomalies detection, Security advisories, patch management,	No Change, additional feature will be consider as value add

1124	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Server UAT > HCI Rack Servers > 13> Server Security	Request New Point to be added		Request to add the below point for security and management features for HCI Nodes Day2 operations and management of HCI Nodes for updates on Hardware and Software. HCI Node management tool should integrate with Virtual platform and Network switches. Should be able to do Firmware updates, Manage Cluster and deployment, Full stack visibility of HCI Node, TAC/Case Support, Continuous Health checks on Networking, Server, VMs , Anomalies detection, Security advisories, patch management etc.	HCI Node should integrate with Virtual platform and Network switches, Should have management software for a Firmware update, Manage Cluster and deployment, Full stack visibility HCI Node, TAC/Case Support, Continuous Health checks on Networking, Server, VMs , Anomalies detection, Security advisories, patch management,	No Change, additional feature will be consider as value add
1125	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Microsegmentation > 1	The Solution should be capable of supporting major hardware OEMs like Juniper, Arista, Cisco, HPE and Dell. The proposed solution should be a purely software-based solution and should not be dependent on any hardware make and model.		Request below modified clause be considered: The Solution should be capable of supporting major hardware OEMs like Juniper, Arista, Cisco, HPE and Dell. The proposed solution should be a purely software-based solution and should not be dependent on any hardware make and model by creating overlay tunnels between the hosts.	The key benefits of no dependecy on hardware is by using software defined networking i.e overlay. Overlay is mandatory for network & Security automation as part of software defined data center.	No Change
1126	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Microsegmentation > 2	The solution should provide a distributed firewall such that the firewalling for Virtual Machines can be provided closest to the application within the server itself without traffic going to a Physical Firewall.		Request below modified clause be considered which includes additonal points The solution should provide a distributed firewall such that the application aware and identity based statefull firewalling for Virtual Machines can be provided closest to the application within the server itself without traffic going to a Physical Firewall or regardless of underlying L2 Netwrork topology. The solution should also provide an integrated networking solution (CNI implementations) as well as provide advance turnkey container networking & firewalling services. Solution should support for container networking plug-ins, support for pod to pod communication and support for ingress controllers. The micro-segmentation solution should have a capability for stateful firewalling and ALGs (Application Level Gateway) on a per-workload granularity regardless of the underlying L2 network topology (i.e. possible on either logical network overlays or underlying VLANs), embedded in the hypervisor kernel, distributed	*As per security framework its recommended not to use standard ports for your applications and hence to have effective security on per VM basis an application/L7 firewalling is must.* Containers & Kubernetes are now part of all modern applications hence networing and security for container shall also be considered for end to end application security. there is App ID requirement is mentioned in RFP as part of "Internal Firewall" spec point # 23 hence same should be considered for mirosegmenation as well otherwise it will create non standard architecture.	No Change

1127	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Microsegmenation >5	The proposed solution should provide the ability to define firewall rules at VM level for east-west traffic in order to implement Zero Trust Security		Request below modified clause be considered: The proposed solution should provide the ability to define Layer 7 application firewall rules at VM level for east-west traffic in order to implement Zero Trust Security alongwith URL Filtering and TLS inspection for encrypted traffic	Zero trust Security framework mandates TLS inspection for encrypted traffic, URL Filtering and Layer 7 application firewalling.	No Change, additional feature will be consider as value add
1128	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Microsegmenation >4	The Proposed Solution including Hypervisor, SDS and Micro segmentation must be from the same OEM.		Request below modified clause be consideredL The Proposed Solution including Hypervisor, SDS, SDN and Micro segmentation must be from the same OEM.	SDN is missing in the spec, SDN will be mandatory to create complete automated Software Defined data center by creating an abstraction of the network enabling programming of network behavior in a centrally controlled manner through software applications.	No Change, SDN will be consider as value add
1129	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Microsegmenation >6	The proposed solution should allow users to define granular firewall rules based on IP Addresses, Tags/Categories and Subnets to segment User Applications		Request below modified clause be considered which includes additonal points The proposed solution should allow users to define granular firewall rules for both VM and conatiners based on IP Addresses, VM Names, Tags/Categories and Subnets to segment User Applications by creating dynamic security groups. The solution should have capability to provide stateful micro-segmentation for virtual machines and Kubernetes workloads from a single console. The solution should also support enforcement of stateful distributed firewall for IPv6 VM workloads. These firewall rules can use IPv6 addresses, IPv6 CIDR, IP Sets that include both IPv4 and IPv6 addresses and security groups that can include logical ports that have both IPv4 and IPv6 addresses. IPv6 capability should be available both at management and data plane	Its necessary to have dynamic security group capability to ensure complete automation. Mentioned in the RFP page 8 -> 2.0 --> Requirement Summary--> 2.1 Intent--> mentions requirement for IPv6 "The proposed solution should support both IPv4 and IPv6."	No Change
1130	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Microsegmenation >7	Solution should provide capability to create network segments by defining them entirely in software and avoid the need to re-architect your network or deploy physical appliances		Request below modified clause be accmodated: Solution should provide capability to create network segments and L2 Streching between DC and DR by defining them entirely in software and avoid the need to re-architect your network or deploy physical appliances	L2 Streching is required for better application availability considering RFP asks for 99.99 % availability on monthly basis. RFP Page 17 -> "4. Service Levels "-->"SLA: The solution is expected to be available for 99.99% on 24x7 and up time availability will be calculated on monthly basis."	No Change, L2 stretching implementation will be discuss with elected bidder.

1131	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Container >2	The solution must be able to manage Kubernetes clusters. Licenses for managing Kubernetes clusters should be implemented from Day-1		Request below modified clause be accmodated: The solution must be able to manage Kubernetes clusters. Licenses for managing Kubernetes clusters along with components such as backup, container registry and monitoring alongwith Windows Container support should be implemented from Day-1	Kubernetes Cluster doesn't work in isloation but require other components such as container registry and backup solution. If not included than Bob Card will have procure them separately. And Not aving Windows Container support will block any windows based apps to be deployed on Kubernetes Platform.	Yes, BOBCARD will take care such requirement
1132	NA	Appendix02 Techno Functional Requirements- Network components > internal FW NG Firewall Features NEW POINT	Must have provisioning, operations and lifecycle management of Kubernetes, automated deployment, scaling, and operation of Kubernetes clusters		Request below modified clause be accmodated: Must have provisioning, operations and lifecycle management of Kubernetes, automated deployment, Auto scaling & Auto Healing, and operation of Kubernetes clusters	Complete Automation is not possible without Auto Scaling and Auto Healing of Kubernetes Clusters. One has to manually add nodes in case of failure or unprovisioned increase in load.	No Change
1133	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Container >4	Container Platform should provide single pane of Glass for Lifecycle Management of all K8S clusters deployed on prem.		Request below modified clause be accmodated: Container Platform should provide single pane of Glass for Lifecycle Management of all K8S clusters alongwith ingress, backup and container registry deployed on prem.	Kubernetes Cluster doesn't work in isloation but require other components such as container registry and backup solution. These shall too be considered for life cycle management	Yes, BOBCARD will take care such requirement
1134	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management >1	The solution should provide capability of generating reports for usage, performance, compliance, health, forecasting and capacity.		Request below modified clause be accmodated: The solution should provide capability of generating reports for health, Capacity Optmization - Right Sizing (Under sized, Oversized), Reclamation (Idle, Powered off , Snapshot, Orphaned Disk , Forecasting - Capacity Forecasting, Migration assessment, Migration Planning Usage - Process and service utlization Compliance - Regulatory Benchmark (PCIDSS and ISO) Security Guidelines for Infrastructure and Cloud Management	Bob Cards will need capacity optimization capabilities to identify over-provisioned & under-provisioned resources and provide recommendations, alerts and automated actions on right-sizing and resource consumption so they can be right-sized for adequate performance and avoid resource wastage. Should provide visibility of capacity and VMs which can be reclaimed and cost visibility of the reclaimed capacity and VMs.	No Change, additional feature will be consider as value add

1135	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform >Cloud Management >11	The solution should have intelligent operations with anomaly detection which will allow monitoring seasonal trends and automatically send email alert		The solution should have AI/ML driven intelligent operations & troubleshooting workbench with anomaly detection,third party infra (Server, Storage , Network, database and Application) along with parent child relatiohship mapping, service and process monitoring which will allow monitoring seasonal trends and automatically send email alert. The solution should also have log management capability for infrastructure and applications . log management solution should delivers intuitive, actionable dashboards, sophisticated analytics, and broad third-party extensibility across physical, virtual, and cloud environments.	BoB Cards will not be able to manage the infrastructure without comprhesive log management capability. Its also mandatory for from regulation/compliance perspective to have log stored for given period of time for audit. BoB Card would need apps (database and Application) to infra (Server, Storage , Network) level visibility for toubleshooting and performance monitoring.	No Change, additional feature will be consider as value add
1136	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform >Cloud Management >7	The solution must have an approval process to review, reject or approve the deployment requests from the marketplace.		Request below modified clause be considered: The Solution must support multiple levels of approval with E-mail notifications with ability to automate manual provisioning and de-provisioning of the tasks and policies embedded in each layer of their application including auto - approve and auto-reject capability based on application criticality	The solution must have an approval process to review, multi level & auto reject or approve the deployment requests from the marketplace.	No Change, additional feature will be consider as value add
1137	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform >Hypervisor > 6	Hypervisor should support container and opensource integration for cloud native application from day-1. Must be a Kubernetes ready from day-1.		Request below modified clause be accmodated: Hypervisor should support container both Linux and Windows along with other kubernetes ecosystems such as container registry, backup, ingress & monitoring and opensource integration for cloud native application from day-1. Must be a Kubernetes ready from day-1.	Kubernetes does't work in isolation and requires multiple components for production setup.	Yes, BOBCARD will take care such requirement
1138	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform >Hypervisor > 16	Virtualization Manager should provide feature which can perform quick, as-needed deployment of additional virtualized hosts. When the service is running, it can push out update images, eliminating patching and update without impacting production.		Please clarify the scenario and expected outcome out of the below point in this clause: "When the service is running, it can push out update images, eliminating patching and update without impacting production."		Virtualization manager should allow addition of new nodes and patching/upgrade of hypervisor running on the node without any VM downtime.
1139	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform >Hypervisor > 22	Unlimited VM replication from DC to DR (No restriction on VM replication and DR orchestration) with the capability to define Recovery Plans		Request to provide the number of VMs to be orchestrated for automated recovery and not keep open as unlimited since this approach is OEM specific . The VMs to be protected/orchestrated are limited to what can be provisioned on these 14 servers of production. Furehr pls clarify the need for Recovery Plans		No Change, can not predict the exact number of VMs for next 5 Years which need to be replicated.

1140	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Hypervisor > 23	Proposed solution should have a self-service restore feature on a per-VM basis to allow trusted application administrators to recover their own files with the ability to mount snapshots as a drive in Windows VMs		Request this be modified as below or clarify the requriement: Proposed solution should have a self-service restore feature on a per-VM basis to allow trusted application administrators to recover their own VMs from the snapshot	Please clarify this requirement, this looks like back and restore requirements so the modified clause	This will help BOBCARD to recover file without losing current state of virtual machine.
1141	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Hypervisor > 24	Hypervisor should provide Visibility for Running VM and their connectivity co-relationship with Network Ports on attached Physical TOR / Core Direct which Include Network RX/TX Bytes.		Request below modified clause with additional inputs be considered : Hypervisor should provide Visibility for Running VM and their connectivity co-relationship with Network Ports on attached Physical TOR / Core Direct which Include Network RX/TX Bytes.Solution Should provide end to end visibility across physical firewall, switch and storage, Flow Analysis and Security Planning,Guided Troubleshooting, Microsegmentation planning, RCA (Connectivity Problem, Packet Loss, N/W latency), Application Discovery, Service Monitoring , Application Dependency Mapping and monitoring of non compliant ports	Monitoring is not considering all components of the stack. Unless end to end visibility is provided as part of this solution BoB Card has to spend separately on monitoring.	Yes, BOBCARD will take care such requirement. However Hypervisor should provide Visibility for Running VM and their connectivity co-relationship with Network Ports on attached Physical Port which Include Network RX/TX Bytes.
1142	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Hypervisor > 30	Virtualization software or the solution should provide Cluster level encryption protects unauthorized data access at-rest.		Request below modified clause be considered : Virtualization software or the solution should provide Cluster level, VM Level encryption protects unauthorized data access at-rest and in transit.	Having capability to do the enscryption at app VM level and in transit is required to complete solution.	No Change, additional feature will be consider as value add
1143	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Software Defined Storage > 1	Maintain primary working set copy of active data on the Local Node as VM's are hosted to provide high IOPS and low latency. Proposed solution must be proposed for faster reads and write for Business-critical Apps.		Request below additional point be added in theis clause : Proposed solution must be proposed for faster reads and write for Business-critical Apps.	Architecture is specific to one vendor, request BoB Cards to consider on outcome than specific architecture. There is no specific latency requirements mentioned in the spec.	No Change.
1144	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Software Defined Storage >2	The solution must have De-duplication and Compression features licensed and implemented from day one (Should not have dependency on any proprietary hardware device).		Request below modified clause be considered: The solution must have De-duplication/Compression features licensed and implemented from day one (Should not have dependency on any proprietary hardware device).	Solution should have flexibility to implement either compression and de-duplication. BoB Cards should conisder overhead while deciding on both.	No Change
1145	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Software Defined Storage >24	The proposed solution should support 1 min RPO & 1 hour RTO for critical workload in case BOB Cards wants to have this capability replication for Future use. The proposed solution should have native Replication and DR Orchestration from Day-1		What is the use case for 1 min RPO and 1 Hour RTO? is this linked with some regulatory requirement?	Replication is best handled at application level as having additional solution for infrastructure will complexity and cost for BoB Cards Its best to use extends the existing DR orchestration solution for this environment as well.	This is required for BOBCARD mission critical application. The solution should capable to support 1min RPO. The propose replication solution should be same OEM as the virtualization solution to provide seamless integration.

1146	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Software Defined Storage >25	The solution provided should function even after one node failure.		Request below modified clause be considered: The solution provided should function even after two node failure.	RFP asks for 99.99 % availability SLA for the proposed solution. It will require minimum N+2 configuration for required resiliency and uptime.	No Change, additional feature will be consider as value add
1147	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Software Defined Storage >31	The solution should provide enterprise data services such as compression completely in software. Software Defined Storage solution must have de-duplication and compression features Licensed and implemented from day one. These functionalities should be part of the proposed solution. The solution must have functionality to support compression and or deduplication online on data container without any downtime and data loss as per business requirement.		Request below modified clause be considered: The solution should provide enterprise data services such as compression completely in software. Software Defined Storage solution must have de-duplication or compression features Licensed and implemented from day one. These functionalities should be part of the proposed solution. The solution must have functionality to support compression and or deduplication online on data container without any downtime and data loss as per business requirement.	Solution should have flexibility to implement either compression and de-duplication. BoB Cards should conisder overhead while deciding on both.	No Change
1148	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmentation > new point	Additional Point for consideration		The solution must ensure that there is not alteration in the IP address of the Virtual machine, by blocking the traffic from or to the VM inherited as a feature in the Solution.	IP/MAC spoofing is major security concern for organizations like BoB Cards handing customers data.	No Change, additional feature will be consider as value add
1149	NA				The solution should support multi-tenancy to isolate networking/security for different departments/function within BoB Cards upto a minimum of 4 tenants and 5 VPCs	VPC will enable Bob Cards to create isolation from access, resources, network and security.	ange, additional feature will be consider as valu
1150	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Container > 6	Should support cluster scale out i.e addition of worker nodes as and when required.		Request below modified clause be considered: Should support Automated cluster scale out i.e addition of worker nodes as and when required.	Complete Automation is not possible without Auto Scaling and Auto Healing of Kubernetes Clusters. One has to manually add nodes in case of failure or unprovisioned increase in load.	No Change
1151	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > 3	The solution shall provide a single pane of glass for automated provisioning with model-based orchestration of compute, network and storage through a unified multi-tenant self-service catalog.		Request below modified clause be consiered The solution shall provide a single pane of glass for automated provisioning with model-based orchestration of compute, network, storage and Kubernetes through a unified multi-tenant self-service catalog .	All modern applications are combination of both container and VM form factor.	No Change, additional feature will be consider as value add
1152	NA	Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > 5	The solution must provide a self-service portal to allow user to consume the creation of infrastructure easily.		Request below modified clause be considered: The solution must provide a self-service portal to allow user to consume the creation of infrastructure easily for both VM and Kubernetes	All modern applications are combination of both container and VM form factor.	No Change, additional feature will be consider as value add

1153	NA	Appendix01 Techno Functional Requirements-Server and Virtual platform > Cloud Management > 8	The software must allow the designer to use shell script, PowerShell script to code the automation.		Request below modified clause be considered:

The software must allow the designer to use shell script, PowerShell script, Python and node JS to code the automation. | Python and nodeJs are very popular language for scrpting in terms resource availability and community support | No Change, additional scripting will be value add |
| 1154 | NA | Appendix01 Techno Functional Requirements-Server and Virtual platform > Cloud Management > 9 | The software must allow the designer to design VM blueprints. | | Request below modified clause be considered:

The software must allow the designer to design Multi VM & Kubernetes blueprints. | All modern applications are combination of both container and VM form factor. | No Change, additional feature will be consider as value add |
| 1155 | NA | Appendix01 Techno Functional Requirements-Server and Virtual platform > Cloud Management > 12 | The solution should have simple low-code, no-code automation engine which allows automating day-to-day routine tasks | | Request below modified clause and adidtoinal inpurs on the clause be considered:

The solution should have simple low-code, no-code automation engine which allows automating day-to-day routine tasks such as Snapshot creation, Addition of Disk, Power Cycle (Suspend , Shutdown, Reboot, reset), Resize, Rebuild, Additional of Network, VM Unregister , Delete,connect remote console, Change Security Group with capability to create additional resource actions as out of the box capability. | All modern applications are combination of both container and VM form factor. | No Change, additional feature will be consider as value add |
| 1156 | NA | Appendix01 Techno Functional Requirements-Server and Virtual platform > Cloud Management > New Point | New Point | | Solution should provide capability to define and showcase cost to create cloud like experience to the business unit with the overall cost spend on the infrastructure [server hardware, storage, licenses, application, maintenance, labor, network, facilities , etc. | Bob Cards will need Cost transparency (Showback and Chargeback capability) across private, hybrid to optimize planning and prioritization of VM/Server/Application onboarding/provisioning | No Change, additional feature will be consider as value add |
| 1157 | NA | Appendix02 Techno Functional Requirements-Network components > LB+WAF & IPS | New Point | | We request BoB Card to allow for both software and hardware based solution for Load Balancer, WAF, IPS/IDS. As these components are dynamic as per application consumption requirements and considering bob card is directly managing customer data, its very critcal that these components are added as part of sofwate defined stack. | Modern applications increasingly require software-defined networking (SDN) and security solutions due to their need for greater flexibility, agility, and scalability. Traditional networking and security methods often lack the adaptability to support the dynamic nature of modern application environments, especially in cloud | No Change |
| 1158 | NA | Appendix02 Techno Functional Requirements-Network components > LB+WAF C.Solution Capabilites Pont #5 | The solution must support and integrate the web application vulnurability tools (Web application scanners) being proposed by bidder as part of this RFP at minimum to virtually patch web application vulnurabilies or else solution should have ready plug-ins to integrate banks VAPT tool. | | Requesting you to modify the clause as below:

The solution must support and integrate the web application vulnurability tools (Web application scanners) being proposed by bidder as part of this RFP, solution should have ready plug-ins to integrate banks VAPT tool. | Solution should be capable to protect against zero-day vulnerability using positive security model without being dependent on virtual patching. Virtual patch can even lead to false positive. | No Change |

1159	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #2	Appliance/Chassis based Hardware should support scalability with license upgrade. -18 vCPU from day 1 | Scalable to 32 vCPU -128 GB DDR RAM from day 1 -1 TB X 1 SSD M.2 SSD (in Raid) from Day 1		The clause represents single OEM offering for sizing		No Change
1160	NA	7/B.Hardware & InAppendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #7	The proposed appliance shoulde provide minimum 1.2 Gbps of real world WAF throughput from day 1 and should be scalable to 2.2 Gbps with license upgrade on the same hardware or additional blades in case of a chassis based solution. The WAF throughput mentioned should be inclusive after enabling the below mentioned features: With all WAF functions enabled per intance in blocking mode SSL inspection.		The clause represents single OEM offering for sizing		No Change
1161	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #8	The appliance should support the layer 7 throughput should be at least 58 Gbps scalable to 92 Gbps on same hardware with license upgrade. (Data rerernces for above should be verified from publicly available datasheet)		The clause represents single OEM offering for sizing		No Change
1162	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #9	The proposed appliance must have minimum hardware compression of 34 Gbps for HTTP traffic form day 1 and scalable upto 48 Gbps with add on license on same hardware. (Data rerernces for above should be verified from publicly available datasheet)		The clause represents single OEM offering for sizing		No Change
1163	NA	Appendix02 Techno Functional Requirements- Network components > LB+WAF B.Hardware & Interfaces requirement Point #10	The proposed appliance should support minimum hardware based SSL offloading from day 1 up to : 34 Gbps Scalable upto 48 Gbps on same hardware with license upgrade. (The SSL encryption & decryption process must be hardware-based proccessor for acceleration) (Data rerernces for above should be verified from publicly available datasheet)		The clause represents single OEM offering for sizing		No Change

1164	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF B.Hardware & Interfaces requirement Point #11	The solution must support minimum SSL TPS/CPS: -29 K ECDSA P-256-bit keys from day 1 -58 K RSA 2048-bit keys from day 1 scalable to minimum SSL TPS/CPS -68 K ECDSA P-256-bit keys -98 K of RSA 2048-bit Keys (Data rerernces for above should be verified from publicly available datasheet with SSL)		The clause represents single OEM offering for sizing		No Change
1165	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF B.Hardware & Interfaces requirement Point #12	The proposed appliance should support minimum 74 million L4 concurrent connections from day one and scalable upto 99 Million on same hardware with license upgrade.		The clause represents single OEM offering for sizing		No Change
1166	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF B.Hardware & Interfaces requirement Point #13	The proposed appliance should support minimum 2.4 million L7 requests per seconds from day 1 and scalable upto 4.2 Million on same hardware with with license upgrade.		The clause represents single OEM offering for sizing		No Change
1167	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF General Requirement Point #13	The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide traffic performance statistics for last 30 days including Active Connections, Active Sessions, CPU Usage By Core, HTTP Requests, Memory Used, RAM Cache Utilization, Rewrite Transaction, Data Rewrite Transactions, SSL Transactions, Throughput(bits), Throughput(packets), & Total New Connections		The clause should mention the functionality should be achieved without being dependent on tools.	The clause represents single OEM offering.	No Change
1168	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF B.Hardware & Interfaces requirement Point #14	The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide a security event timeline dashboard where critical events like Audit logs, Pool status change, Failover status change, DOS attacks etc. must be shown for ease of troubleshooting with last 20 Failed logins details		The clause should mention the functionality should be achieved without being dependent on tools.	The clause represents single OEM offering.	No Change
1169	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF B.Hardware & Interfaces requirement Point #15	The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide a Bug tracker option, where an admin can login and find any bugs affecting the devices		The clause should mention the functionality should be achieved without being dependent on tools.	The clause represents single OEM offering.	No Change

1170	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF B.Hardware & Interfaces requirement Point #16	The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide an upgrade Options suggestions for next hotfix and stability release for ease of day-2 operations with single click access to release notes a nd EOS dates		The clause should mention the functionality should be achieved without being dependent on tools.	The clause represents single OEM offering.	No Change
1171	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF B.Hardware & Interfaces requirement Point #17	The HDTS (Health Diagnostic Tool which is delivered as a service) should also provide an ability to execute CLI commands which are essential for diagnostics which will show historic data or data at the time of file captured. E.g show history of all executed commands on the CLI		Request you to remove this clause	Database Load Balancer is provided as inbuilt feature from database solution provider and hence not needed from SLB solution	No Change
1172	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF C.Solution Capabilities Point #23	Solution should have the capability to highlight (In red / any color code) only malicious payload from the entire attack payload on the event analysis dashboard for detailed fornsics analysis. This is extermly critical when our incident response teams are in combat with the attackers during wartime. This feature/functionality has to be live demonstrated by the bidder after the prebid query meeting, by setting up a lab in the cloud/on-premises		Forensics are not required for LB or WAF kind of solution. This is required for DDoS kind of solution and it is not recommended to have DDoS solution within WAF+LB as DDoS should be a stateless technology and it's placement should be at perimeter level above firewall to protect complete infrastruture		No Change
1173	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF C.Solution Capabilities Point #36	The Proposed WAF Solution should provide built-in L7 layer DDoS detection and mitigation features based on machine learning and behavioral analytics and dynamic signatures. It should have CAPTCHA support or other mechanism to avoid distributed attack. This feature/functionality has to be live demonstrated by the bidder after the prebid query meeting, by setting up a lab in the cloud/on-premises		Request to remove this point	DDoS should be a stateless device and it's placement should be at perimeter level above firewall. This ensures protection to network from any advanced DDoS attacks. Hence, it should not be expected to be part of other security solutions within the network.	No Change

1174	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF C.Solution Capabilities Point #58	The Solution should have IPSEC tunneling capabiltiies		Request to remove this point	VPN is recommended to be a dedicated solution since it relies on TLS protocol. It is also recommended to terminate the traffic on Firewall or before Firewall as it will check for security parameters on the same. If this is done on ADC, there won't be any security check and can possess threat or security flaw.	No Change
1175	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF C.Solution Capabilities Point #59	The proposed solution should support a comprehensive list of ways in which LB can monitor the backend services including Daimeter, DNS, FTP, Gateway ICMP, HTTP, HTTPS, TCP half open, TCP , LDAP, MSSQL, MYSQL, MQTT , POSTGRESQL, POP3 , IMAP, NNTP, Radius , SIP and custom external scripts		Request to modify the clause as below: The proposed solution should support a comprehensive list of ways in which LB can monitor the backend services including DNS, FTP, Gateway ICMP, HTTP, HTTPS, TCP half open, TCP , LDAP, MSSQL, MYSQL , POSTGRESQL, POP3 , IMAP, NNTP, Radius and custom external scripts	SIP, Diameter & MQTT Traffic are used in Service Provider environment and are not relevant and used in any Enterprise environment like BOB Cards.	No Change
1176	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF C.Solution Capabilities Point #61	The proposed solution should support various types of LB config for handling traffic, including standard reverse proxy, forwarding in L2 , Forwarding in IP, High performance mode, Stateless mode , Reject mode, DHCP relay, and Message routing for SIP, Daimeter and MQTT traffic		Request this clause be modified as below: The proposed solution should support various types of LB config for handling traffic, including standard reverse proxy, forwarding in L2 , Forwarding in IP, High performance mode, Stateless mode , Reject mode, DHCP relay	SIP, Diameter & MQTT Traffic are used in Service Provider environment and are not relevant and used in any Enterprise environment like BOB Cards.	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.
1177	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF C.Solution Capabilities Point #70	The proposed solution should support native integration with kubernetes based platforms hosting microservices e.g. Openshift, TKG cluster etc. Solution should update the configuration of LB automatically by observing events within kubernetes clusters form day 1 without add on license.		Solution should be able to support by means of same solution.		No Change
1178	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF C.Solution Capabilities Point #81	The proposed LB solution should also support secure remote access to admin users (concurrency of not more than 10); where the solution can do endpoint checks for the admins and establist a secure tunnel with autentication against AD/OAUTH/Radius and MFA via Google authenticator. The system should allow per user basis a login schedule ?(e.g night shift employee cannot login during working hours)		The clause represents single OEM offering.		No Change

1179	NA	Appendix02 Techno Functional Requirements-Network components > LB+WAF D.Availability #2	The solution should support SQL-based querying for the following databases for the health checks: for Oracle, MSSQL, MySQL, PostgresSQL and other databases if required in future.		Request this clause be removed	Database Load Balancer is provided as inbuilt feature from database solution provider and this is proprietary load balancing feature of Database solution provider and hence not needed from ADC solution.	No Change
1180	NA	Appendix02 Techno Functional Requirements-Network components > perimeter FW Specifications Point #7	The Firewall appliance should have certifications like ICSA /EAL4/CCNDPP		Request this be modified as below: The Firewall solution should have certifications like ICSA /EAL4/CCNDPP	Every OEM has its own solution offering and certification ask may align to the approach solution is provided rather than mandating it on the appliance inline to a particular OEM	No Change
1181	NA	Appendix02 Techno Functional Requirements-Network components > perimeter FW Specifications Point #9	OEM/Bidder should provide below transceivers from Day-1. Firewall and SFP should be from same OEM. Below mentioned SFP quantity is required per appliance. 4 X 10GE SR SFP+ 4 X 1G SFP 4 x 25G SFP28		OEM/Bidder should provide below transceivers from Day-1. Firewall and SFP should be from same OEM. Below mentioned SFP quantity is required per appliance. 4 X 1G RJ 45 4 X 10G SFP+ 4 x 25G SFP28	Requesting if 1G can be considered using Copper Links and not SFP	No Change
1182	NA	Appendix02 Techno Functional Requirements-Network components > perimeter FW Specifications Point #15	Solution should have minimum 450 GB SSD pair, system storage		Request to modify this as below Solution should have minimum 900 GB SSD pair, system storage	Perimeter Firewall needs high storage numbers as visible with mid/large scale deployments for storing logs considering 3/6 months retention in case the remote Management device is impacted , so good to ask for more	No Change, additional feature will consider as value add
1183	NA	Appendix02 Techno Functional Requirements-Network components > perimeter FW Specifications Point #16	Solution should have minimum 32 GB		Request clause to be modifiedL Solution should have minimum 128 GB RAM	Perimeter Firewall has to have good RAM and such baselining will help with operations of critical banking infra	No Change, additional feature will consider as value add

1184	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #19	"The proposed firewall must provide minimum 10 Gbps of Threat prevention throughput with Real world traffic. (Throughput must be derived from Appmix traffic and not Video/JPEG based traffic) (enterprise testing condition). The throughput must remain 10 Gbps even after enabling NGFW + IPS/IDS + Antivirus + Anti Spyware + Anti Bot + DoS/DDOS + All signature enabled + Logging enabled + Bidirectional inspection + File Blocking. OEM to provide publicly available The Test methodology and result should be compliant to the benchmark testing methodology for the above parameters provided in the Internet Engineering Task Force (IETF)- 'Benchmarking Methodology for	Request below modified clause be considered , instead of Appmix traffic , real world traffic should be mentioned for deriving throughput "The proposed firewall must provide minimum 10 Gbps of Threat prevention throughput with Real world traffic. (Throughput must be derived from real world traffic and not Video/JPEG based traffic) (enterprise testing condition). The throughput must remain 10 Gbps even after enabling NGFW + IPS/IDS + Antivirus + Anti Spyware + Anti Bot + DoS/DDOS + All signature enabled + Logging enabled + Bidirectional inspection + File Blocking. OEM to provide publicly available The Test methodology and result should be compliant to the benchmark testing methodology for the above parameters provided in the Internet Engineering Task Force (IETF)- 'Benchmarking Methodology for Network Security Device	instead of appmix traffic real world traffic will be rifht measure of throuhgput , so requesting the change	No Change
1185	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #21	NGFW appliance must be capable of handling minimum 2 M concurrent sessions utilizing HTTP transactions with all Security feature Turned ON and not based on UDP / Lab environment / ideal testing environment, this claim has to be supported with declaration of concurrent connections claim from OEM	Request below modified clause to accomodate support for 5M concurrent sessions NGFW appliance must be capable of handling minimum 5 M concurrent sessions utilizing HTTP transactions with all Security feature Turned ON and not based on UDP / Lab environment / ideal testing environment, this claim has to be supported with declaration of concurrent connections claim from OEM	Mid/Large scale deployments need higher concurrent session support and baselining this to 50 Lakh concurrent sessions will be in the interest of the Bank , so the requested change	No Change, additional feature will consider as value add
1186	NA	Appendix02 Techno Functional Requirements- Network components > perimeter FW Specifications Point #49	Solution should support creation of minimum 1 virtual context / instance from Day-1 without any compromise on system performance and network bandwidth.	Solution should support creation of minimum 5 virtual context /instance from Day-1 without any compromise on system performance and network bandwidth.	Support for only 1 Virtual context may not be scalable for the DC design and min support for 5 instances is the need for any DC infra Perimeter Firewall understanding furture state architecure and growing needs.	No Change, additional feature will consider as value add

1187	NA	Appendix02 Techno Functional Requirements-Network components > perimeter FW Specifications Point #54	The proposed NGFW solution architecture should have Control Plane separated from the Data Plane in the Firewall appliance architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup, QoS, NAT etc). Control plane must have dedicated resources such as CPU, RAM etc. This is to ensure Bank always has management access to NGFW irrespective of Firewall load / Traffic Spike / Cyber Attack driving higher CPU utilization. Bank should able to login to the firewall and carry out reporting /		Request below modified clause be considered The proposed NGFW solution architecture should have Control Plane separated from the Data Plane in the Firewall solution architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup, QoS, NAT etc). Control plane must have dedicated resources such as CPU, RAM etc. This is to ensure Bank always has management access to NGFW irrespective of Firewall load / Traffic Spike / Cyber Attack driving higher CPU utilization. Bank should able to login to the firewall and carry out reporting / management / packet capture etc to identify the root cause and accordingly take necessary action to remediate it.	OEMs have different approaches to achieving the use case and instead of the ask on the appliance itself , the Firewall Solution will be a generic term to use in requirements so this suggestion	No Change
1188	NA	Appendix02 Techno Functional Requirements-Network components > perimeter FW Specifications Point #72	IPS should provide detailed information on each protection, including: Vulnerability and threat descriptions, Threat severity, Performance impact, Release date, Industry Reference, Confidence level etc.		Request below changed clause : IPS should provide detailed information on each protection, including: Vulnerability and threat descriptions, Threat severity, Release date, etc	Performance impact, industry reference and confidence level are subject to configuration and infrastructure in the bank.	No Change
1189	NA	Appendix02 Techno Functional Requirements-Network components > perimeter FW Specifications Point #76	Should have more than 60+ predefined Categories based on Urls, Application types, Security Risk level etc. However solution should be able to create custom categories for URL and application.		Request below modified clause with increased number of categories: Should have more than 80+ predefined Categories based on Urls, Application types, Security Risk level etc. However solution should be able to create custom categories for URL and application.	Having more predefined categories support would help bank with improved threat detection and better granular policy control with less manual effort.	No Change, additional feature will consider as value add
1190	NA	Appendix02 Techno Functional Requirements-Network components > perimeter FW Specifications Point #89	Solution should give information related to Performance impact and confidence level of protections while creating profiles.		Request this clause be deleted	performance can be subject to policy configurations and existing infra at bank.	No Change

1191	NA	Appendix02 Techno Functional Requirements-Network components > perimeter FW Specifications Point #114	"Management server should support the following for rule optimization: • Unused Rules Calculation for specific time-period based on Firewall Traffic Logs. • Analysis on Covered/Shadow/Hidden Rules • Analysis on Rules Consolidation (Merging of similar kind of rules) • Analysis on Redundant Rules • Tightening of Overly Permissive Rules (Any-Any) • Analysis on Unattached/Unused Objects to simplify objects management • Analysis on Rule-Reordering to improve the performance of the Firewall • Analysis on Disabled/Expired Rules for enhanced visibility on the Firewall Rules sets"		"Management server should support the following for rule optimization: • Unused Rules Calculation for specific time-period based on Firewall Traffic Logs / HIt count • Analysis on Covered/Shadow/Hidden Rules • Analysis on Redundant Rules • Analysis on Unattached/Unused Objects to simplify objects management • Analysis on Disabled/Expired Rules for enhanced visibility on the Firewall Rules sets"	OEMs could be handling the use case suggested for removal differently or have no dependency on the performance of the Firewall , so requesting these be removed from the ask	No Change
1192	NA	Appendix02 Techno Functional Requirements-Network components > IPS Features Point #15	Should support more than 3000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness		Should support more than 5000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness	Increasing number of signature support is beneficial for the Bank's operations and for Effective Security reasons	No Change
1193	NA	Appendix02 Techno Functional Requirements-Network components > internal FW Point #11	The Firewall solution Should support more than 4000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness and should be able to create 40 or more application categories for operational efficiency. Dedicated IPS solution shall be in corporated by the bidder to achive this scale of IPS AVC signatures in this solution.		Request this clause be modfied as below: The Firewall solution Should support more than 6000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness and should be able to create 40 or more application categories for operational efficiency. Dedicated IPS solution shall be in corporated by the bidder to achive this scale of IPS AVC signatures in this solution.	Increasing number of signature support is Beneficial for the Bank's operations and for Effective Security reasons	No Change, additional feature will consider as value add
1194	NA	Appendix02 Techno Functional Requirements-Network components > internal FW NG Firewall Features NEW POINT	New Point to be added		The solution should provide Change Management capability for the organizations needs to implement more formal processes for configuration changes, including audit tracking and official approval before changes are deployed.	By leveraging these features and integrating with external change management tools, organizations can implement a robust change management process that includes formal approval, audit tracking, and compliance reporting within Cisco FMC.	No Change

1195	NA	Features NEW POINT		The solution should provide traffic hit count, Rule Conflict Detection (Redundant & Shadowed) and policy warning for streamlining firewall policies.	These features are crucial for optimizing firewall policies, ensuring efficient traffic flow, and maintaining security posture.	No Change, additional feature will be consider as value add
1196	NA	Appendix02 Techno Functional Requirements- Network components > internal FW Hardware Architecture Point #3	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 8x64 GB of RAM.	Request below modified clause be considered as correction on the ask which seems typo: 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.		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.
1197	NA	Appendix02 Techno Functional Requirements- Network components > Mngmt Switch 6 Product Support Point #2	The OEM support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support	Request below modified clause be considered The OEM/OEM certified partner support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support	OEM Certified partner has thorough experience of OS version upgrades and maintaining network operations troubleshooting issues and it will be cost effective to include this in the ask	The OEM/OEM certified partner support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support
1198	NA	Appendix02 Techno Functional Requirements- Network components > Mngmt Switch 9 Miscellaneous Points Point #1	Console cable and power cable (As per Indian standards) as per customer requirement to be provided. All Cables shall be factory-terminated.	Since Console Cables are common for all devices per OEM , Request Bank to clarify the count of console cables to be provided , is it one each with each Switch or one per DC and DR Each ?.		No Change
1199	NA	Appendix02 Techno Functional Requirements- Network components > Mngmt Switch 10 Product Support Point #2	The OEM support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support	Request below modified clause be considered The OEM/OEM certified partner support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support	OEM Certified partner has thorough experience of OS version upgrades and maintaining network operations troubleshooting issues and it will be cost effective to include this in the ask	The OEM/OEM certified partner support should include the below (a) Software updates and OS version Upgrades (b)Troubleshooting Issues with 24x7 TAC support
1200	NA	Appendix02 Techno Functional Requirements- Network components > Core Swtich >9 Manageability > Appliance point 9.4	Switch Anomolies related with Advisories , PSIRT and Field Notices	Request this clause be removed from the telemetry asks	This feature is not requireed for the design at the BOB DataCenter and may be removed	No Change
1201	NA	Appendix02 Techno Functional Requirements- Network components > Core Swtich >13 Fabric Management > Appliance point 13.1	Solution must provide Centralized Management Appliance – Single pane of glass for managing, monitoring and provisioning the entire Solution within Data Center & across all Data Centers	Request BOBCards to provide VM compute resources for spinning up the VMs to provide this functionality while we can provide the necessary sw and support.		Requested product functionality should be comply, BOBCards will provide VM compute resources for spinning up the VMs to provide this functionality however bidder should provide the necessary sw and support.
1202	NA	Appendix02 Techno Functional Requirements- Network components > Core Swtich >5 Layer 2 Features > Appliance point 5.11	Switch Hardware should have capability to support BGP EVPN Route Type 1, Type 2, Type 3, Type 4, Route Type 5, Type 6/Type 7/Equivalent routes	Request this point be removed	BOBCards design doesn't have Fabric so this is not applicable	No Change

1203	NA	Appendix02 Techno Functional Requirements- Network components > Core Swtich >13 Fabric Management > Appliance point 13.36	Solution should provides reports using predefined templates, including inventory, use, and health reports.		Request below modified clause be considered: Solution should provides reports including inventory, use, and health reports.		No Change
1204	9, 13	2.2 and 3.1.17	The tenure of the contract initially would be for 1 year from the date of the issuance of first purchase order. BOBCARD can further extend to 2 years at its at mutually agreed terms. The initial term of this contract shall be 3 years and may be extended to another 2 years subject to satisfactory performance by successful bidder and OEM(s).		Clarification required on the exact term of the contract, as template has been shared for 5 years YoY maintenance, whereas in the clause, its specified as 1 year and can be extended to 2 years, and again it has been mentioned that contract is for 3 years and can be extended for another 2 years		Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
1205	10	3.1.1	BOBCARD expressly stipulates that Bidder's selection under this RFP is on the express understanding that this RFP contains only the broad provisions for the entire assignment and that the deliverables and the services in connection therewith are only a part of the assignment. The Bidder shall be required to undertake to perform all such tasks, render requisite services and make available all such resources as may be required for the successful completion of the entire assignment at no additional cost to the BOBCARD notwithstanding what is stated here and what is not stated.			The Bidder will be responsible for providing the services limited to the scope specified in the RFP. Additional services if required(and if not part of the RFP) will attract additional costs	No Change
1206	11	3.1.1	The supplied Hardware and Software shall be of the latest versions and should not be end of life / end of support for the next 7 years. In cases where the offered model is being superseded with new model by OEM due to better technology / specifications etc., the successful bidder is required to offer the new model at no extra cost or charges to the BOBCARD			In case where the offered model is being superseded with new model by OEM due to better technology, additional costs will be charged to BOBCARD if the same is being charged to Bidder by OEM	The supplied Hardware and Software shall be of the latest versions and should not be end of life / end of support for the next 5 years from the date of delivery

1207	10	3.1.2	Any service, which forms a part of facilities management that is not explicitly mentioned in this RFP as excluded would form part of this RFP, and the Bidder is expected to provide the same at no additional costs to the Company			Kindly delete this clause as it is not applicable	No Change
1208	17	5.2.2	The prices and other terms offered by vendors must be firm for an acceptance period of 180 days from the opening of the commercial bid			Validity of the prices can be offered for 90 days, as per the OEM costs validity	No Change
1209	42	9.24	The proposed rate of penalty would be 0.5% of the entire project cost/TCO per week of delay or non-compliance. The maximum amount that may be levied by way of penalty pursuant to clause above shall not exceed 10% of the Total Contract value.			Requesting customer to modify the clause as per below - " The proposed rate of penalty would be 0.5% of the entire project cost/TCO per week of delay or non-compliance. The maximum amount that may be levied by way of penalty pursuant to clause above shall not exceed 5% of the Total Contract value."	The maximum amount that may be levied by way of penalty pursuant to clause above shall not exceed 5% of the Total Contract value. All clauses remain same
1210	31	8	Payment terms : Activity : Supply of Servers & Network Delivery timelines : Within 5-6 weeks Payment terms : 20% of Total Cost of Equipment outlined in BOM			Payment terms to be modified as below : Activity : Supply of Servers & Network Delivery timelines : Within 5-6 weeks Payment terms : 70% of Total Cost of Equipment outlined in BOM	Supply of Servers & Network component as prescribed under hardware requirement Within 6-8 weeks from date of PO. Rest all clause remain same
1211	31	8	Payment terms : Activity : Supply of Software as prescribed under software requirement Delivery timelines : Within 1 week - post confirmation from BOBCARD Payment terms : 20% of Total Cost of Equipment outlined in BOM			Payment terms to be modified as below : Activity : Supply of Software as prescribed under software requirement Delivery timelines : Within 1 week - post confirmation from BOBCARD Payment terms : 70% of Total Cost of Equipment outlined in BOM	Supply of Servers & Network component as prescribed under hardware requirement Within 6-8 weeks from date of PO. Rest all clause remain same

1212	31	8	Payment terms : Activity : Acceptance / Go-live by BOBCARD Delivery timelines : After 30 days of Acceptance / Go-Live Payment terms : Balance 50% of Hardware and software licenses amount and 70% of installation within 45 days from the date of acceptance of Tax Invoice by BOBCARD.			Payment terms to be modified as below : Activity : Acceptance / Go-live by BOBCARD Delivery timelines : After 30 days of Acceptance / Go-Live Payment terms : Balance 30% of Hardware and software licenses amount and 70% of installation within 45 days from the date of acceptance of Tax Invoice by BOBCARD.	Supply of Servers & Network component as prescribed under hardware requirement Within 6-8 weeks from date of PO. Rest all clause remain same
1213	34	9.4	Extension of Contract Post Expiry: The Company desires to appoint the vendor for a total period specified in the RFP, considering the effort and investments required in the arrangement. However, understanding the complexities of the entire arrangement, Company would like to safe guard the interests of all the entities involved in the arrangement. Therefore, the Company would like to have options to revisit the arrangements and terms of contract as well as to re-price the same (rates similar or less than existing arrangement) after the contract expiry, if necessary			This clause needs to agreed mutually by both Bidder and Customer	No Change
1214	NA	NA	NA		Specifications are arrived at by BOBCard, kindly clarify the method for sizing		query is not clear
1215	9	2.2	Tenure		Will monitoring and managed services be in bidder scope?		Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
1216	NA	NA	NA		The asset procured shuld be under BOBcard name / ownership and should it be under capex or opex.		All the asset procured to support and implement this setup should be on BOBCARD name and owned by BOBCARD. This will be in Capex as cost as asked in BOM
1217	NA	NA	NA		What is the existing virtualization platform used? Is the application test on all major virtualization platforms?		This is not relevant query
1218	NA	NA	NA		The optional licenses in Bill of Material specifies quantity of licenses but does not match with the number of servers requested, kindly clarify on whether these licenses are required for the HCI platform only. Windows licenses are based on number of cores and not number of servers, kindly clarify on total number of core based and server based licenses for Windows and Redhat.		As mentioned in this corrigendum

1219					Kindly clarify on MS SQL and MySQL Db Editions. MySQL licenses are required for how many sockets/servers?		As mentioned in this corrigendum
1220	NA	NA	In appendix 03 - BoQ sheet		license qty mentinoed for windows and linux - is it for qty of servers or licenses ??		quantity of servers
1221	10	3.1	Project Scope		should TC propose underlay circuits as well along with routers & switches. As per RFP description, it seems ask for DAY0, DAY1 & DAY2 use case.		query is not clear
1222	NA	NA	Appendix 02 (Mgmt Switch)		Exact use case for management switches & topology considered for required routers & switches		Management switch will be use only to connect management port of devices
1223	NA	NA	Techno Functional Requirements (router)		Please clarify on day 1 itself about number of additional interfaces & exact types of interfaces.		It is clearly mentioned in appendix 2 router specification
1224	NA	NA	Techno Functional Requirements (WAN switch)		To understand functionality section more better, need to understand exact topology & traffic flow expected by BOBCARD from DAY1 itself.		This will be share only with elected bidder
1225	NA	NA	Techno Functional Requirements (core switch)		To gain more clarity from feature requirment (L2 & L3, both) standpoint, need to understand exact use case or traffic flow by BOBCARD.		This will be share only with elected bidder
1226	12	12	The resolution time for the hardware/software related issues should be 4 hours, there should be 24*7*365 support from the OEM for all the supplied products through this RFP.		BoBCARD should allow for bidder can leverage partner ecosystem to ensure SLA to comply for ADHOC or On call requirements	The resolution time for the hardware/software related issues should be 4 hours, there should be 24*7*365 support from the OEM for all the supplied products through this RFP. Bidder can leverage partner ecosystem	No Change.
1227	12	7	The successful bidder should also integrate existing infrastructure setup (like existing LAN, proxy, MFA, SIEM) with the new devices to be supplied.		Provided infrastructure needs to integrate with existing BoB card SIEM ? If existing SIEM kindly share the platform name Or shall we provide SIEM service as part of proposal.		This will be market leading product only. Basis on compatibility Bidder has to integrate the existing infra setup with new setup. All the product will be share only with the final bidder
1228	1	1	Appendix02 Techno Functional Requirements- Network components		What will be the required throughput for WAF & LB		IT is mentioned in Technical spec. Appendix 2
1229	5	5	Appendix02 Techno Functional Requirements- Network components		Will it be ok to IPS and Firewall devices from same OEM or should be from saperate OEM		IT should be from different OEM
1230	4	4	Appendix02 Techno Functional Requirements- Network components		What will be the required throughput for Firewall ? & IPS or Consolidated ?		IPS will be separate appliance
1231	1	1	Appendix02 Techno Functional Requirements- Network components		Is API security required as part of WAF ?		Yes
1232	1	1	Appendix02 Techno Functional Requirements- Network components		Any Firewall modules required apart from Firewall and IPS ? e.g. Application filtering or ATP ?		Yes, required application filtering and ATP
1233	1	1	Appendix02 Techno Functional Requirements- Network components		How many IPsec Tunnels & SSL VPN users needs to be configured as part of implementation ? if required ?		This will be share with final bidder

1234	Internal Firewall Section 1 - NG Firewall	8	Should have the capability of passively gathering information about virtual machine traffic, network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance.		Host information like IP address, OS, MAC etc can be detected by Firewall Also, applications being access by host will be visible in Web filter logs. However, Open ports and vulnerabilities are usually inspected by 3rd party assessment tools and not by Firewall. Firewall can inspect traffic and detect if vulnerabilities are getting exploited by applying IPS signatures, Web filters and find exploitation attempts like C&C connections etc.	Hence request you to modify this clause as following Should have the capability of passively gathering information about virtual machine traffic / network hosts and their activities, such as operating system, services & ports being accessed, applications being accessed to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance.
1235	Internal Firewall Section 6 - Performance & Scalability	1	Shall support minimum 5 Gbps of NGFW throughput (Firewall + Application Visibility Control)		As there are IPS and malware inspection features also asked in the RFP specs, throughput requirement should be considered along with IPS, App control and AV, Malware inspection services, hence request you to modify this clause as below	Hence request you to modify this clause as following Shall support minimum 5 Gbps of threat prevention throughput (Firewall + Application Visibility Control + IPS+ Antivirus+ AntiMalware)
1236	Internal Firewall Section 6 - Performance & Scalability	2	Solution should support at least 1.5 million concurrent sessions with Application Visibility Control.		Considering the throughput asked in the RFP specs, concurrent sessions support should be on higher side. This will ensure that Firewall would not compromise during the DDOS attack as it will have enough state table (concurrent connections and sessions per sec) to accomodate DDOS attack	Hence request you to modify this clause as following Solution should support at least 5 million concurrent sessions
1237	Internal Firewall Section 6 - Performance & Scalability	3	Solution should support at least 90,000 new connections per second with Application Visibility Control.		Considering the throughput asked in the RFP specs, concurrent sessions support should be on higher side. This will ensure that Firewall would not compromise during the DDOS attack as it will have enough state table (concurrent connections and sessions per sec) to accomodate DDOS attack	Hence request you to modify this clause as following Solution should support at least 400,000 new connections per second
1238	Internal Firewall Section 1 - NG Firewall	9	The Firewall solution Should support more than 4000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness and should be able to create 40 or more application categories for operational efficiency. Dedicated IPS solution shall be in corporated by the bidder to achive this scale of IPS AVC signatures in this solution.		Every OEM has their own methods of creating application signatures and seggregating them into different categories. Custom application signatures can be created on Fortigate, however categorization of signatures is done by threat intelligence engine i.e. Fortiguard.	Hence request you to modify this clause as following The Firewall solution Should support more than 4000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness. Dedicated IPS solution shall be in corporated by the bidder to achive this scale of IPS AVC signatures in this solution.

1239	Internal Firewall Section 1 - NG Firewall	10	Should be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention.		IPS signature tuning is typically done by threat intelligence engine as it requires large amount of resources like malware samples/IOCs etc.	Request you to modify this clause as below - Should be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) using threat intelligence engine with minimal human intervention.	No Change
1240	Internal Firewall Section 1 - NG Firewall	11	The firewall solution should support at least 30,000 out of the box IPS signatures from Day 1. Should support capability to configure correlation rule where multiple rules/event can be combined together for better efficacy. Dedicated IPS solution shall be in corporated by the bidder to achive this scale of IPS signatures in this solution.		Every OEM has their own language for creating signatures and ways to optimize the number of signatures hence comparing number of signatures will not help to identify effectiveness of a Firewall. Instead, you can ask for 3rd party reports for testing Firewall effectiveness and performance. Also, dedicated IPS solution is asked in RFP, so please confirm whether IPS features needs to be considered for internal Firewall or not.	Request you to modify this clause as below- The firewall solution should support minimum 18,000 out of the box IPS signatures from Day 1. Should support capability to configure correlation rule where multiple rules/event can be combined together for better efficacy. Vendor should also ensure security effectiveness of the proposed solution to protect BOB's environment by providing 3rd party security testing reports like Cyber ratings / NSS labs	No Change
1241	Internal Firewall Section 4 - Management platform and support	2	The management platform must be a dedicated OEM appliance and VM running on server will not be accepted.		It is recommended to use a Virtual machine as it provides ability to scale it in future when number of devices managed by management device increases. Hardware appliance will have a fix number of capacity in terms of devices being managed by it, which cannot be increased further.	Request you to modify this clause as below The management platform must be a dedicated OEM appliance or VM running on server. Required server hardware / resources should be provieded by the bidder.	No Change
1242	Internal Firewall Section 4 - Management platform and support	4	The management appliance should have integrated redundant power supply from day one.		It is recommended to use a Virtual machine as it provides ability to scale it in future when number of devices managed by management device increases. Hardware appliance will have a fix number of capacity in terms of devices being managed by it, which cannot be increased further.	Request you to modify this clause as below In case OEM hardware appliance for management is proposed, it should have integrated redundant power supply from day one.	No Change
1243	Internal Firewall Section 4 - Management platform and support	5	The management platform must be able to store record of at least 600,000 users or hosts.		Logging solution is sized based on the logs getting generated on Firewalls per day.	Request you to provide the expected log size getting generated on Firewall on per day bassis. (e.g 10 Gb, 50 Gb etc)	It is clearly call out in appendix 2, point no 23 of Management Platform and Support
1244	Internal Firewall Section 5 - Hardware Architecture	2	The appliance should support 8x1G Copper ports and 8*10G SFP+ ports on board plus option of having another 1/10G port 8 numbers for expansion		Considering the throughput asked in the specifications, number of ports ask is on very higher side. These many number of 10G ports are typically supported on appliances more than 10 Gbps Threat prevention capacity.	Request you to modify this clause as below The appliance should support 8x1G Copper ports and 8*10G SFP+ ports on board plus option of having additional copper 1G port x 8 numbers for expansion or inbuilt additional 1G copper x 8 ports from day 1	another 1/10G port 8 numbers for expansion will be consider as value add

1245	Internal Firewall Section 5 - Hardware Architecture	3	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 8x64 GB of RAM.		Every OEM has a different hardware architecture and different ways of utilizing hardware resources like RAM / Flash. RAM and CPU are not sizing parameters for any Firewall, it is usually considered for servers and storage.	Request you to modify this clause as below 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 16 GB of RAM.	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.
1246	Internal Firewall Section 5 - Hardware Architecture	5	The appliance shall have redundant and hot swappable power supply and fan(s) module(s).		Redundant / Hotswappable fans are specific to one OEM It is typically supported in very higher series appliances, hence request you to modify this clause	Request you to modify this clause as below The appliance shall have redundant and hotswappable power supply	No Change
1247	Internal Firewall Section 1 - NG Firewall	28	Solution should be able to detect HTTP/3 and SMB over QUIC. Should detect applications over QUIC without enabling decryption. Should be able to assign access control rules based on the service detected over QUIC protocol.		It is recommended practice to enable SSL inpsection for better security controls, because some of the applications might not be detected without SSL inspection, regardless of any OEM technology. Most of the today's applications runs over http and https, hence it will make more sense to run http / https traffic over QUIC protocol for better performance for roaming devices.	Hence request you to modify this clause as below - Solution should be able to inspect and detect HTTP/3 and QUIC traffic. Should detect applications over QUIC. Should be able to assign access control rules based on the service detected over QUIC protocol.	Solution should be able to inspect and detect HTTP/3 and QUIC traffic. Should detect applications over QUIC. Should be able to assign access control rules based on the service detected over QUIC protocol.
1248	Internal Firewall Section 1 - NG Firewall	29	Solution should be able to generate indications of compromise (IoC) connection events based unsafe client applications detected by the system. IoC events should be triggered for encrypted sessions, without decryption, generated from a host using a malicious client. The system should capture the following information in the event viewer/dashboard "such as IP address, MAC address, and OS information of the malicious host, and the timestamp of the suspicious activity". The feature should work with all the TLS versions including TLS 1.3		It is recommended practice to enable SSL inpsection for better security controls, because not all the applications or threats can be detected without SSL inspection, regardless of any OEM technology. Also, information like MAC address, OS information can be available provided Firewall has reachability to users at layer 2	Hence request you to modify this clause as below - Solution should be able to generate indications of compromise (IoC) connection events based unsafe client applications detected by the system. IoC events should be triggered for sessions generated from a host using a malicious client. The system should capture the following information in the event viewer/dashboard "such as IP address, and OS information of the malicious host, and the timestamp of the suspicious activity". The feature should work with all the TLS versions including TLS 1.3	No Change
1249	Internal Firewall Section 1 - NG Firewall	30	Solution should be able to block malicious communications in encrypted traffic based on threat score without decrypting the traffic. Solution should be able to reassemble fragmented Client Hello packets for detection purposes.		Without decryption, any Firewall has limited visibility into applications and threats and such limited visibility can also lead to false positives.	Hence request you to modify this clause as below - Solution should be able to block malicious communications in encrypted traffic based on threat score. Solution should be able to reassemble fragmented Client Hello packets for detection purposes.	No Change

1250	Internal Firewall Section 1 - NG Firewall	31	Solution should be able to identify flows which are extremely large (in total bytes) flows measured over a network link. These flows are larger than 1 GB/10 seconds. Solution should be able to bypass and throttle these flows.		This clause is specific to the OEMs which do not support or has performance impact when processing large flows. This feature may be required in future to support high bandwidth sessions for east-west traffic	Hence Request you to either remove this clause or modify this clause as below Solution should be able to identify flows which are extremely large (in total bytes) flows measured over a network link. These flows are larger than 1 GB/10 seconds. Solution should be able to process these flows.	No Change
1251	Internal Firewall Section 3 - Anti-APT Fearures	1	Should support the capability of providing network-based detection of malware by checking the disposition of unknown files using SHA-256 file-hash or signature (update to be provided in 300 seconds) as they transit the network and capability to do dynamic analysis.		If Sandboxing solution is required, it is recommended to enable inline sandboxing so that firewall can hold the file till the time Sandbox returns the verdict. This way Firewall will be able to avoid patient zero infection.	Hence request you to modify this clause as below - Should support the capability of providing network-based detection of malware by checking the disposition of unknown files using SHA-256 file-hash or signature (update to be provided in 300 seconds) as they transit the network and capability to do dynamic analysis using onprem hardware based sandbox. For dynamic analysis for files, Sandboxing solution is required. Please provide the sandbox sizing details - - Files needs to be scanned per hr - Number of Sandbox appliance in DC and DR We recommed to include below specification for sandboxing - 1) The solution should include onprem sandboxing appliance at DC and DR	No Change
1252	Internal Firewall Section 4 - Management Platform and Support	9	The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows.		3rd party vulnerability exposures are managed by Fortiguard threat intelligence database on continuous bassis and required signatures are automatically pushed to Fortigate devices. Hence request you to modify this clause as following	The proposed solution must be capable of detecting third party vulnerability exposure and apply required signatures to Firewall policies to protect internal servers / apps from getting expoited	No Change
1253	Internal Firewall Section 4 - Management Platform and Support	15	The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows.		Every OEM has different ways of sizing the solution. And for any logging appliance there would always be log capacity that it can handle. Logging solution is sized based on number of logs received on per day basis.	Hence request you to modify this clause as below - Solution should be able to provide insights of hosts/user on basis of indicators of compromise, any license required for this to be included from day one.	No Change

1254	32	9.2	9.2 Indemnity		Request you to pelase consider proposed changes /modification in the adjacent column	We request indemnification should remain limited to direct losses/damages. The Bidder hereby covenants and agrees to indemnify and shall at all times keep indemnified the Bank against loss or damage that Bank may sustain as a result of third party claims arising from damage to tangible property , personal injury or death caused by bidder's negligence. However, Bidder's liability will exclude any special,without limitation loss of profit, loss of revenue, loss of data, negligence, damage to data etc. For any liability excluded by the foregoing and below section (i)Bidder's overall liability shall be limited to immediately preceding 12 months of charges collected by the Bidder under the order in which the liability has arisen. (I) Further Bank sole remedy and the bidder sole liability for any service related matters shall remain limited to applicable liquidated damages/penalties imposed by Bank under this RFP. " This section should be read together with the Limitation	No Change
1255	34	9.3	9.3 No liability		Request you to pelase consider proposed changes /modification in the adjacent column	We suggest the below section to replace the existing clause in the RFP: " *In no event shall either party be liable to the other for any indirect, incidental, special, consequential, exemplary or punitive damages including, but not limited to, damages for lost revenue, lost profits, loss of goodwill, loss of data, technology, equipment or types of damages whatsoever, whether or not caused by any acts of omission or commission and regardless whether such party has been informed of the possibility or the likelihood of such damages. Maximum liability of the Bidder shall be limited to 12months amount paid to Bidder under the relevant PO giving rise to the liability.*"	No Change

1256	34		9.5 Termination of Contract	No Change	Request you to pelase consider proposed changes /modification in the adjacent column	We suggest the existing RFP section to be replaced by the below section: " (i)Either Party may terminate an individual Service at the end of its Initial Term or Service Term (whichever is applicable), by providing no less than ninety (90) days advance written notice to the other Party subject to Bank's payment to Bidder of any outstanding Service Fees, including connection and/or disconnection charges, for the Service(s) so terminated. (ii) Either Party (the "Non-Defaulting Party") may terminate a Service upon written notice of termination to the other Party ("Defaulting Party") if (i) the Defaulting Party breaches a material provision of this Agreement or the applicable PO and the Defaulting Party fails to cure such breach within thirty (30) days after receipt of written notice of breach from the Non-Defaulting Party; or (ii) any bankruptcy, insolvency, administration, liquidation, receivership or winding up	No Change
1257	37	9.6	9.6 Compliance with Laws		Request you to pelase consider proposed changes /modification in the adjacent column	This section shall be subject to the Limitation of liability section.	No Change
1258	38	9.7	9.7 Assignment		Request you to pelase consider proposed changes /modification in the adjacent column	We suggest to include the below: "Notwithstanding the above, either Party may assign this Agreement to an Affiliate or as part of a corporate reorganization, consolidation, merger or sale of substantially all of its assets by providing advance written notice to the other Party of any such proposed assignment".	No Change
1259	38	9.1	9.10 Publicity		Request you to pelase consider proposed changes /modification in the adjacent column	Kindly make this clause mutual	No Change
1260	42	9.23	9.23 Service Level Agreement and Non-Disclosure Agreement		Request you to pelase consider proposed changes /modification in the adjacent column	Please share the document for our review	Not Applicable

1261			Additional Query		We propose the Limitation of Liability clause set out in the adjacent column be added in the RFP.	In no event shall either party be liable to the other for any indirect, incidental, special, consequential, exemplary or punitive damages including, but not limited to, damages for lost revenue, lost profits, loss of goodwill, loss of data, technology, equipment or types of damages whatsoever, whether or not caused by any acts of omission or commission and regardless whether such party has been informed of the possibility or the likelihood of such damages. Maximum liability of the Bidder shall be limited to 12months amount paid to Bidder under the relevant PO giving rise to the liability.	No Change
1262	9	2.1	Bidder should provide 1year of hand holding support post Go-Live, this may extend to 2 years on mutual understanding			Request you pls amend this as -Bidder should provide hand holding support upto 30 days from Go-Live	Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
1263	Additional Query	Additional Query	Additional Query		Kindly confirm that Bidder along with its affiliate including its subsidiaries shall participate in the bid. The contracting and invoicing for proposed services/goods specified in this RFP will be managed by bidder or its wholly owned subsidiary.	Kindly confirm that Bidder along with its affiliate including its subsidiaries shall participate in the bid. The contracting and invoicing for proposed services/goods specified in this RFP will be managed by bidder or its wholly owned subsidiary.	PO and Invoice will be assign to single bidder only
1264	General Query	General Query	RPO/RTO		What is the current RPO and RTO and what tool/s are used for DR replication ?		We will share this details only with final bidder
1265	General Query	General Query	DC/DR		Where is the DC and DR setup running currently? Who is currently managing the DC and DR?		We will share this details only with final bidder
1266	General Query	General Query	Locations and Inventory		Please share HO and Branch details. Please share the inventory for DC/DR and other locations if any.		We will share this details only with final bidder
1267	General Query	General Query	Backup		What is the backup tool used? What is the backup frequency?		This is not relevant question to this RFP
1268	General Query	General Query	Resources		Which are the locations where bidder is expected to have resources.		Mumbai
1269	Appendix01	Virtual Platform	The Bidder should provide 1 Technical Resource from Software OEM for a period of 1 Year to provide timely health check, suggest OEM best practice, conduct timely health check of the deployed solution and submit a report indicating OEM best practices.			Request this resource to be provided by the bidder as they would have completed certification by OEM. Also request you to clarify the detailed Scope to be done by the resource. Timely health checks are provided by the platform anyway and can be handled by operations team	This clause stand removed

1270	Appendix01	Virtual Platform	The Bidder should provide 1 Technical Resource Certified by the Software OEM for the period of the contract to provide operations support, work on day-to day activities of managing the infrastructure, perform infrastructure updates and upgrades.			Is this resource only required to manage the HCI platform? Kindly clarify the skillset and Scope this resource is supposed to handle. Since only one resource is asked, kindly clarify the scope of managed services for the rest of the scope	Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
1271	Annexure02 - Technical Evaluation criteria	1	The bidder should have supplied and installed similar to proposed hardware in last three (3) financial years, i.e. 2021-2022, 2022-23, 2023-24 (Bidder to provide details in Annexure K and submit PO / Contract details)		Request to amend clause as per following column	The bidder should have supplied and installed similar hardware in last three (3) financial years, i.e. 2021-2022, 2022-23, 2023-24 (Bidder to provide details in Annexure K and submit PO / Contract details)	No Change
1272	Annexure02 - Technical Evaluation criteria	2	The bidder should have deployed and configured proposed software as per OEM standard on proposed hardware in last three (3) financial years, i.e. 2021-2022, 2022-23, 2023-24 (Bidder to provide details / submit PO / Contract details)		Request to amend clause as per following column	The bidder should have deployed and configured virtualization software as per OEM standard on proposed hardware in last three (3) financial years, i.e. 2021-2022, 2022-23, 2023-24 (Bidder to provide details / submit PO / Contract details)	The bidder should have deployed and configured proposed software as per OEM certified and standard hardware in last three (3) financial years, i.e. 2021-2022, 2022-23, 2023-24 (Bidder to provide details / submit PO / Contract details)
1273	8	2.1	Bidder should provide onsite support to fix the issues for the period of 1 Year.			Kindly clarify if this is required for all stacks including Server, Virtualization, Network, Security, etc? Why is this asked only for 1 year?	The price quoted by the bidder should cover all the support to the solution including any updates/upgrades and fixing any issues faced. Bidder should provide onsite support to fix the issues for the period of 1 Year after declared the project Go-Live. Remote access would not be permitted for any support / training / change / upgrade / patch management etc Future engagement will be decided basis on the 1st year performance.
1274	9	2.1	Bidder should provide 1year of hand holding support post Go-Live, this may extend to 2 years on mutual understanding.			What kind of support is required for hand holding? Is this entire managed services scope for all components detailed in the Hardware BoM? Should the bidder factor for 24x7 support?	Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
1275	12	3.1	Successful bidder should allocate a network architect to design the network architecture.			Kindly clarify scope of network architect in detail along with provision to quote in commercials. What will be the duration of assignment?	Successful bidder should allocate a network architect to design the network architecture for propose solution during implementation.
1276	12	3.1	The successful bidder should also integrate existing infrastructure setup (like existing LAN, proxy, MFA, SIEM) with the new devices to be supplied.			Kindly provide details of infra to be integrated	This will be market leading product only. Basis on compatibility Bidder has to integrate the existing infra setup with new setup. All the product will be share only with the final bidder

1277	12	3.1	The successful bidder will be expected to provide all the necessary software licenses, implement, train and handover the solution to BOBCARD IT team. They would subsequently provide first, second and third level of support through configuration changes, bug fixes, updates and upgrades.			This clearly states scope is only implementation and handover to BoBCard IT team, kindly clarify?	No Change
1278	12	3.1	The successful bidder's SME should provide onsite support to test out existing or new feature on the solutions during the entire project tenure.			Kindly include resource in commercial sheet. Is this across entire technology stack?	Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live. Till to support of 1 year
1279	13	3.1	Break fix Support			Since bidder is expected to implemented and handover to BoBCard IT team, this should be in scope of BoBCard. If resources are required for the entire technology stack, this needs to be called out in commercial sheet.	Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
1280	13	3.1	L2 and L3 onsite support post implementation a. Software upgradation b. Hardware Upgradation c. Mass Changes for compliance d. Major, minor changes in feature/functionality roll out on the same infrastructure.			Since bidder is expected to implemented and handover to BoBCard IT team, this should be in scope of BoBCard. If resources are required for the entire technology stack, this needs to be called out in commercial sheet.	Contract will be of 5years as per BOM for TCO. Monitoring and managed services SLA base will be in bidder scope for 1year after project declared as Go-Live
1281	17	4	Service Levels			Since bidder is only providing a resource (or handing over operations to BoBCard IT team), this section should not be part of this RFP	No Change
1282	17	4	SLA: The solution is expected to be available for 99.99% on 24x7			Since hardware and configuration is sized by BoBCard IT team, this should not be part of bidder scope	Here ask of SLA for implemented solution and not for uptime of BOBCARD application
1283	31	8	Payment terms : Activity : Supply of Servers & Network Delivery timelines : Within 5-6 weeks Payment terms : 20% of Total Cost of Equipment outlined in BOM			Request to change delivery timeline to 8-12 weeks as this is OEM specific	Supply of Servers & Network component as prescribed under hardware requirement Within 6-8 weeks from date of PO. Rest all clause remain same
1284	37	9.5	The selected Bidder will assist the company in migration exercise without any cost to the company.			Kindly clarify scope of data migration and provide details on the type and volume of data to be migrated including VM, DB and storage details.	As mentioned in this addendum
1285	IPS / Platform Requirement	3	The device should have functionality of in-built hardware based fail-open & software fail-open		As per our understanding, the device should support Layer 2 fallback functionality and not a bypass NIC card at hardware, which provides seamless traffic in case of appliance failure. "Is our understanding correct?		No Change

1286	IPS / Performance & Scalability	3	The appliance should support 8x1G Copper ports and 8*10G SFP+ ports on board plus option of having another 1/10G port 8 numbers for expansion		The requirement is for 5 Gbps throughput and there are many ports asked in the RFP, So request to remove additional ports requirements.	Reuest for change "The appliance should support 8x1G Copper ports and 8*10G SFP+ ports on board".	another 1/10G port 8 numbers for expansion will be consider as value add
1287	IPS / Features	15	Should support more than 3000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness		IPS solution provides IPS signatures including applications, vulnerabilities..ect.. IS there any specific reason to ask seperately 3000 sigantures for applications	Request for deletion	No Change
1288	IPS / Features	16	Should support more than 50,000 (excluding custom signatures) IPS signatures or more		This is vendor specific, as there is only one OEM provides 50,000 + IPS signatures. So request to change it to at least 20,000+ IPS signatures	Request for change "Should support more than 20,000 (excluding custom signatures) IPS signatures or more".	No Change
1289	IPS / Management	1	The management platform must be accessible via a web-based interface and ideally with no need for additional client software		The management platform provides ease of operational administrattion. It should not depend on the way to get access to the management platform, so request to remove "ideally with no need for additional client software".	Request for deletion	No Change
1290	IPS / Management	3	The management appliance should have 2 x 1G and 2*10G port and integrated redundant power supply from day one		As per experience, most organizations have dedicated management zone and run with 1G port. Is there any specific reason to ask 10G port for the management appliance?	Request for deletion	10G is for uplink
1291	IPS / Management	6	The management platform must domain multi-domain management		Please provide more clarity for multi domain management		IPS solution should manage multiple domains belongs to the BOBCARD
1292		Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 1	The proposed solution should be a Hyperconverged infrastructure (HCI) with 5 years comprehensive warranty		Not having the option to use extenal storage limits customer's ability from leveraging existing/external storage for specific application requirement which may come in future or on going setup. These application then will have to be hosted in seprate infrastructure adding to cost and will create seprate silo to manage along with migration effort of existing data	The proposed solution should be a Hyperconverged infrastructure (HCI) with option to use external storage with 5 years comprehensive warranty	The proposed solution should be a Hyperconverged infrastructure (HCI) with an option to use as external storage
1293		Appendix01 Techno Functional Requirements- Server and Virtual platform > Software Defined Storage > 14	The proposed solution should support Replication factor RF-2 (1 Node failure). Proposed Solution must be planned with N+1 without considering Dedup, compression, erasure coding at both DC and DR location.		RFP asks for 99.99 % availability SLA for the proposed solution. It will require minimum N+2 configuration. 99.99 % SLA would also require BoB Cards to consider four site (DC, DR , NDC and NDR) architecture along with streched cluster (both Infrastructire & kubernetes) between DC and NDC . Request Bob Cards to clarify the business impact of missing 99.99 % availability SLA. Is current setup also has 99.99 % availability ?	The proposed solution should support Replication factor RF-3 (2 Node failure). Proposed Solution must be planned with N+2 without considering Dedup, compression at both DC and DR location.	No Change, additional feature will be consider as value add
1294		Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmentation > 1	The Solution should be capable of supporting major hardware OEMs like Juniper, Arista, Cisco, HPE and Dell. The proposed solution should be a purely software-based solution and should not be dependent on any hardware make and model.		The key benefits of no dependecy on hardware is by using software defined networking i.e overlay. Overlay is mandatory for network & Security automation as part of software defined data center.	The Solution should be capable of supporting major hardware OEMs like Juniper, Arista, Cisco, HPE and Dell. The proposed solution should be a purely software-based solution and should not be dependent on any hardware make and model by creating overlay tunnels between the hosts.	No Change, additional feature will be consider as value add

1295		Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmentation > 2	The solution should provide a distributed firewall such that the firewalling for Virtual Machines can be provided closest to the application within the server itself without traffic going to a Physical Firewall.		*As per security framework its recommended not to use standard ports for your applications and hence to have effective security on per VM basis an application/L7 firewalling is must.* Containers & Kubernetes are now part of all modern applications hence networing and security for container shall also be considered for end to end application security. there is App ID requirement is mentioned in RFP as part of "Internal Firewall" spec point # 23 hence same should be considered for mirosegmenation as well otherwise it will create non standard architecture.	The solution should provide a distributed firewall such that the application aware and identity based statefull firewalling for Virtual Machines can be provided closest to the application within the server itself without traffic going to a Physical Firewall or regardless of underlying L2 Netwrork topology. The solution should also provide an integrated networking solution (CNI implementations) as well as provide advance turnkey container networking & firewalling services. Solution should support for container networking plug-ins, support for pod to pod communication and support for ingress controllers. The micro-segmentation solution should have a capability for stateful firewalling and ALGs (Application Level Gateway) on a per-workload granularity regardless of the underlying L2 network topology (i.e. possible on either logical network overlays or underlying VLANs), embedded in the hypervisor kernel, distributed across entire environment with centralized policy and management	No Change
1296		Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmenation >5	The proposed solution should provide the ability to define firewall rules at VM level for east-west traffic in order to implement Zero Trust Security		Zero trust Security framework mandates TLS inspection for encrypted traffic, URL Filtering and Layer 7 application firewalling.	The proposed solution should provide the ability to define Layer 7 application firewall rules at VM level for east-west traffic in order to implement Zero Trust Security alongwith URL Filtering and TLS inspection for encrypted traffic	No Change, additional feature will be consider as value add
1297		Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmenation >4	The Proposed Solution including Hypervisor, SDS, SDN and Micro segmentation must be from the same OEM.		SDN is missing in the spec, SDN will be mandatory to create complete automated Software Defined data center by creating an abstraction of the network enabling programming of network behavior in a centrally controlled manner through software applications.	The Proposed Solution including Hypervisor, SDS, SDN and Micro segmentation must be from the same OEM.	No Change, additional feature will be consider as value add
1298		Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmenation >6	The proposed solution should allow users to define granular firewall rules based on IP Addresses, Tags/Categories and Subnets to segment User Applications		Its necessary to have dynamic security group capability to ensure complete automation. RFP page 8 -> 2.0 --> Requirement Summary--> 2.1 Intent--> mentions requirement for IPv6 "The proposed solution should support both IPv4 and IPv6."	The proposed solution should allow users to define granular firewall rules for both VM and conatiners based on IP Addresses, VM Names, Tags/Categories and Subnets to segment User Applications by creating dynamic security groups. The solution should have capability to provide stateful micro-segmentation for virtual machines and Kubernetes workloads from a single console. The solution should also support enforcement of stateful distributed firewall for IPv6 VM workloads. These firewall rules can use IPv6 addresses, IPv6 CIDR, IP Sets that include both IPv4 and IPv6 addresses and security groups that can include logical ports that have both IPv4 and IPv6 addresses. IPv6 capability should be available both at management and data plane	No Change
1299		Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmenation >7	Solution should provide capability to create network segments by defining them entirely in software and avoid the need to re-architect your network or deploy physical appliances		L2 Streching is required for better application availability considering RFP asks for 99.99 % availability on monthly basis. RFP Page 17 -> "4. Service Levels "-->"SLA: The solution is expected to be available for 99.99% on 24x7 and up time availability will be calculated on monthly basis."	Solution should provide capability to create network segments and L2 Streching between DC and DR by defining them entirely in software and avoid the need to re-architect your network or deploy physical appliances	No Change, L2 stretching implementation will be discuss with elected bidder.

1300		Appendix01 Techno Functional Requirements- Server and Virtual platform > Container >2	The solution must be able to manage Kubernetes clusters. Licenses for managing Kubernetes clusters should be implemented from Day-1		Kubernetes Cluster doesn't work in isloation but require other components such as container registry and backup solution. If not included than Bob Card will have procure them separately. And Not aving Windows Container support will block any windows based apps to be deployed on Kubernetes Platform.	The solution must be able to manage Kubernetes clusters. Licenses for managing Kubernetes clusters along with components such as backup, container registry and monitoring alongwith Windows Container support should be implemented from Day-1	Yes, BOBCARD will take care such requirement
1301		Appendix01 Techno Functional Requirements- Server and Virtual platform > Container >3	Must have provisioning, operations and lifecycle management of Kubernetes, automated deployment, scaling, and operation of Kubernetes clusters		Complete Automation is not possible without Auto Scaling and Auto Healing of Kubernetes Clusters. One has to manually add nodes in case of failure or unprovisioned increase in load.	Must have provisioning, operations and lifecycle management of Kubernetes, automated deployment, Auto scaling & Auto Healing, and operation of Kubernetes clusters	Must have provisioning, operations and lifecycle management of Kubernetes, automated deployment, Auto scaling & Auto Healing, and operation of Kubernetes clusters
1302		Appendix01 Techno Functional Requirements- Server and Virtual platform > Container >4	Container Platform should provide single pane of Glass for Lifecycle Management of all K8S clusters deployed on prem.		Kubernetes Cluster doesn't work in isloation but require other components such as container registry and backup solution. These shall too be considered for life cycle management	Container Platform should provide single pane of Glass for Lifecycle Management of all K8S clusters alongwith ingress, backup and container registry deployed on prem.	No Change, additional feature will be consider as value add
1303		Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management >1	The solution should provide capability of generating reports for usage, performance, compliance, health, forecasting and capacity.		Bob Cards will need capacity optimization capabilities to identify over-provisioned & under-provisioned resources and provide recommendations, alerts and automated actions on right-sizing and resource consumption so they can be right-sized for adequate performance and avoid resource wastage. Should provide visibility of capacity and VMs which can be reclaimed and cost visibility of the reclaimed capacity and VMs.	The solution should provide capability of generating reports for health, Capacity Optmization - Right Sizing (Under sized, Oversized), Reclamation (Idle, Powered off , Snapshot, Orphaned Disk , Forecasting - Capacity Forecasting, Migration assessment, Migration Planning Usage - Process and service utlization Compliance - Regulatory Benchmark (PCIDSS and ISO) Security Guidelines for Infrastructure and Cloud Management	No Change, additional feature will be consider as value add
1304		Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management >11	The solution should have intelligent operations with anomaly detection which will allow monitoring seasonal trends and automatically send email alert		BoB Cards will not be able to manage the infrastructure without comprhesive log management capability. Its also mandatory for from regulation/compliance perspective to have log stored for given period of time for audit. BoB Card would need apps (database and Application) to infra (Server, Storage , Network) level visibility for troubleshooting and performance monitoring.	The solution should have AI/ML driven intelligent operations & troubleshooting workbench with anomaly detection,third party infra (Server, Storage , Network, database and Application) along with parent child relatiohship mapping, service and process monitoring which will allow monitoring seasonal trends and automatically send email alert. The solution should also have log management capability for infrastructure and applications . log management solution should delivers intuitive, actionable dashboards, sophisticated analytics, and broad third-party extensibility across physical, virtual, and cloud environments.	No Change, additional feature will be consider as value add
1305		Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management >7	The solution must have an approval process to review, reject or approve the deployment requests from the marketplace.		The solution must have an approval process to review, multi level & auto reject or approve the deployment requests from the marketplace.	Bob Cards would need multiple levels of approval with E-mail notifications with ability to automate manual provisioning and de-provisioning of the tasks and policies embedded in each layer of their application including auto -approve and auto-reject capability based on application criticality	No Change, additional feature will be consider as value add
1306		Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 6	Hypervisor should support container and opensource integration for cloud native application from day-1. Must be a Kubernetes ready from day-1.		Kubernetes does't work in isolation and requires multiple components for production setup.	Hypervisor should support container both Linux and Windows along with other kubernetes ecosystems such as container registry, backup, ingress & monitoring and opensource integration for cloud native application from day-1. Must be a Kubernetes ready from day-1.	Yes, BOBCARD will take care such requirement

1307		Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 16	Virtualization Manager should provide feature which can perform quick, as-needed deployment of additional virtualized hosts. When the service is running, it can push out update images, eliminating patching and update without impacting production.		Please clarify the scenario "When the service is running, it can push out update images, eliminating patching and update without impacting production." Its not clear from the language as what is the expected outcome.	Virtualization Manager should provide feature which can perform quick, as-needed deployment of additional virtualized hosts. When the service is running, it can push out update images, eliminating patching and update without impacting production. Proposed solution should allow live patching of select critcal security patches.	Virtualization manager should allow addition of new nodes and patching/upgrade of hypervisor running on the node without any VM downtime.
1308		Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 22	Unlimited VM replication from DC to DR (No restriction on VM replication and DR orchestration) with the capability to define Recovery Plans		Unlimted is open terms, request you to provide the number of VMs to orchestrated for automated recovery. As unlimited is relevant for one specific vendor . The VMs to be protected/orchestrated are limited to what can be provisioned on these 14 servers of production.	Request BoB cards to Clarify the need for Recovery Plans- We do provide unlimited Replication from DC to DR which is orchestrated. In Terms of Recovery Plans (which is automation) We request bank to consider defining specific number of Virtual Machines. Its however best to use extends the existing DR orchestration solution fot this environment as well.	No Change, can not predict the exact number of VMs for next 5 Years which need to be replicated.
1309		Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 23	Proposed solution should have a self-service restore feature on a per-VM basis to allow trusted application administrators to recover their own files with the ability to mount snapshots as a drive in Windows VMs		Please clarify this requirement, this looks like back and restore requirements	Proposed solution should have a self-service restore feature on a per-VM basis to allow trusted application administrators to recover their own VMs from the snapshot	This will help BOBCARD to recover file without losing current state of virtual machine.
1310		Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 24	Hypervisor should provide Visibility for Running VM and their connectivity co-relationship with Network Ports on attached Physical TOR / Core Direct which Include Network RX/TX Bytes.		Monitoring is not considering all components of the stack. Unless end to end visibility is provided as part of this solution BoB Card has to spend separately on monitoring.	Hypervisor should provide Visibility for Running VM and their connectivity co-relationship with Network Ports on attached Physical TOR / Core Direct which Include Network RX/TX Bytes.Solution Should provide end to end visibility across physical firewall, switch and storage, Flow Analysis and Security Planning,Guided Troubleshooting, Microsegmentation planning, RCA (Connectivity Problem, Packet Loss, N/W latency), Application Discovery, Service Monitoring , Application Dependency Mapping and monitoring of non compliant ports	Yes, BOBCARD will take care such requirement. However Hypervisor should provide Visibility for Running VM and their connectivity co-relationship with Network Ports on attached Physical Port which Include Network RX/TX Bytes.
1311		Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 30	Virtualization software or the solution should provide Cluster level encryption protects unauthorized data access at-rest.		Having capability to do the enscryption at app VM level and in transit is required to complete solution.	Virtualization software or the solution should provide Cluster level, VM Level encryption protects unauthorized data access at-rest and in transit.	No Change, additional feature will be consider as value add
1312		Appendix01 Techno Functional Requirements- Server and Virtual platform > Software Defined Storage > 1	Maintain primary working set copy of active data on the Local Node as VM's are hosted to provide high IOPS and low latency. Proposed solution must be proposed for faster reads and write for Business-critical Apps.		Architecture is specific to one vendor, request BoB Cards to consider on outcome than specific architecture. There is no specific latency requirements mentioned in the spec.	Proposed solution must be proposed for faster reads and write for Business-critical Apps.	No Change
1313		Appendix01 Techno Functional Requirements- Server and Virtual platform > Software Defined Storage >2	The solution must have De-duplication and Compression features licensed and implemented from day one (Should not have dependency on any proprietary hardware device).		Solution should have flexibility to implement either compression and de-duplication. BoB Cards should conisder overhead while deciding on both.	The solution must have De-duplication/Compression features licensed and implemented from day one (Should not have dependency on any proprietary hardware device).	No Change
1314		Appendix01 Techno Functional Requirements- Server and Virtual platform > Software Defined Storage >24	The proposed solution should support 1 min RPO & 1 hour RTO for critical workload in case BOB Cards wants to have this capability replication for Future use. The proposed solution should have native Replication and DR Orchestration from Day-1		What is the use case for 1 min RPO and 1 Hour RTO? is this linked with some regulatory requirement? Replication is best handled at application level as having additional solution for infrastructure will complexity and cost for BoB Cards Its best to use extends the existing DR orchestration solution for this environment as well.	What is the use case for 1 min RPO and 1 Hour RTO? is this linked with some regulatory requirement? Replication is best handled at application level as having additional solution for infrastructure will complexity and cost for BoB Cards Its best to use extends the existing DR orchestration solution for this environment as well.	This is required for BOBCARD mission critical application. The solution should capable to support 1min RPO. The propose replication solution should be same OEM as the virtualization solution to provide seamless integration.

1315		Appendix01 Techno Functional Requirements- Server and Virtual platform > Software Defined Storage >25	The solution provided should function even after one node failure.		RFP asks for 99.99 % availability SLA for the proposed solution. It will require minimum N+2 configuration for required resiliency and uptime.	The solution provided should function even after two node failure.	No Change, additional feature will be consider as value add
1316		Appendix01 Techno Functional Requirements- Server and Virtual platform > Software Defined Storage >31	The solution should provide enterprise data services such as compression completely in software. Software Defined Storage solution must have de-duplication and compression features Licensed and implemented from day one. These functionalities should be part of the proposed solution. The solution must have functionality to support compression and or deduplication online on data container without any downtime and data loss as per business requirement.		Solution should have flexibility to implement either compression and de-duplication. BoB Cards should conisder overhead while deciding on both.	The solution should provide enterprise data services such as compression completely in software. Software Defined Storage solution must have de-duplication or compression features Licensed and implemented from day one. These functionalities should be part of the proposed solution. The solution must have functionality to support compression and or deduplication online on data container without any downtime and data loss as per business requirement.	No Change
1317		Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmentation > new point	New Point		IP/MAC spoofing is major security concern for organizations like BoB Cards handing customers data.	The solution must ensure that there is not alteration in the IP address of the Virtual machine, by blocking the traffic from or to the VM inherited as a feature in the Solution.	No Change
1318		Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmentation > new point			VPC will enable Bob Cards to create isolation from access , resources, network and security.	The solution should support multi-tenancy to isolate networking/security for different departments/function within BoB Cards upto a minimum of 4 tenants and 5 VPCs	No Change, additional feature will be consider as value add
1319		Appendix01 Techno Functional Requirements- Server and Virtual platform > Container > 6	Should support cluster scale out i.e addition of worker nodes as and when required.		Complete Automation is not possible without Auto Scaling and Auto Healing of Kubernetes Clusters. One has to manually add nodes in case of failure or unprovisioned increase in load.	Should support Automated cluster scale out i.e addition of worker nodes as and when required.	No Change
1320		Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > 3	The solution shall provide a single pane of glass for automated provisioning with model-based orchestration of compute, network and storage through a unified multi-tenant self-service catalog.		All modern applications are combination of both container and VM form factor.	The solution shall provide a single pane of glass for automated provisioning with model-based orchestration of compute, network , storage and Kubernetes through a unified multi-tenant self-service catalog .	No Change, additional feature will be consider as value add
1321		Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > 5	The solution must provide a self-service portal to allow user to consume the creation of infrastructure easily.		All modern applications are combination of both container and VM form factor.	The solution must provide a self-service portal to allow user to consume the creation of infrastructure easily for both VM and Kubernetes.	No Change, additional feature will be consider as value add
1322		Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > 8	The software must allow the designer to use shell script, PowerShell script to code the automation.		Python and nodeJs are very popular language for scrpting in terms resource availability and community support	The software must allow the designer to use shell script, PowerShell script, Python and node JS to code the automation.	No Change, additional scripting will be value add
1323		Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > 9	The software must allow the designer to design VM blueprints.		All modern applications are combination of both container and VM form factor.	The software must allow the designer to design Multi VM & Kubernetes blueprints.	No Change, additional feature will be consider as value add
1324		Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > 12	The solution should have simple low-code, no-code automation engine which allows automating day-to-day routine tasks		All modern applications are combination of both container and VM form factor.	The solution should have simple low-code, no-code automation engine which allows automating day-to-day routine tasks such as Snapshot creation, Addition of Disk, Power Cycle (Suspend , Shutdown, Reboot, reset), Resize, Rebuild, Additional of Network, VM Unregister , Delete,connect remote console, Change Security Group with capability to create additional resource actions as out of the box capability.	No Change, additional feature will be consider as value add
1325		Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > New Point	New Point		Bob Cards will need Cost transparency (Showback and Chargeback capability) across private, hybrid to optimize planning and prioritization of VM/ Server/Application onboarding/provisioning	Solution should provide capability to define and showcase cost to create cloud like experience to the business unit with the overall cost spend on the infrastructure [server hardware, storage, licenses, application, maintenance, labor, network, facilities , etc.	No Change, additional feature will be consider as value add

1326		Appendix02 Techno Functional Requirements- Network components > LB/WAF & IPS	New Point		Modern applications increasingly require software-defined networking (SDN) and security solutions due to their need for greater flexibility, agility, and scalability. Traditional networking and security methods often lack the adaptability to support the dynamic nature of modern application environments, especially in cloud	We request BoB Card to allow for both software and hardware based solution for Load Balancer, WAF, IPS/IDS. As these components are dynamic as per application consumption requirements and considering bob card is directly managing customer data, its very critcal that these components are added as part of sofwate defined stack.	No Change
1327		Eligibility Criteria	Client references and contact details (email/ landline/ mobile) of customers for whom the Bidder has executed similar projects in India. (Start and End Date of the Project to be mentioned) in the past (At least 3 client references are required)		In a comprehensive technical evaluation, all components—servers, storage, networking, security, and support—must be assessed individually and as part of the broader system. The interaction between different components will often highlight strengths and weaknesses that are not immediately obvious when evaluating them in isolation. Given the complexity of such projects, a holistic, integrated approach to the evaluation is essential to ensure	Kind request to clarify technical evaluation criteria on depth.	No change, it will be as per annexure 2
1328		Annexure 2 - Evaluation Criteria	Project plan,Deliverables, Timelines, Experience on proposed solution, value add - Weightage is 30%				Query is not mentioned
1329	31	Payment Terms	Balance 50% of Hardware and software licenses amount and 70% of installation within 45 days from the date of acceptance of Tax Invoice by BOBCARD.		Acceptance / Go-live by BOBCARD / After 30 days of Acceptance / Go-Live	kindly keep 10% instead of 50% as it process to Golive will take atleast 8 to 12 months and will be financial loss for the bidders.	Supply of Servers & Network component as prescribed under hardware requirement Within 6-8 weeks we expect solution implementation and go live in 4-6week, migration of existing setup will not be done once project declare as go live.
1330	Annexure1	3	The Bidder must have turnover of minimum 100 Cr avarage during last 03 (three) financial year(s) i.e. FY 2021-2022, 2022-23, 2023-24 and 100+cr for FY 2023-24			The turnover should be defined as such like that the snall, mid level compnaies can be eligible to bid for this tender.	No Change
1331	Annexure1	5	Bidder should have experience of minimum 3 years in providing the Proposed Products/Services mentioned in the RFP.			Experience Criteria should not be there so that small, mid level companies having less experience can be eligible for this bid.	No Change
1332	NA	NA	Consortium clause is not there.			Consortium clause should be there as small compnaies can jointly tie up with the mid level companies to do this bid jointly.	No Change
1333	5	7	Last date & time for submission of Bids 19-11-24 at 03:00 pm			Bid submission last date should be extended as OEMs needs clarificationon the compliance part shared to study & deep go through. Last date should be extended to 30th Nov, 24 as per our suggestion so that we can do this bid.	This is taken care in corrigendum
1334		Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 1	The proposed solution should be a Hyperconverged infrastructure (HCI) with 5 years comprehensive warranty		Not having the option to use extenal storage limits customer's ability from leveraging existing/external storage for specific application requirement which may come in future or on going setup. These application then will have to be hosted in seprate infrastructure adding to cost and will create seprate silo to manage along with migration effort of existing data	The proposed solution should be a Hyperconverged infrastructure (HCI) with option to use external storage with 5 years comprehensive warranty	The proposed solution should be a Hyperconverged infrastructure (HCI) with an option to use as external storage
1335		Appendix01 Techno Functional Requirements- Server and Virtual platform > Software Defined Storage > 14	The proposed solution should support Replication factor RF-2 (1 Node failure). Proposed Solution must be planned with N+1 without considering Dedup, compression, erasure coding at both DC and DR location.		RFP asks for 99.99 % availability SLA for the proposed solution. It will require minimum N+2 configuration. 99.99 % SLA would also require BoB Cards to consider four site (DC, DR , NDC and NDR) architecture along with streched cluster (both Infrastuctire & kubernetes) between DC and NDC . Request Bob Cards to clarify the business impact of missing 99.99 % availability SLA. Is current setup also has 99.99 % availability ?	The proposed solution should support Replication factor RF-3 (2 Node failure). Proposed Solution must be planned with N+2 without considering Dedup, compression at both DC and DR location.	No Change, additional feature will be consider as value add

1336		Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmentation > 1	The Solution should be capable of supporting major hardware OEMs like Juniper, Arista, Cisco, HPE and Dell. The proposed solution should be a purely software-based solution and should not be dependent on any hardware make and model.		The key benefits of no dependecy on hardware is by using software defined networking i.e overlay. Overlay is mandatory for network & Security automation as part of software defined data center.	The Solution should be capable of supporting major hardware OEMs like Juniper, Arista, Cisco, HPE and Dell. The proposed solution should be a purely software-based solution and should not be dependent on any hardware make and model by creating overlay tunnels between the hosts.	No Change, additional feature will be consider as value add
1337		Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmentation > 2	The solution should provide a distributed firewall such that the firewalling for Virtual Machines can be provided closest to the application within the server itself without traffic going to a Physical Firewall.		*As per security framework its recommended not to use standard ports for your applications and hence to have effective security on per VM basis an application/L7 firewalling is must.* Containers & Kubernetes are now part of all modern applications hence networing and security for container shall also be considered for end to end application security. there is App ID requirement is mentioned in RFP as part of "Internal Firewall" spec point # 23 hence same should be considered for mirosegmentation as well otherwise it will create non standard architecture.	The solution should provide a distributed firewall such that the application aware and identity based statefull firewalling for Virtual Machines can be provided closest to the application within the server itself without traffic going to a Physical Firewall or regardless of underlying L2 Netwrork topology. The solution should also provide an integrated networking solution (CNI implementations) as well as provide advance turnkey container networking & firewalling services. Solution should support for container networking plug-ins, support for pod to pod communication and support for ingress controllers. The micro-segmentation solution should have a capability for stateful firewalling and ALGs (Application Level Gateway) on a per-workload granularity regardless of the underlying L2 network topology (i.e. possible on either logical network overlays or underlying VLANs), embedded in the hypervisor kernel, distributed across entire environment with centralized policy and management	No Change
1338		Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmenation >5	The proposed solution should provide the ability to define firewall rules at VM level for east-west traffic in order to implement Zero Trust Security		Zero trust Security framework mandates TLS inspection for encrypted traffic, URL Filtering and Layer 7 application firewalling.	The proposed solution should provide the ability to define Layer 7 application firewall rules at VM level for east-west traffic in order to implement Zero Trust Security alongwith URL Filtering and TLS inspection for encrypted traffic	No Change, additional feature will be consider as value add
1339		Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmenation >4	The Proposed Solution including Hypervisor, SDS, SDN and Micro segmentation must be from the same OEM.		SDN is missing in the spec, SDN will be mandatory to create complete automated Software Defined data center by creating an abstraction of the network enabling programming of network behavior in a centrally controlled manner through software applications.	The Proposed Solution including Hypervisor, SDS, SDN and Micro segmentation must be from the same OEM.	No Change, additional feature will be consider as value add
1340		Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmenation >6	The proposed solution should allow users to define granular firewall rules based on IP Addresses, Tags/Categories and Subnets to segment User Applications		Its necessary to have dynamic security group capability to ensure complete automation. RFP page 8 -> 2.0 --> Requirement Summary--> 2.1 Intent--> mentions requirement for IPv6 "The proposed solution should support both IPv4 and IPv6."	The proposed solution should allow users to define granular firewall rules for both VM and conatiners based on IP Addresses, VM Names, Tags/Categories and Subnets to segment User Applications by creating dynamic security groups. The solution should have capability to provide stateful micro-segmentation for virtual machines and Kubernetes workloads from a single console. The solution should also support enforcement of stateful distributed firewall for IPv6 VM workloads. These firewall rules can use IPv6 addresses, IPv6 CIDR, IP Sets that include both IPv4 and IPv6 addresses and security groups that can include logical ports that have both IPv4 and IPv6 addresses. IPv6 capability should be available both at management and data plane	No Change

1341		Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmenation >7	Solution should provide capability to create network segments by defining them entirely in software and avoid the need to re-architect your network or deploy physical appliances		L2 Streching is required for better application availability considering RFP asks for 99.99 % availability on monthly basis. RFP Page 17 -> "4. Service Levels "-->"SLA: The solution is expected to be available for 99.99% on 24x7 and up time availability will be calculated on monthly basis."	Solution should provide capability to create network segments and L2 Streching between DC and DR by defining them entirely in software and avoid the need to re-architect your network or deploy physical appliances	No Change, L2 stretching implementation will be discuss with elected bidder.
1342		Appendix01 Techno Functional Requirements- Server and Virtual platform > Container >2	The solution must be able to manage Kubernetes clusters. Licenses for managing Kubernetes clusters should be implemented from Day-1		Kubernetes Cluster doesn't work in isloation but require other components such as container registry and backup solution. If not included than Bob Card will have procure them separately. And Not aving Windows Container support will block any windows based apps to be deployed on Kubernetes Platform.	The solution must be able to manage Kubernetes clusters. Licenses for managing Kubernetes clusters along with components such as backup, container registry and monitoring alongwith Windows Container support should be implemented from Day-1	Yes, BOBCARD will take care such requirement
1343		Appendix01 Techno Functional Requirements- Server and Virtual platform > Container >3	Must have provisioning, operations and lifecycle management of Kubernetes, automated deployment, scaling, and operation of Kubernetes clusters		Complete Automation is not possible without Auto Scaling and Auto Healing of Kubernetes Clusters. One has to manually add nodes in case of failure or unprovisioned increase in load.	Must have provisioning, operations and lifecycle management of Kubernetes, automated deployment, Auto scaling & Auto Healing, and operation of Kubernetes clusters	Must have provisioning, operations and lifecycle management of Kubernetes, automated deployment, Auto scaling & Auto Healing, and operation of Kubernetes clusters
1344		Appendix01 Techno Functional Requirements- Server and Virtual platform > Container >4	Container Platform should provide single pane of Glass for Lifecycle Management of all K8S clusters deployed on prem.		Kubernetes Cluster doesn't work in isloation but require other components such as container registry and backup solution. These shall too be considered for life cycle management	Container Platform should provide single pane of Glass for Lifecycle Management of all K8S clusters alongwith ingress, backup and container registry deployed on prem.	No Change, additional feature will be consider as value add
1345		Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management >1	The solution should provide capability of generating reports for usage, performance, compliance, health, forecasting and capacity.		Bob Cards will need capacity optimization capabilities to identify over-provisioned & under-provisioned resources and provide recommendations, alerts and automated actions on right-sizing and resource consumption so they can be right-sized for adequate performance and avoid resource wastage. Should provide visibility of capacity and VMs which can be reclaimed and cost visibility of the reclaimed capacity and VMs.	The solution should provide capability of generating reports for health, Capacity Optmization - Right Sizing (Under sized, Oversized), Reclamation (Idle, Powered off , Snapshot, Orphaned Disk , Forecasting - Capacity Forecasting, Migration assessment, Migration Planning Usage - Process and service utlization Compliance - Regulatory Benchmark (PCIDSS and ISO) Security Guidelines for Infrastructure and Cloud Management	No Change, additional feature will be consider as value add
1346		Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management >11	The solution should have intelligent operations with anomaly detection which will allow monitoring seasonal trends and automatically send email alert		BoB Cards will not be able to manage the infrastructure without comprhesive log management capability. Its also mandatory for from regulation/compliance perspective to have log stored for given period of time for audit. BoB Card would need apps (database and Application) to infra (Server, Storage , Network) level visibility for toubleshooting and performance monitoring.	The solution should have AI/ML driven intelligent operations & troubleshooting workbench with anomaly detection,third party infra (Server, Storage , Network, database and Application) along with parent child relatiohship mapping, service and process monitoring which will allow monitoring seasonal trends and automatically send email alert. The solution should also have log management capability for infrastructure and applications . log management solution should delivers intuitive, actionable dashboards, sophisticated analytics, and broad third-party extensibility across physical, virtual, and cloud environments.	No Change, additional feature will be consider as value add
1347		Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management >7	The solution must have an approval process to review, reject or approve the deployment requests from the marketplace.		The solution must have an approval process to review, multi level & auto reject or approve the deployment requests from the marketplace.	Bob Cards would need multiple levels of approval with E-mail notifications with ability to automate manual provisioning and de-provisioning of the tasks and policies embedded in each layer of their application including auto -approve and auto-reject capability based on application criticality	No Change, additional feature will be consider as value add
1348		Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 6	Hypervisor should support container and opensource integration for cloud native application from day-1. Must be a Kubernetes ready from day-1.		Kubernetes does't work in isolation and requires multiple components for production setup.	Hypervisor should support container both Linux and Windows along with other kubernetes ecosystems such as container registry, backup, ingress & monitoring and opensource integration for cloud native application from day-1. Must be a Kubernetes ready from day-1.	Yes, BOBCARD will take care such requirement

1349		Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 16	Virtualization Manager should provide feature which can perform quick, as-needed deployment of additional virtualized hosts. When the service is running, it can push out update images, eliminating patching and update without impacting production.		Please clarify the scenario "When the service is running, it can push out update images, eliminating patching and update without impacting production." Its not clear from the language as what is the expected outcome.	Virtualization Manager should provide feature which can perform quick, as-needed deployment of additional virtualized hosts. When the service is running, it can push out update images, eliminating patching and update without impacting production. Proposed solution should allow live patching of select critcal security patches.	Virtualization manager should allow addition of new nodes and patching/upgrade of hypervisor running on the node without any VM downtime.
1350		Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 22	Unlimited VM replication from DC to DR (No restriction on VM replication and DR orchestration) with the capability to define Recovery Plans		Unlimted is open terms, request you to provide the number of VMs to orchestrated for automated recovery. As unlimited is relevant for one specific vendor . The VMs to be protected/orchestrated are limited to what can be provisioned on these 14 servers of production.	Request BoB cards to Clarify the need for Recovery Plans- We do provide unlimited Replication from DC to DR which is orchestrated. In Terms of Recovery Plans (which is automation) We request bank to consider defining specific number of Virtual Machines. Its however best to use extends the existing DR orchestration solution fot this environment as well.	No Change, can not predict the exact number of VMs for next 5 Years which need to be replicated.
1351		Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 23	Proposed solution should have a self-service restore feature on a per-VM basis to allow trusted application administrators to recover their own files with the ability to mount snapshots as a drive in Windows VMs		Please clarify this requirement, this looks like back and restore requirements	Proposed solution should have a self-service restore feature on a per-VM basis to allow trusted application administrators to recover their own VMs from the snapshot	This will help BOBCARD to recover file without losing current state of virtual machine.
1352		Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 24	Hypervisor should provide Visibility for Running VM and their connectivity co-relationship with Network Ports on attached Physical TOR / Core Direct which Include Network RX/TX Bytes.		Monitoring is not considering all components of the stack. Unless end to end visibility is provided as part of this solution BoB Card has to spend separately on monitoring.	Hypervisor should provide Visibility for Running VM and their connectivity co-relationship with Network Ports on attached Physical TOR / Core Direct which Include Network RX/TX Bytes.Solution Should provide end to end visibility across physical firewall, switch and storage, Flow Analysis and Security Planning,Guided Troubleshooting, Microsegmentation planning, RCA (Connectivity Problem, Packet Loss, N/W latency), Application Discovery, Service Monitoring , Application Dependency Mapping and monitoring of non compliant ports	Yes, BOBCARD will take care such requirement. However Hypervisor should provide Visibility for Running VM and their connectivity co-relationship with Network Ports on attached Physical Port which Include Network RX/TX Bytes.
1353		Appendix01 Techno Functional Requirements- Server and Virtual platform > Hypervisor > 30	Virtualization software or the solution should provide Cluster level encryption protects unauthorized data access at-rest.		Having capability to do the enscryption at app VM level and in transit is required to complete solution.	Virtualization software or the solution should provide Cluster level, VM Level encryption protects unauthorized data access at-rest and in transit.	No Change, additional feature will be consider as value add
1354		Appendix01 Techno Functional Requirements- Server and Virtual platform > Software Defined Storage > 1	Maintain primary working set copy of active data on the Local Node as VM's are hosted to provide high IOPS and low latency. Proposed solution must be proposed for faster reads and write for Business-critical Apps.		Architecture is specific to one vendor, request BoB Cards to consider on outcome than specific architecture. There is no specific latency requirements mentioned in the spec.	Proposed solution must be proposed for faster reads and write for Business-critical Apps.	No Change
1355		Appendix01 Techno Functional Requirements- Server and Virtual platform > Software Defined Storage >2	The solution must have De-duplication and Compression features licensed and implemented from day one (Should not have dependency on any proprietary hardware device).		Solution should have flexibility to implement either compression and de-duplication. BoB Cards should conisder overhead while deciding on both.	The solution must have De-duplication/Compression features licensed and implemented from day one (Should not have dependency on any proprietary hardware device).	No Change
1356		Appendix01 Techno Functional Requirements- Server and Virtual platform > Software Defined Storage >24	The proposed solution should support 1 min RPO & 1 hour RTO for critical workload in case BOB Cards wants to have this capability replication for Future use. The proposed solution should have native Replication and DR Orchestration from Day-1		What is the use case for 1 min RPO and 1 Hour RTO? is this linked with some regulatory requirement? Replication is best handled at application level as having additional solution for infrastructure will complexity and cost for BoB Cards Its best to use extends the existing DR orchestration solution for this environment as well.	What is the use case for 1 min RPO and 1 Hour RTO? is this linked with some regulatory requirement? Replication is best handled at application level as having additional solution for infrastructure will complexity and cost for BoB Cards Its best to use extends the existing DR orchestration solution for this environment as well.	This is required for BOBCARD mission critical application. The solution should capable to support 1min RPO. The propose replication solution should be same OEM as the virtualization solution to provide seamless integration.

1357		Appendix01 Techno Functional Requirements- Server and Virtual platform > Software Defined Storage >25	The solution provided should function even after one node failure.	RFP asks for 99.99 % availability SLA for the proposed solution. It will require minimum N+2 configuration for required resiliency and uptime.	The solution provided should function even after two node failure.	No Change, additional feature will be consider as value add
1358		Appendix01 Techno Functional Requirements- Server and Virtual platform > Software Defined Storage >31	The solution should provide enterprise data services such as compression completely in software. Software Defined Storage solution must have de-duplication and compression features Licensed and implemented from day one. These functionalities should be part of the proposed solution. The solution must have functionality to support compression and or deduplication online on data container without any downtime and data loss as per business requirement.	Solution should have flexibility to implement either compression and de-duplication. BoB Cards should conisder overhead while deciding on both.	The solution should provide enterprise data services such as compression completely in software. Software Defined Storage solution must have de-duplication or compression features Licensed and implemented from day one. These functionalities should be part of the proposed solution. The solution must have functionality to support compression and or deduplication online on data container without any downtime and data loss as per business requirement.	No Change
1359		Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmentation > new point	New Point	IP/MAC spoofing is major security concern for organizations like BoB Cards handing customers data.	The solution must ensure that there is not alteration in the IP address of the Virtual machine, by blocking the traffic from or to the VM inherited as a feature in the Solution.	No Change
1360		Appendix01 Techno Functional Requirements- Server and Virtual platform > Microsegmentation > new point		VPC will enable Bob Cards to create isolation from access , resources, network and security.	The solution should support multi-tenancy to isolate networking/security for different departments/function within BoB Cards upto a minimum of 4 tenants and 5 VPCs	No Change, additional feature will be consider as value add
1361		Appendix01 Techno Functional Requirements- Server and Virtual platform > Container > 6	Should support cluster scale out i.e addition of worker nodes as and when required.	Complete Automation is not possible without Auto Scaling and Auto Healing of Kubernetes Clusters. One has to manually add nodes in case of failure or unprovisioned increase in load.	Should support Automated cluster scale out i.e addition of worker nodes as and when required.	No Change
1362		Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > 3	The solution shall provide a single pane of glass for automated provisioning with model-based orchestration of compute, network and storage through a unified multi-tenant self-service catalog.	All modern applications are combination of both container and VM form factor.	The solution shall provide a single pane of glass for automated provisioning with model-based orchestration of compute, network , storage and Kubernetes through a unified multi-tenant self-service catalog .	No Change, additional feature will be consider as value add
1363		Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > 5	The solution must provide a self-service portal to allow user to consume the creation of infrastructure easily.	All modern applications are combination of both container and VM form factor.	The solution must provide a self-service portal to allow user to consume the creation of infrastructure easily for both VM and Kubernetes.	No Change, additional feature will be consider as value add
1364		Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > 8	The software must allow the designer to use shell script, PowerShell script to code the automation.	Python and nodeJs are very popular language for scrpting in terms resource availability and community support	The software must allow the designer to use shell script, PowerShell script, Python and node JS to code the automation.	No Change, additional scripting will be value add
1365		Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > 9	The software must allow the designer to design VM blueprints.	All modern applications are combination of both container and VM form factor.	The software must allow the designer to design Multi VM & Kubernetes blueprints.	No Change, additional feature will be consider as value add
1366		Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > 12	The solution should have simple low-code, no-code automation engine which allows automating day-to-day routine tasks	All modern applications are combination of both container and VM form factor.	The solution should have simple low-code, no-code automation engine which allows automating day-to-day routine tasks such as Snapshot creation, Addition of Disk, Power Cycle (Suspend , Shutdown, Reboot, reset), Resize, Rebuild, Additional of Network, VM Unregister , Delete,connect remote console, Change Security Group with capability to create additional resource actions as out of the box capability.	No Change, additional feature will be consider as value add
1367		Appendix01 Techno Functional Requirements- Server and Virtual platform > Cloud Management > New Point	New Point	eed Cost transparency (Showback and Chargeback capability) across private, hybrid to optimize planning and pr	Solution should provide capability to define and showcase cost to create cloud like experience to the business unit with the overall cost spend on the infrastructure [server hardware, storage, licenses, application, maintenance, labor, network, facilities , etc.	No Change, additional feature will be consider as value add

1368		Appendix02 Techno Functional Requirements- Network components > LB/WAF & IPS	New Point		Modern applications increasingly require software-defined networking (SDN) and security solutions due to their need for greater flexibility, agility, and scalability. Traditional networking and security methods often lack the adaptability to support the dynamic nature of modern application environments, especially in cloud	We request BoB Card to allow for both software and hardware based solution for Load Balancer, WAF, IPS/IDS. As these components are dynamic as per application consumption requirements and considering bob card is directly managing customer data, its very critcal that these components are added as part of sofwate defined stack.	No Change
1369	31-32	8 Payment Terms	Please refer Sheet 2		N/A	Request you to kindly change the payment terms as below: Supply of Servers & Network component as prescribed under hardware requiremen- Delivery - 70% of Total Cost of Equipment outlined in BOM Sign Off - 30% of Total Cost of Equipment outlined in BOM Support for the day-to-day operations -100% Yearly advance on yearly basis	No Change
1370	42-43	Liquidated Damages and penalty	The maximum amount that may be levied by way of penalty pursuant to clause above shall not exceed 10% of the Total Contract value.		N/A	Request you to kindly consider & modfie the point as per below - The maximum amount that may be levied by way of penalty pursuant to clause above shall not exceed 5% of the Total Contract value.	The maximum amount that may be levied by way of penalty pursuant to clause above shall not exceed 5% of the Total Contract value. All clauses remain same
1371		Annexure 1- Eligibility Criteria	Bidder should have experience of minimum 3 years in providing the Proposed Products/Services mentioned in the RFP.		N/A	Request you to kindly consider & modfie the point as per below - Bidder/OEM should have experience of minimum 3 years in providing the Proposed Products/Services mentioned in the RFP.	The maximum amount that may be levied by way of penalty pursuant to clause above shall not exceed 5% of the Total Contract value. All clauses remain same