पंजाब एण्ड सिंध बैंक *(भारत सरकार का उपक्रम)* ***प्रधान कार्यालय : सूचना प्रौद्योगिकी विभाग,*** ***द्वितीय तल, भूखंड संख्या-151,*** ***सेक्टर-44, संस्थागत क्षेत्र,*** ***गुरुग्राम– 122003*** *Email: ho.it@psb.bank.in*		***Punjab & Sind Bank*** *(A Govt. Of India Undertaking)* ***H.O. Information Technology Dept.,*** ***2nd Floor, Plot No. 151,*** ***Sector -44, Institutional Area,*** ***Gurugram - 122003*** *Email: ho.it@psb.bank.in*

Addendum 1
DATED 14-09-2026

FOR

SELECTION OF BIDDER FOR SUPPLY INSTALLATION, IMPLEMENTATION, MAINTENANCE & MANAGEMENT OF IT SECURITY SOLUTION & SERVICES

BID NO: PSB/HOIT/RFP/53/2026-27 dated 19/08/2026
GEM BID No. GEM/2026/B/7936763

Punjab & Sind Bank
Second Floor
IT Department
Plot Number 151, Sector 44,
Gurugram, 122003

पंजाब एण्ड सिंध बैंक
(भारत सरकार का उपक्रम)
प्रधान कार्यालय: सूचना प्रौद्योगिकी विभाग,
द्वितीय तल, भूखंड संख्या-151,
सेक्टर-44, संस्थागत क्षेत्र,
गुरुग्राम– 122003
Email: ho.it@psb.bank.in

Punjab & Sind Bank
(A Govt. Of India Undertaking)
H.O. Information Technology Dept.,
2nd Floor, Plot No. 151,
Sector -44, Institutional Area,
Gurugram - 122003
Email: ho.it@psb.bank.in

Addendum 1

Introduction

Bank has published the RFP vide tender No: BID NO: PSB/HOIT/RFP/53/2026-27 dated 19/08/2026 for SELECTION OF BIDDER FOR SUPPLY INSTALLATION, IMPLEMENTATION, MAINTENANCE & MANAGEMENT OF IT SECURITY SOLUTION & SERVICES.

Following amendments have been made in the above stated RFP. All other terms and conditions of the RFP shall remain unchanged. Please treat this Addendum as an integral part of the RFP documents issued.

With reference to the aforesaid RFP, all are advised to note following:

Section 1: Modification in RFP Dates:

S.No.	Pg No.	RFP Section	Original Date	Revised Date
1.	RFP Page No. 8	**Key Information:** Last Date and Time for submission of Bids	16th September 2026, 3pm	28th September 2026, 3pm
1.	RFP Page No. 8	**Key Information:** Date and Time of Opening of Bids	16th September 2026, 3:30pm	28th September 2026, 3:30pm

पंजाब एण्ड सिंध बैंक *(भारत सरकार का उपक्रम)* ***प्रधान कार्यालय: सूचना प्रौद्योगिकी विभाग,*** ***द्वितीय तल, भूखंड संख्या-151,*** ***सेक्टर-44, संस्थागत क्षेत्र,*** ***गुरुग्राम– 122003*** *Email: ho.it@psb.bank.in*		***Punjab & Sind Bank*** *(A Govt. Of India Undertaking)* ***H.O. Information Technology Dept.,*** ***2nd Floor, Plot No. 151,*** ***Sector -44, Institutional Area,*** ***Gurugram - 122003*** *Email: ho.it@psb.bank.in*

Addendum 1

Section 2: Modification in RFP Clauses:

S. No.	RFP Section no.	RFP Page No.	RFP Clause			Modified Clause		
1.	7.1, IT Security Solution and Services, E. Management layer Security	31	**Solution Name**	**Use Case**	**Deployment Model**	**Solution Name**	**Use Case**	**Deployment Model**
			AI Security	To securely govern, monitor, and control enterprise AI/Generative AI usage by providing AI gateway, prompt inspection, data leakage prevention, AI firewall, model access control, guardrails, prompt injection protection, model risk management, and centralized policy enforcement for all AI services and enterprise LLMs.	On-Premises at DC & DR	AI Security	To securely govern, monitor, and control enterprise AI/Generative AI usage by providing AI gateway, prompt inspection, data leakage prevention, AI firewall, model access control, guardrails, prompt injection protection, model risk management, and centralized policy enforcement for all AI services and enterprise LLMs.	• Data Plane -- At Bank's DC and Bank's DR ; AI Security - Any component processing actual Bank/ AI

पंजाब एण्ड सिंध बैंक *(भारत सरकार का उपक्रम)* ***प्रधान कार्यालय: सूचना प्रौद्योगिकी विभाग,*** ***द्वितीय तल, भूखंड संख्या-151,*** ***सेक्टर-44, संस्थागत क्षेत्र,*** ***गुरुग्राम– 122003*** *Email: ho.it@psb.bank.in*		***Punjab & Sind Bank*** *(A Govt. Of India Undertaking)* ***H.O. Information Technology Dept.,*** ***2nd Floor, Plot No. 151,*** ***Sector -44, Institutional Area,*** ***Gurugram - 122003*** *Email: ho.it@psb.bank.in*

Addendum 1

S. No.	RFP Section no.	RFP Page No.	RFP Clause	Modified Clause
				content for Private AI communication; HA (N+N Active Active, Active/Passive) • Management Plane -- Standalone Deplo

पंजाब एण्ड सिंध बैंक *(भारत सरकार का उपक्रम)* ***प्रधान कार्यालय: सूचना प्रौद्योगिकी विभाग,*** ***द्वितीय तल, भूखंड संख्या-151,*** ***सेक्टर-44, संस्थागत क्षेत्र,*** ***गुरुग्राम– 122003*** *Email: ho.it@psb.bank.in*		***Punjab & Sind Bank*** *(A Govt. Of India Undertaking)* ***H.O. Information Technology Dept.,*** ***2nd Floor, Plot No. 151,*** ***Sector -44, Institutional Area,*** ***Gurugram - 122003*** *Email: ho.it@psb.bank.in*

Addendum 1

S. No.	RFP Section no.	RFP Page No.	RFP Clause	Modified Clause
				ymen t at Bank' s DC / Bank' s DR or Vend or/Cl oud hoste d in India In case of vendor/cloud hosted bidder should comply with cloud security requirement
2.	7.2.1.2,	48	The Bank intends to upgrade its existing Privileged Identity Management (PIM) solution to enhance control and security	The bidder may propose either upgradation of the incumbent PIM solution or replacement with a new PIM solution, based on its

पंजाब एण्ड सिंध बैंक *(भारत सरकार का उपक्रम)* ***प्रधान कार्यालय: सूचना प्रौद्योगिकी विभाग,*** ***द्वितीय तल, भूखंड संख्या-151,*** ***सेक्टर-44, संस्थागत क्षेत्र,*** ***गुरुग्राम– 122003*** *Email: ho.it@psb.bank.in*		***Punjab & Sind Bank*** *(A Govt. Of India Undertaking)* ***H.O. Information Technology Dept.,*** ***2nd Floor, Plot No. 151,*** ***Sector -44, Institutional Area,*** ***Gurugram - 122003*** *Email: ho.it@psb.bank.in*

Addendum 1

S. No.	RFP Section no.	RFP Page No.	RFP Clause	Modified Clause
	Privilege Identity Management (PIM)		over privileged access across its critical IT infrastructure and enterprise applications. The upgraded solution must provide comprehensive privileged account management, including secure credential storage (password vaulting), real-time session monitoring, granular access control, and detailed audit trails to meet regulatory and internal compliance requirements. The objective is to enforce least privilege access, enhance visibility, and ensure accountability of privileged activities across the Bank's IT ecosystem, helping to mitigate insider threats and prevent misuse of elevated privileges.	proposed solution architecture and design. However, compliance with the complete Functional Specification and all other applicable requirements of the RFP is mandatory, irrespective of whether the incumbent solution or a replacement solution is proposed. The bidder shall factor all required licenses, migration, integration, implementation, configuration and associated activities within its scope. The proposed solution must provide comprehensive privileged account management, including secure credential storage (password vaulting), real-time session monitoring, granular access control, and detailed audit trails to meet regulatory and internal compliance requirements. The objective is to enforce least privilege access, enhance visibility, and ensure accountability of privileged activities across the Bank's IT ecosystem, helping to mitigate insider threats and prevent misuse of elevated privileges
3.	7.3.1.5, Zero-Day Attack Protection at Endpoin	38	Fully deployed Zero-Day Attack Protection at Endpoint and network solution covering both network and endpoint layers	Fully deployed Zero-Day Attack Protection for the entire network

पंजाब एण्ड सिंध बैंक *(भारत सरकार का उपक्रम)* ***प्रधान कार्यालय: सूचना प्रौद्योगिकी विभाग,*** ***द्वितीय तल, भूखंड संख्या-151,*** ***सेक्टर-44, संस्थागत क्षेत्र,*** ***गुरुग्राम– 122003*** *Email: ho.it@psb.bank.in*		***Punjab & Sind Bank*** *(A Govt. Of India Undertaking)* ***H.O. Information Technology Dept.,*** ***2nd Floor, Plot No. 151,*** ***Sector -44, Institutional Area,*** ***Gurugram - 122003*** *Email: ho.it@psb.bank.in*

Addendum 1

S. No.	RFP Section no.	RFP Page No.	RFP Clause	Modified Clause
	t and network – Key Deliverables			
4.	7.3.1.5, Zero-Day Attack Protection at Endpoint and network – Key Deliverables	38	Incident response plan including rapid action and forensics procedures	Clause stands deleted
5.	7.5.8, Training	62	Training Type / Duration per Session / Minimum Number of Sessions Beginner / Foundation Training — 2 Days — 5 Sessions Advanced / Administrator Training — 3 Days — 5 Sessions	Training Type / Duration per Session / Minimum Number of Sessions Beginner / Foundation Training — 1 Day — 1 Session Advanced / Administrator Training — 1 Day — 1 Session

पंजाब एण्ड सिंध बैंक *(भारत सरकार का उपक्रम)* ***प्रधान कार्यालय: सूचना प्रौद्योगिकी विभाग,*** ***द्वितीय तल, भूखंड संख्या-151,*** ***सेक्टर-44, संस्थागत क्षेत्र,*** ***गुरुग्राम– 122003*** *Email: ho.it@psb.bank.in*	पंजाब एण्ड सिंध बैंक (भारत सरकार का उपक्रम)	***Punjab & Sind Bank*** *(A Govt. Of India Undertaking)* ***H.O. Information Technology Dept.,*** ***2nd Floor, Plot No. 151,*** ***Sector -44, Institutional Area,*** ***Gurugram - 122003*** *Email: ho.it@psb.bank.in*

Addendum 1

<table>
<tr><th>S. No.</th><th>RFP Section no.</th><th>RFP Page No.</th><th>RFP Clause</th><th>Modified Clause</th></tr>
<tr><td></td><td></td><td></td><td>Backend Administration, Troubleshooting & Maintenance Training 3 Days 5 Sessions</td><td>Backend Administration, Troubleshooting & Maintenance Training 1 Day 1 Session</td></tr>
<tr><td>6.</td><td>7.11, Resource Requirement (Security Layer table)</td><td>74</td><td>
<table>
<tr><td>Security Layer</td><td>Solutions</td><td>Shift A – L1</td><td>Shift A – L2</td><td>Shift B – L1</td><td>Shift B – L2</td><td>Shift C – L1</td><td>Shift C – L2</td><td>Shift A – L3</td></tr>
<tr><td>Perimeter & Network Security</td><td>6</td><td>0</td><td>0</td><td>1</td><td>1</td><td>1</td><td>1</td><td rowspan="4">1</td></tr>
<tr><td>Endpoint Security</td><td>3</td><td rowspan="2">1</td><td rowspan="2">1</td><td>0</td><td rowspan="2">1</td><td>0</td><td rowspan="2">1</td></tr>
<tr><td>Data Security</td><td>2</td><td>0</td><td>0</td></tr>
<tr><td>Application AND</td><td>9</td><td>1</td><td>1</td><td>2</td><td>2</td><td>1</td><td>0</td></tr>
</table>
</td><td>
<table>
<tr><td>Security Layer</td><td>Solutions</td><td>Shift A – L1</td><td>Shift A – L2</td><td>Shift B – L1</td><td>Shift B – L2</td><td>Shift C – L1</td><td>Shift C – L2</td><td>Shift A – L3</td></tr>
<tr><td>Perimeter & Network Security</td><td>6</td><td>0</td><td>0</td><td>1</td><td>1</td><td>1</td><td>1</td><td rowspan="4">1</td></tr>
<tr><td>Endpoint Security</td><td>3</td><td rowspan="2">1</td><td rowspan="2">1</td><td>0</td><td rowspan="2">1</td><td>0</td><td rowspan="2">1</td></tr>
<tr><td>Data Security</td><td>2</td><td>0</td><td>0</td></tr>
<tr><td>Application AND</td><td>10</td><td>1</td><td>1</td><td>2</td><td>2</td><td>1</td><td>0</td></tr>
</table>
</td></tr>
</table>

पंजाब एण्ड सिंध बैंक *(भारत सरकार का उपक्रम)* ***प्रधान कार्यालय: सूचना प्रौद्योगिकी विभाग,*** ***द्वितीय तल, भूखंड संख्या-151,*** ***सेक्टर-44, संस्थागत क्षेत्र,*** ***गुरुग्राम– 122003*** *Email: ho.it@psb.bank.in*		***Punjab & Sind Bank*** *(A Govt. Of India Undertaking)* ***H.O. Information Technology Dept.,*** ***2nd Floor, Plot No. 151,*** ***Sector -44, Institutional Area,*** ***Gurugram - 122003*** *Email: ho.it@psb.bank.in*

Addendum 1

S. No.	RFP Section no.	RFP Page No.	RFP Clause	Modified Clause
			Management layer Security Total: 20 (3, 3, 2, 3, 2, 2, 1)	Management layer Security Total: 21 (3, 3, 2, 3, 2, 2, 1)
7.	7.11 Resource Requirement		**# / Resource Type / Deployment / Minimum Qualification & Experience** **Implementation Phase** **1** Project Manager – Implementation — Onsite – as per Bank's timings/ Shift Timings (Full Time) — • Graduate/B.E./B.Tech/MCA with PMP/PRINCE2 or equivalent certification. • Minimum 8 years of experience • Proven experience in managing at least two Security Solution implementations (including at least one Perimeter Security solution) in PSU/PSE/Government/BF	**# / Resource Type / Deployment / Minimum Qualification & Experience** **Implementation Phase** **1** Project Manager – Implementation — Onsite – as per Bank's timings/ Shift Timings (Full Time) — • Graduate/B.E./B.Tech/MCA with PMP/PRINCE2 or equivalent certification. • Minimum 8 years of experience • Proven experience in managing at least two Security Solution implementations (including at least one Perimeter Security solution) in PSU/PSE/Government/BFSI/Regulatory organizations. **2** OEM Implem — Onsite – as — OEM shall submit a detailed resource deployment plan before

पंजाब एण्ड सिंध बैंक *(भारत सरकार का उपक्रम)* ***प्रधान कार्यालय: सूचना प्रौद्योगिकी विभाग,*** ***द्वितीय तल, भूखंड संख्या-151,*** ***सेक्टर-44, संस्थागत क्षेत्र,*** ***गुरुग्राम– 122003*** *Email: ho.it@psb.bank.in*		***Punjab & Sind Bank*** *(A Govt. Of India Undertaking)* ***H.O. Information Technology Dept.,*** ***2nd Floor, Plot No. 151,*** ***Sector -44, Institutional Area,*** ***Gurugram - 122003*** *Email: ho.it@psb.bank.in*

Addendum 1

S. No.	RFP Section no.	RFP Page No.	RFP Clause				Modified Clause			
						SI/Regulatory organizations.				
			2	OEM Implementation Resources	Onsite – as per Bank's timings/ Shift Timings (Full Time)	OEM shall submit a detailed resource deployment plan before commencement of requirement gathering. Any replacement or modification shall require prior Bank approval.		ntation Resources	per Bank's timings/ Shift Timings (Full Time)	commencement of requirement gathering. Any replacement or modification shall require prior Bank approval.
			3	Bidder Implementation Resources	Onsite – as per Bank's timings/ Shift Timings	Bidder shall submit a detailed resource deployment plan before commencement of requirement gathering. Any replacement or modification shall require prior Bank approval.		3 Bidder Implementation Resources	Onsite – as per Bank's timings/ Shift Timings (Full Time)	Bidder shall submit a detailed resource deployment plan before commencement of requirement gathering. Any replacement or modification shall require prior Bank approval.
								Operations & Maintenance (O&M) Phase		
								4 L1 Security Resources	Onsite – as per Bank's timing	• Graduate/B.E./B.Tech/MCA with minimum 2 years of experience. • Minimum one OEM security certifications or equivalent

पंजाब एण्ड सिंध बैंक *(भारत सरकार का उपक्रम)* ***प्रधान कार्यालय: सूचना प्रौद्योगिकी विभाग,*** ***द्वितीय तल, भूखंड संख्या-151,*** ***सेक्टर-44, संस्थागत क्षेत्र,*** ***गुरुग्राम– 122003*** *Email: ho.it@psb.bank.in*		***Punjab & Sind Bank*** *(A Govt. Of India Undertaking)* ***H.O. Information Technology Dept.,*** ***2nd Floor, Plot No. 151,*** ***Sector -44, Institutional Area,*** ***Gurugram - 122003*** *Email: ho.it@psb.bank.in*

Addendum 1

S. No.	RFP Section no.	RFP Page No.	RFP Clause				Modified Clause			
					(Full Time)				s/ Shift Timings (Full Time)	certifications such as CEH, Security+, etc. • Experience in managing at least one IT Security solution.
			Operations & Maintenance (O&M) Phase							
			4	L1 Security Resources	Onsite – as per Bank's timings/ Shift Timings (Full Time)	• Graduate/B.E./B.Tech/MCA with minimum 2 years of experience. • Minimum one OEM security certifications or equivalent certifications such as CEH, Security+, etc. • Experience in managing at least one IT Security solution in PSU/PSE/Government/BFSI/Regulatory organizations.	**5**	L2 Security Resources	Onsite – as per Bank's timings/ Shift Timings (Full Time)	• Graduate/B.E./B.Tech. /MCA with minimum 5 years of experience. • Minimum two OEM security certifications or equivalent certifications such as CEH, CISA, etc. • Experience in managing at least one IT Security solution.
			5	L2 Security Resources	Onsite – as per Bank's timings/ Shift Timings (Full Time)	• Graduate/B.E./B.Tech. /MCA with minimum 5 years of experience. • Minimum two OEM security certifications or	**6**	L3/ Project Manager – Operations	Onsite – as per Bank's timings/ Shift Timings (Full Time)	• Graduate/B.E./B.Tech. /MCA with PMP/PRINCE2 or equivalent certification. • Minimum 8 years of experience in IT Security operations and management. • Experience in managing at least three IT Security solution implementation

पंजाब एण्ड सिंध बैंक *(भारत सरकार का उपक्रम)* ***प्रधान कार्यालय: सूचना प्रौद्योगिकी विभाग,*** ***द्वितीय तल, भूखंड संख्या-151,*** ***सेक्टर-44, संस्थागत क्षेत्र,*** ***गुरुग्राम– 122003*** *Email: ho.it@psb.bank.in*		***Punjab & Sind Bank*** *(A Govt. Of India Undertaking)* ***H.O. Information Technology Dept.,*** ***2nd Floor, Plot No. 151,*** ***Sector -44, Institutional Area,*** ***Gurugram - 122003*** *Email: ho.it@psb.bank.in*

Addendum 1

S. No.	RFP Section no.	RFP Page No.	RFP Clause				Modified Clause			
					timings/ Shift Timings (Full Time)	equivalent certifications such as CEH, CISA, etc. • Experience in managing at least one IT Security solution in PSU/PSE/Government/BFSI/Regulatory organizations.			and/or operations engagements in PSU/PSE/ Government/BFSI/ Regulatory organizations.
			6	L3/ Project Manager – Operations	Onsite – as per Bank's timings/ Shift Timings (Full Time)	• Graduate/B.E./B.Tech. /MCA with PMP/PRINCE2 or equivalent certification. • Minimum 8 years of experience in IT Security operations and management. • Experience in managing at least three IT Security solution implementation and/or operations engagements in PSU/PSE/ Government/BFSI/ Regulatory organizations.	**IT Infrastructure Resources**			
			IT Infrastructure Resources				**7**	L1 IT Infrastructure Resources	Onsite – as per Bank's timings / Shift Timings (Full Time)	• Graduate or equivalent. • Minimum 2 years of experience in IT Infrastructure operations. • Experience in managing at least one IT Infrastructure solution.
							8	L2 IT Infrastructure Resources	Onsite – as per Bank's timings / Shift Timing	• Graduate or equivalent. • Minimum 3 years of experience in IT Infrastructure operations. Experience in managing at least two IT Infrastructure solution.

पंजाब एण्ड सिंध बैंक *(भारत सरकार का उपक्रम)* ***प्रधान कार्यालय: सूचना प्रौद्योगिकी विभाग,*** ***द्वितीय तल, भूखंड संख्या-151,*** ***सेक्टर-44, संस्थागत क्षेत्र,*** ***गुरुग्राम– 122003*** *Email: ho.it@psb.bank.in*	पंजाब एण्ड सिंध बैंक (भारत सरकार का उपक्रम) जहाँ सेवा ही जीवन - ध्येय है	***Punjab & Sind Bank*** *(A Govt. Of India Undertaking)* ***H.O. Information Technology Dept.,*** ***2nd Floor, Plot No. 151,*** ***Sector -44, Institutional Area,*** ***Gurugram - 122003*** *Email: ho.it@psb.bank.in*

Addendum 1

S. No.	RFP Section no.	RFP Page No.	RFP Clause				Modified Clause			
			7	L1 IT Infrastructure Resources	Onsite – as per Bank's timings / Shift Timings (Full Time)	• Graduate or equivalent. • Minimum 2 years of experience in IT Infrastructure operations. • Experience in managing at least one IT Infrastructure solution in PSU/PSE/Government/BFSI/Regulatory organizations.			s (Full Time)	
			8	L2 IT Infrastructure Resources	Onsite – as per Bank's timings / Shift Timings (Full Time)	• Graduate or equivalent. • Minimum 3 years of experience in IT Infrastructure operations. Experience in managing at least two IT Infrastructure solution in PSU/PSE/Government/BFSI/Regulatory organizations.				

पंजाब एण्ड सिंध बैंक *(भारत सरकार का उपक्रम)* ***प्रधान कार्यालय: सूचना प्रौद्योगिकी विभाग,*** ***द्वितीय तल, भूखंड संख्या-151,*** ***सेक्टर-44, संस्थागत क्षेत्र,*** ***गुरुग्राम– 122003*** *Email: ho.it@psb.bank.in*		***Punjab & Sind Bank*** *(A Govt. Of India Undertaking)* ***H.O. Information Technology Dept.,*** ***2nd Floor, Plot No. 151,*** ***Sector -44, Institutional Area,*** ***Gurugram - 122003*** *Email: ho.it@psb.bank.in*

Addendum 1

S. No.	RFP Section no.	RFP Page No.	RFP Clause	Modified Clause
8.	8, Contract Period		The Bidder is required to sign the contract within 15 days from the date of acceptance of the Purchase Order.	Bidder to submit duly signed Contract, NDA, SLA and other documents required under the RFP within the 21 days of PO Acceptance. Failure to execute or submit such documents within the stipulated period shall entitle the Bank to take action in accordance with the RFP, including forfeiture of EMD and/or cancellation of the Purchase Order/award, or any other as applicable. Effective start date for the contract would be date of acceptance of the PO
9.	10.1, Eligibility Criteria, Preliminary Scrutiny		During evaluation of the Tenders, the Bank, at its discretion, may ask the Bidder for clarification in respect of its tender. The request for clarification and the response shall be in writing, and no change in the substance of the tender shall be sought, offered, or permitted. The Bank reserves the right to accept or reject any tender in whole or in part without assigning any reason thereof. The decision of the Bank shall be final and binding on all the bidders to this document and the bank will not entertain any correspondence in this regard. Bidders are therefore advised to ensure that all required documents and supporting evidence are submitted along with the bid. The Bank shall evaluate the bid based on the documents submitted and the Bank's decision regarding the adequacy, relevance, interpretation, compliance, and evaluation of the	During evaluation of the Tenders, the Bank, at its discretion, may ask the Bidder for clarification in respect of its tender. The request for clarification and the response shall be in writing, and no change in the substance of the tender shall be sought, offered, or permitted. The Bank reserves the right to accept or reject any tender in whole or in part without assigning any reason thereof. The decision of the Bank shall be final and binding on all the bidders to this document and the bank will not entertain any correspondence in this regard. The evaluation of bids shall be based on the documents, credentials, experience references, and information submitted by the bidder as part of its bid response on or before the bid submission deadline. Any new credential, experience reference, document, or supporting evidence that was not originally

पंजाब एण्ड सिंध बैंक *(भारत सरकार का उपक्रम)* ***प्रधान कार्यालय: सूचना प्रौद्योगिकी विभाग,*** ***द्वितीय तल, भूखंड संख्या-151,*** ***सेक्टर-44, संस्थागत क्षेत्र,*** ***गुरुग्राम– 122003*** *Email: ho.it@psb.bank.in*		***Punjab & Sind Bank*** *(A Govt. Of India Undertaking)* ***H.O. Information Technology Dept.,*** ***2nd Floor, Plot No. 151,*** ***Sector -44, Institutional Area,*** ***Gurugram - 122003*** *Email: ho.it@psb.bank.in*

Addendum 1

S. No.	RFP Section no.	RFP Page No.	RFP Clause	Modified Clause
			submitted documents and information shall be final, conclusive, and binding on all bidders.	submitted with the bid may, at the Bank's discretion, not be accepted or considered during the evaluation process. Bidders are therefore advised to ensure that all required documents and supporting evidence are submitted along with the bid. The Bank shall evaluate the bid based on the documents submitted and the Bank's decision regarding the adequacy, relevance, interpretation, compliance, and evaluation of the submitted documents and information shall be final, conclusive, and binding on all bidders.
10.	10.2, Eligibility Evaluation Criteria, Point 4	100	The bidder should have a minimum average annual turnover of INR 1000 crore in India during the last 3 financial years (i.e. 2022-23, 2023-24 & 2024–25) along with positive net worth.	The bidder should have a minimum average annual turnover of INR 500 crore in India during the last 3 financial years (i.e. 2022-23, 2023-24 & 2024–25) along with positive net worth.
11.	10.2, Eligibility Evaluation Criteria, Point 6	101	Bidder must have at least enrolled manpower (on bidder's payroll) of 150 experienced employees skilled in areas of Cyber/IT security.	Bidder must have at least enrolled manpower (on bidder's payroll) of 100 experienced employees skilled in areas of Cyber/IT security.

पंजाब एण्ड सिंध बैंक *(भारत सरकार का उपक्रम)* ***प्रधान कार्यालय: सूचना प्रौद्योगिकी विभाग,*** ***द्वितीय तल, भूखंड संख्या-151,*** ***सेक्टर-44, संस्थागत क्षेत्र,*** ***गुरुग्राम– 122003*** *Email: ho.it@psb.bank.in*		***Punjab & Sind Bank*** *(A Govt. Of India Undertaking)* ***H.O. Information Technology Dept.,*** ***2nd Floor, Plot No. 151,*** ***Sector -44, Institutional Area,*** ***Gurugram - 122003*** *Email: ho.it@psb.bank.in*

Addendum 1

S. No.	RFP Section no.	RFP Page No.	RFP Clause	Modified Clause
12.	13.14 Make in India	140	The policy of the Govt. of India to encourage "Make in India" and promote manufacturing and production of goods and services in India, "Public Procurement (Preference to Make in India), Order 2017 and the revised order issued vide GOI, Ministry of Commerce and Industry, Department for Promotion of Industry and Internal trade, vide Order No. P-45021/2/2017-PP (BE-II) dated 19th July 2024 subsequent amendments. The local supplier at the time of submission of bid shall be required to provide a certificate as per Annexure 7 from the statutory auditor or cost auditor of the company (in the case of companies) or from a practicing cost accountant or practicing chartered accountant (in respect of suppliers other than companies) giving the percentage of local content. The Bank shall follow all the guidelines/ notifications for public procurement.	The policy of the Govt. of India to encourage "Make in India" and promote manufacturing and production of goods and services in India, "Public Procurement (Preference to Make in India), Order 2017 and the revised order issued vide GOI, Ministry of Commerce and Industry, Department for Promotion of Industry and Internal trade, vide Order No. P-45021/2/2017-PP (BE-II) dated 19th July 2024 subsequent amendments. The local supplier at the time of submission of bid shall be required to provide a certificate as per Annexure 7 from the statutory auditor or cost auditor of the company (in the case of companies) or from a practicing cost accountant or practicing chartered accountant (in respect of suppliers other than companies) giving the percentage of local content. The Bank shall follow all the guidelines/ notifications for public procurement. 1. The minimum average annual financial turnover of the bidder during the last three years, ending on 31st March of the previous financial year, should be as indicated above in the bid document. Documentary evidence in the form of certified Audited Balance Sheets of relevant periods or a certificate from the Chartered Accountant / Cost Accountant indicating the turnover details for the relevant period shall be uploaded with the bid. In case the date of constitution / incorporation of the bidder is less than 3-year-

पंजाब एण्ड सिंध बैंक *(भारत सरकार का उपक्रम)* ***प्रधान कार्यालय: सूचना प्रौद्योगिकी विभाग,*** ***द्वितीय तल, भूखंड संख्या-151,*** ***सेक्टर-44, संस्थागत क्षेत्र,*** ***गुरुग्राम– 122003*** *Email: ho.it@psb.bank.in*		***Punjab & Sind Bank*** *(A Govt. Of India Undertaking)* ***H.O. Information Technology Dept.,*** ***2nd Floor, Plot No. 151,*** ***Sector -44, Institutional Area,*** ***Gurugram - 122003*** *Email: ho.it@psb.bank.in*

Addendum 1

S. No.	RFP Section no.	RFP Page No.	RFP Clause	Modified Clause
				old, the average turnover in respect of the completed financial years after the date of constitution shall be taken into account for this criteria. 2. Purchase preference to Micro and Small Enterprises (MSEs): Purchase preference will be given to MSEs having valid Udyam Certificate and whose credentials are validated online through Udyam Registration portal as defined in Public Procurement Policy for Micro and Small Enterprises (MSEs) Order, 2012 dated 23.03.2012 issued by Ministry of Micro, Small and Medium Enterprises and its subsequent Orders/Notifications issued by concerned Ministry. If the bidder wants to avail themselves of the Purchase preference, the bidder must be the manufacturer / OEM of the offered product on GeM. In respect of bid for Services, the bidder must be the Service provider of the offered Service. Traders are excluded from the purview of Public Procurement Policy for Micro and Small Enterprises and hence resellers offering products manufactured by some other OEM are not eligible for any purchase preference. Relevant documentary evidence in this regard shall be uploaded along with the bid in respect of the offered product or service, and Buyer will decide eligibility for purchase preference based on documentary evidence submitted in case of product bids, whereas in case of services the eligibility is automatically validated. If L-1 is not an

पंजाब एण्ड सिंध बैंक *(भारत सरकार का उपक्रम)* ***प्रधान कार्यालय: सूचना प्रौद्योगिकी विभाग,*** ***द्वितीय तल, भूखंड संख्या-151,*** ***सेक्टर-44, संस्थागत क्षेत्र,*** ***गुरुग्राम– 122003*** *Email: ho.it@psb.bank.in*		***Punjab & Sind Bank*** *(A Govt. Of India Undertaking)* ***H.O. Information Technology Dept.,*** ***2nd Floor, Plot No. 151,*** ***Sector -44, Institutional Area,*** ***Gurugram - 122003*** *Email: ho.it@psb.bank.in*

Addendum 1

S. No.	RFP Section no.	RFP Page No.	RFP Clause	Modified Clause
				MSE and MSE Seller (s) has / have quoted price within L-1+ 15% (Selected by Buyer) of margin of purchase preference /price band defined in relevant policy, such MSE Seller shall be given opportunity to match L-1 price and contract will be awarded for % (selected by Buyer) percentage of total quantity. The buyers are advised to refer the OM_No.1_4_2021_PPD_dated_18.05.2023 for compliance of Concurrent application of Public Procurement Policy for Micro and Small Enterprises Order, 2012 and Public Procurement (Preference to Make in India) Order, 2017. Benefits of MSE will be allowed only if seller is validated on-line in GeM profile as well as validated and approved by Buyer after evaluation of documents submitted. 3. If L-1 is not an MSE and MSE Service Provider (s) has/have quoted price within L-1+ 15% of margin of purchase preference /price band as defined in the relevant policy, then 100% order quantity will be awarded to such MSE bidder subject to acceptance of L1 bid price. 4. Estimated Bid Value indicated above is being declared solely for the purpose of guidance on EMD amount and for determining the Eligibility Criteria related to Turn Over, Past Performance and Project / Past Experience etc. This has no relevance or bearing on the price to be quoted by the bidders and is also not going to have any impact on bid participation. Also this is not going to be used as a criteria in determining reasonableness of quoted prices which

पंजाब एण्ड सिंध बैंक *(भारत सरकार का उपक्रम)* ***प्रधान कार्यालय: सूचना प्रौद्योगिकी विभाग,*** ***द्वितीय तल, भूखंड संख्या-151,*** ***सेक्टर-44, संस्थागत क्षेत्र,*** ***गुरुग्राम– 122003*** *Email: ho.it@psb.bank.in*	पंजाब एण्ड सिंध बैंक (भारत सरकार का उपक्रम)	***Punjab & Sind Bank*** *(A Govt. Of India Undertaking)* ***H.O. Information Technology Dept.,*** ***2nd Floor, Plot No. 151,*** ***Sector -44, Institutional Area,*** ***Gurugram - 122003*** *Email: ho.it@psb.bank.in*

Addendum 1

S. No.	RFP Section no.	RFP Page No.	RFP Clause	Modified Clause
				would be determined by the buyer based on its own assessment of reasonableness and based on competitive prices received in Bid / RA process.
13.	Annexure 21, 15.21.4 Deployment & Data Retention, S. No. 20	212	S. No. | Solution Name | Application/Solution/Appliance Deployment Requirement | Retention Requirement | Volumetrics **20** | AI Security | 1. Bank's DC - HA (N+N Active-Active) deployment 2. Bank's DR - HA (N+N Active-Active) deployment | 1 Month (Logs and Data Storage on Appliance / Primary Storage) | Business Users - 12000 scalable to 16000 Enterprise AI Applications- 10 Qty AI Models- Unlimited AI Users - Unlimited Prompts- Unlimited API Calls- Unlimited AI Sessions- Unlimited	S. No. | Solution Name | Application/Solution/Appliance Deployment Requirement | Retention Requirement | Volumetrics **20** | AI Security | 3. Bank's DC - HA (N+N Active-Active) deployment 4. Bank's DR - HA (N+N Active-Active) deployment | 1 Month (Logs and Data Storage on Appliance / Primary Storage) | • Business Users - 12000 scalable to 16000 • Internet Users - 500 Users scalable to 1000 • Enterprise AI Applications- 10 Qty

पंजाब एण्ड सिंध बैंक *(भारत सरकार का उपक्रम)* ***प्रधान कार्यालय: सूचना प्रौद्योगिकी विभाग,*** ***द्वितीय तल, भूखंड संख्या-151,*** ***सेक्टर-44, संस्थागत क्षेत्र,*** ***गुरुग्राम– 122003*** *Email: ho.it@psb.bank.in*		***Punjab & Sind Bank*** *(A Govt. Of India Undertaking)* ***H.O. Information Technology Dept.,*** ***2nd Floor, Plot No. 151,*** ***Sector -44, Institutional Area,*** ***Gurugram - 122003*** *Email: ho.it@psb.bank.in*

Addendum 1

S. No.	RFP Section no.	RFP Page No.	RFP Clause	Modified Clause
			AI Policies- Unlimited	• AI Models- Unlimited • AI Users - Unlimited • Prompts- Unlimited • API Calls- Unlimited • AI Sessions- Unlimited • AI Policies- Unlimited

पंजाब एण्ड सिंध बैंक *(भारत सरकार का उपक्रम)* ***प्रधान कार्यालय: सूचना प्रौद्योगिकी विभाग,*** ***द्वितीय तल, भूखंड संख्या-151,*** ***सेक्टर-44, संस्थागत क्षेत्र,*** ***गुरुग्राम– 122003*** *Email: ho.it@psb.bank.in*		***Punjab & Sind Bank*** *(A Govt. Of India Undertaking)* ***H.O. Information Technology Dept.,*** ***2nd Floor, Plot No. 151,*** ***Sector -44, Institutional Area,*** ***Gurugram - 122003*** *Email: ho.it@psb.bank.in*

Addendum 1

S. No.	RFP Section no.	RFP Page No.	RFP Clause					Modified Clause				
14.	Annexure 21, 15.21.4 Deployment & Data Retention, S. No. 22	212	S. No.	Solution Name	Application/Solution/Appliance Deployment Requirement	Retention Requirement	Volumetrics	S. No.	Solution Name	Application/Solution/Appliance Deployment Requirement	Retention Requirement	Volumetrics
			22	Backup & Retention *(Provided and maintained by bank)*	Centralized Backup & Retrieval Solution deployed across DC and DR. Solution shall support automated backup, replication, indexing, retrieval, and immutable archival of all logs, alerts, events, configurations, reports, incidents, and security		Bidder to right size	22	Backup & Retention	Centralized Backup & Retrieval Solution deployed across DC and DR. Solution shall support automated backup, replication, indexing, retrieval, and immutable archival of all logs, alerts, events, configurations, reports, incidents, and security artefacts generated by all proposed solutions.		Bidder to right size

पंजाब एण्ड सिंध बैंक *(भारत सरकार का उपक्रम)* ***प्रधान कार्यालय: सूचना प्रौद्योगिकी विभाग,*** ***द्वितीय तल, भूखंड संख्या-151,*** ***सेक्टर-44, संस्थागत क्षेत्र,*** ***गुरुग्राम– 122003*** *Email: ho.it@psb.bank.in*		***Punjab & Sind Bank*** *(A Govt. Of India Undertaking)* ***H.O. Information Technology Dept.,*** ***2nd Floor, Plot No. 151,*** ***Sector -44, Institutional Area,*** ***Gurugram - 122003*** *Email: ho.it@psb.bank.in*

Addendum 1

S. No.	RFP Section no.	RFP Page No.	RFP Clause	Modified Clause
			artefacts generated by all proposed solutions.	
15.	Appendix 1A, ZTNA – 3		The ZTNA solution should have device posture validation across multiple parameters like Device Encryption, Registry Check, Process Check, AD Domain Check, OPSWAT and Certificates etc. to provide specific URL or Internet Access based on granular policy controls. The device posture check should be recurring and check the compliance of the posture periodically to maintain the Device Trust.	The ZTNA solution should have device posture validation across multiple parameters like Device Encryption, Registry Check, Process Check, AD Domain Check, and Certificates etc. to provide specific URL or Internet Access based on granular policy controls. The device posture check should be recurring and check the compliance of the posture periodically to maintain the Device Trust.
16.	Appendix 1A, ZTNA – 4		Any component installed in DC's (On-premise) must not need any inbound ACL rule in customer DC/DR Firewall to provide access to Private Application.	Any ZTNA component deployed within the Bank's DC/DR environment shall not require any inbound Internet-initiated ACL, NAT, or port-publishing rule on the Bank's DC/DR perimeter firewall for providing remote access to Private Applications. The solution shall support an outbound-initiated secure connectivity model from the on-premise component to the ZTNA service.
17.	Appendix 1A, ZTNA – 11		The solution should provide the capability to add any number of App Connectors in DC without any additional price or license.	The solution should provide the capability to add any number of connector or gateway in DC and DR without any additional price or license. Or The solution should not have separate user based licenses for the private access it should be part of the internet access user based licenses.

पंजाब एण्ड सिंध बैंक *(भारत सरकार का उपक्रम)* ***प्रधान कार्यालय: सूचना प्रौद्योगिकी विभाग,*** ***द्वितीय तल, भूखंड संख्या-151,*** ***सेक्टर-44, संस्थागत क्षेत्र,*** ***गुरुग्राम– 122003*** *Email: ho.it@psb.bank.in*		***Punjab & Sind Bank*** *(A Govt. Of India Undertaking)* ***H.O. Information Technology Dept.,*** ***2nd Floor, Plot No. 151,*** ***Sector -44, Institutional Area,*** ***Gurugram - 122003*** *Email: ho.it@psb.bank.in*

Addendum 1

S. No.	RFP Section no.	RFP Page No.	RFP Clause	Modified Clause
18.	Appendix 1A, ZTNA – 13		The ZTNA components including ZTNA broker, App Connector/Gateway should be deployed on-premises in SDC	The ZTNA components including ZTNA broker, App Connector/Gateway should be deployed on-premises in DC and DR
19.	Appendix 1A, ZTNA – 24		Solution must support Connector Dashboard provides insight into application traffic,app connector health, and utilization, enabling decision on resource allocation, connection optimization, and troubleshooting.	Solution must support Connector Dashboard or gateway dashboard provides insight into application traffic, app connector or gateway health, and utilization, enabling decision on resource allocation, connection optimization, and troubleshooting.
20.	Appendix 1A, ZTNA – 26		Solution should support extensive coverage with in-built Data types like Aadhar card, PII, etc with different File Types etc. Solution should support extensive coverage with 100+ in-built Data types with minimum 200 File Types.	Solution should support extensive coverage with in-built Data types like Aadhar card, PII, etc with different File Types etc. Solution should support extensive coverage with 100+ in-built Data types with minimum 50 File Types.
21.	Appendix 1A, ZTNA – 29		Additional Clause	ZTNA Security must provide ability to restrict upload/download
22.	Appendix 1A, ZTNA – 30		Additional Clause	The solution must apply real-time Inline Data Loss Prevention (DLP) capabilities to private application traffic (Data-in-Motion) without relying on external ICAP servers or third-party add-ons or Isolation Mechanisms and prevent lateral movement of sensitive financial data (e.g., PII, PCI-DSS, internal financial records).
23.	Appendix 1A, AI		Discovery of Embedded AI browser extensions, plug-ins and connectors using AI with Agent and Agentless	The solution shall provide continuous discovery and visibility of embedded / Shadow AI capabilities like AI browser extension/plugins/connectors

पंजाब एण्ड सिंध बैंक *(भारत सरकार का उपक्रम)* ***प्रधान कार्यालय: सूचना प्रौद्योगिकी विभाग,*** ***द्वितीय तल, भूखंड संख्या-151,*** ***सेक्टर-44, संस्थागत क्षेत्र,*** ***गुरुग्राम– 122003*** *Email: ho.it@psb.bank.in*		***Punjab & Sind Bank*** *(A Govt. Of India Undertaking)* ***H.O. Information Technology Dept.,*** ***2nd Floor, Plot No. 151,*** ***Sector -44, Institutional Area,*** ***Gurugram - 122003*** *Email: ho.it@psb.bank.in*

Addendum 1

S. No.	RFP Section no.	RFP Page No.	RFP Clause	Modified Clause
	Security (General) – 1.3			
24.	Appendix 1A, AI Security (General) – 1.4		Enterprise-wide protection across Email, SaaS, Files, Endpoints and AI prompts.	Enterprise-wide protection across Web Email, SaaS, Files, Endpoints and AI prompts.
25.	Appendix 1A, AI Security (General) – 1.5		Configurable enforcement actions including Content Moderation, Coach in addition to Block/Monitor.	Configurable enforcement actions including Content Moderation
26.	Appendix 1A, AI Security (General) – 1.6		Browser and Endpoint agents distributable through MSI packages/MDM.	Clause Stands Deleted
27.	Appendix 1A, AI		Context-aware user coaching with safer alternatives.	Clause Stands Deleted

पंजाब एण्ड सिंध बैंक *(भारत सरकार का उपक्रम)* ***प्रधान कार्यालय: सूचना प्रौद्योगिकी विभाग,*** ***द्वितीय तल, भूखंड संख्या-151,*** ***सेक्टर-44, संस्थागत क्षेत्र,*** ***गुरुग्राम– 122003*** *Email: ho.it@psb.bank.in*		***Punjab & Sind Bank*** *(A Govt. Of India Undertaking)* ***H.O. Information Technology Dept.,*** ***2nd Floor, Plot No. 151,*** ***Sector -44, Institutional Area,*** ***Gurugram - 122003*** *Email: ho.it@psb.bank.in*

Addendum 1

S. No.	RFP Section no.	RFP Page No.	RFP Clause	Modified Clause
	Security (General) – 1.13			
28.	Appendix 1A, AI Security (General) – 1.16		AI Central Command Center for the view of Inventory including models, agents, MCP servers, tools, hooks, repositories and permissions.	AI Central Command Center/Dashboard for the view of Inventory including models, agents, MCP servers, tools, hooks, repositories and permissions.
29.	Appendix 1A, AI Security (General) – 1.18		API or Inline compatibility with OpenAI, Anthropic, Bedrock and Vertex AI schemas without application code changes.	API or Inline compatibility with AI schemas without application code changes.
30.	Appendix 1A, AI Security (General) – 1.20		Ability for the Bank to create its own semantic detectors without vendor professional services.	Ability for the Bank to create its own semantic/ML detectors without vendor professional services.
31.	Appendix 1A, AI		Detailed operational dashboards and exportable reports (tokens, prompts, models, providers, users, streaming, tool usage).	Detailed operational dashboards and exportable reports (tokens, prompts, models, providers, users, tool usage etc.).

Addendum 1

S. No.	RFP Section no.	RFP Page No.	RFP Clause	Modified Clause
	Security (General) – 1.26			
32.	Appendix 1A, AI Security (General) – 1.30		Control on MCP server capabilities (Tools, Resources, Prompts, Schemas).	Control on MCP server capabilities (like Tools, Resources, Prompts, Schemas etc.).
33.	Appendix 1A, AI Security (General) – 1.32		Complete logging of MCP protocol payloads, tool invocations and policy decisions.	Complete logging of MCP protocol
34.	Appendix 1A, AI Security (General) – 1.38		Mapping Red Team findings to OWASP LLM Top 10, MITRE ATLAS, Agentic AI and NIST AI RMF.	The proposed solution should enable configuration of policies aligned with the requirements of the bank, regulators etc. like OWASP LLM Top 10, MITRE ATLAS, Agentic AI and NIST AI RMF
35.	Appendix 1A, AI		Selective re-testing of attack categories.	Clause Stands Deleted

पंजाब एण्ड सिंध बैंक *(भारत सरकार का उपक्रम)* ***प्रधान कार्यालय: सूचना प्रौद्योगिकी विभाग,*** ***द्वितीय तल, भूखंड संख्या-151,*** ***सेक्टर-44, संस्थागत क्षेत्र,*** ***गुरुग्राम– 122003*** *Email: ho.it@psb.bank.in*		***Punjab & Sind Bank*** *(A Govt. Of India Undertaking)* ***H.O. Information Technology Dept.,*** ***2nd Floor, Plot No. 151,*** ***Sector -44, Institutional Area,*** ***Gurugram - 122003*** *Email: ho.it@psb.bank.in*

Addendum 1

S. No.	RFP Section no.	RFP Page No.	RFP Clause	Modified Clause
	Security (General) – 1.39			
36.	Appendix 1A, AI Security (General) – 1.40		Exportable Red Team reports with raw prompts and responses.	Clause Stands Deleted
37.	Appendix 1A, AI Security (General) – 1.41		Native integration of Guardrails within AI Gateway	Clause Stands Deleted
38.	Appendix 1A, AI Security (General) – 1.42		Additional Clause	The solution shall provide administrator controlled override policy or kill switch to immediately suspend agent activity and communication in case of operational risk or security compromise
39.	Appendix 1A, AI		Additional Clause	The solution shall provide configurable rate-limiting controls for AI/LLM requests to prevent abuse and support controlled management of AI resource consumption

पंजाब एण्ड सिंध बैंक *(भारत सरकार का उपक्रम)* ***प्रधान कार्यालय: सूचना प्रौद्योगिकी विभाग,*** ***द्वितीय तल, भूखंड संख्या-151,*** ***सेक्टर-44, संस्थागत क्षेत्र,*** ***गुरुग्राम– 122003*** *Email: ho.it@psb.bank.in*		***Punjab & Sind Bank*** *(A Govt. Of India Undertaking)* ***H.O. Information Technology Dept.,*** ***2nd Floor, Plot No. 151,*** ***Sector -44, Institutional Area,*** ***Gurugram - 122003*** *Email: ho.it@psb.bank.in*

Addendum 1

S. No.	RFP Section no.	RFP Page No.	RFP Clause	Modified Clause
	Security (A. General) – 1.43			
40.	Appendix 1A, AI Security (A. General) – 1.44		Additional Clause	The solution shall provide a unified access mechanism for multiple LLM/AI providers, enabling consistent security policies and controls across supported AI models and services
41.	Appendix 1A, AI Security (AI Gateway) – 2		Automatically maintain an inventory and control of all Model Context Protocol (MCP) servers and tools connected to, or invoked from, the enterprise environment.	Automatically maintain an inventory and control/logs of all Model Context Protocol (MCP) servers and tools connected to, or invoked from, the enterprise environment.
42.	Appendix 1A, AI Security (AI		The Proposed solution's all components (on-prem HW or Software if any) should connect to management plane within India for any kind of monitoring/health checks of components. The proposed solution should have CSA STAR, SOC 2, CIS, ISO 27001, ISO 27017, ISO 27018 certification and must be a part of Microsoft Active Protections Program (MAPP)	The Proposed solution's all components (on-prem HW or Software if any) should connect to management plane, if not hosted at bank's DC & DR, within India for any kind of monitoring/health checks of components.

पंजाब एण्ड सिंध बैंक *(भारत सरकार का उपक्रम)* ***प्रधान कार्यालय: सूचना प्रौद्योगिकी विभाग,*** ***द्वितीय तल, भूखंड संख्या-151,*** ***सेक्टर-44, संस्थागत क्षेत्र,*** ***गुरुग्राम– 122003*** *Email: ho.it@psb.bank.in*		***Punjab & Sind Bank*** *(A Govt. Of India Undertaking)* ***H.O. Information Technology Dept.,*** ***2nd Floor, Plot No. 151,*** ***Sector -44, Institutional Area,*** ***Gurugram - 122003*** *Email: ho.it@psb.bank.in*

Addendum 1

S. No.	RFP Section no.	RFP Page No.	RFP Clause	Modified Clause
	Gateway) – 7			
43.	Appendix 1A, AI Security (AI Gateway) – 8		Solution is available as a lightweight virtual appliance for public cloud deployments in AWS, or private cloud deployments with VMware ESXi.	Solution is available as a lightweight virtual appliance for public cloud deployments in AWS, or private cloud deployments with VMware ESXi or hardware based deployment.
44.	Appendix 1A, AI Security (AI Gateway) – 11		Solution use only authenticated agents for the communication, by using token from AI gateway	Solution use only authenticated agents for the communication
45.	Appendix 1A, AI Security (AI Gateway) – 13		The proposed solution should support over 30 languages (including East Asian and European) for AI inspection.	Clause Stands Deleted

पंजाब एण्ड सिंध बैंक *(भारत सरकार का उपक्रम)* ***प्रधान कार्यालय: सूचना प्रौद्योगिकी विभाग,*** ***द्वितीय तल, भूखंड संख्या-151,*** ***सेक्टर-44, संस्थागत क्षेत्र,*** ***गुरुग्राम– 122003*** *Email: ho.it@psb.bank.in*		***Punjab & Sind Bank*** *(A Govt. Of India Undertaking)* ***H.O. Information Technology Dept.,*** ***2nd Floor, Plot No. 151,*** ***Sector -44, Institutional Area,*** ***Gurugram - 122003*** *Email: ho.it@psb.bank.in*

Addendum 1

S. No.	RFP Section no.	RFP Page No.	RFP Clause	Modified Clause
46.	Appendix 1A, AI Security (AI Gateway) – 15		The solution must provide the capability to block or allow the download of MCP server code from Private MCP	The solution must provide the capability to block or allow the download of MCP server code from Private MCP like a private GitHub, private MCP marketplace etc.
47.	Appendix 1A, AI Security (AI Gateway) – 16		All AI Gateway has to be native managed by common AI Security and Guardrails in Line with unified agent and Management	AI Gateways shall be integrated with AI Security and AI Guardrails platform
48.	Appendix 1A, AI Security (AI Guardrails) – 1		The proposed solution should provide detailed visibility, granular activity control, and protection for both Gen-AI prompts and responses — blocking content that bypasses LLM safety protocols, constitutes prompt injection/jailbreaking attempts, or is harmful/ hateful/ biased/ inappropriate/ risky — with policies mapped to MITRE ATLAS and OWASP Top 10 for LLMs.	The proposed solution should provide detailed visibility, granular activity control, and protection for both Gen-AI prompts and responses — blocking content that bypasses LLM safety protocols, constitutes prompt injection/jailbreaking attempts, or is harmful/ hateful/ biased/ inappropriate/ risky — with policies mapped to MITRE ATLAS or OWASP Top 10 for LLMs.
49.	Appendix 1A, AI		The proposed solution should support over 30 languages (including East Asian and European) for AI inspection.	The proposed solution should support English and Hindi for AI Inspection

Addendum 1

S. No.	RFP Section no.	RFP Page No.	RFP Clause	Modified Clause
	Security (AI Guardrails) – 9			
50.	Appendix 1A, AI Security (AI Guardrails) – 13		The AI security layer must integrate with enterprise-grade DLP to prevent upload of PII, PCI, or PHI into LLMs, while providing real-time feedback to educate users on safe AI usage. The solution should support real-time visibility for cloud applications with dynamic risk score/rating based on Cloud Security Alliance Standards. The solution must be able to report the security compliances and certifications achieved by these apps.	The AI security layer must integrate with enterprise-grade DLP to prevent upload of PII, PCI, or PHI into LLMs. The Solution shall continuously discover and classify all standalone, embedded, and API-driven GenAI/LLM applications across network, endpoint, and identity vectors, with risk ratings based on a centrally maintained and continuously updated AI application risk database/index.
51.	Appendix 1A, AI Security (AI Security) – 1		The proposed solution must provide Shadow Discovery of Gen AI apps running in the customer environment, differentiate private vs Public instances, sanctioned/unsanctioned, restrict sensitive data upload to public-instance Gen AI apps, and maintain a curated catalog of Gen AI applications and MCP servers with automated risk scoring/rating based on security attributes, data handling practices, and compliance.	The proposed solution must provide Shadow Discovery of Gen AI apps running in the bank environment and differentiate sanctioned/unsanctioned, restrict sensitive data upload to public-instance Gen AI apps, and maintain a curated catalog of Gen AI applications and MCP servers with automated risk scoring or rating based on security attributes, how AI handling data and compliance.
52.	Appendix 1A, AI Security (AI		Apply DLP, threat/data protection and access control to AI traffic in a single inspection pass to minimize latency and avoid repeated TLS decrypt/re-encrypt cycles.	Apply Shadow AI protection and access control to AI traffic in a single inspection pass to minimize latency and avoid repeated TLS decrypt/re-encrypt cycles.

Addendum 1

S. No.	RFP Section no.	RFP Page No.	RFP Clause	Modified Clause
	Security) – 7			
53.	Appendix 1A, AI Security (AI Security) – 9		Enforce AI security policy consistently for corporate-managed devices, BYOD and remote/unmanaged endpoints via a cloud-delivered security service edge.	AI Security Policy enforcement and control of sanctioned and unsanctioned AI applications and services
54.	Appendix 1A, AI Security (AI Security) – 10		The solution must include an Agentic Visibility and Control capability providing centralized visibility and control over AI agents, ensuring all agent-to-agent and agent-to-data interactions (including via MCP) are monitored, governed, and secured in real time — with granular control to permit AI agents to "Read" from enterprise data sources while strictly blocking "Update"/"Delete" operations. This must be available on the same agent/platform with additional licenses as required in future.	The solution must include a Command Center/ dashboard to have Agentic Visibility and Control capability providing centralized visibility and control over AI agents, ensuring all agent-to-agent and agent-to-data interactions (including via MCP) are monitored, governed, and secured in real time.
55.	Appendix 1A, AI Security (AI		The proposed solution should provide DLP-level controls to block and monitor data exfiltration over Gen-AI apps, including detailed user coaching that redirects users to corporate Gen AI apps, with an option for users to justify business use case before interacting further.	The proposed solution should provide DLP-level controls to block and monitor data exfiltration over Gen-AI apps

पंजाब एण्ड सिंध बैंक *(भारत सरकार का उपक्रम)* ***प्रधान कार्यालय: सूचना प्रौद्योगिकी विभाग,*** ***द्वितीय तल, भूखंड संख्या-151,*** ***सेक्टर-44, संस्थागत क्षेत्र,*** ***गुरुग्राम– 122003*** *Email: ho.it@psb.bank.in*		***Punjab & Sind Bank*** *(A Govt. Of India Undertaking)* ***H.O. Information Technology Dept.,*** ***2nd Floor, Plot No. 151,*** ***Sector -44, Institutional Area,*** ***Gurugram - 122003*** *Email: ho.it@psb.bank.in*

Addendum 1

S. No.	RFP Section no.	RFP Page No.	RFP Clause	Modified Clause
	Security) – 13			
56.	Appendix 1A, AI Security (AI Security) – 17		The Proposed solution should have capable to setup policy based on: End-User Device Posture Assessment:	The proposed solution shall provide policy-based access and decisions using end-user device posture.
57.	Appendix 1A, AI Security (AI Security) – 17.1		Posture Check including Certificate check, Domain check, AV agent check, customer's Custom apps check, process and registry check on endpoints.	Clause stands Deleted
58.	Appendix 1A, AI Security (AI Security) – 17.2		The Posture assessment must be periodic in nature and repeat in every 15 minutes or less to ensure continued compliance"	Clause stands Deleted

पंजाब एण्ड सिंध बैंक *(भारत सरकार का उपक्रम)* ***प्रधान कार्यालय: सूचना प्रौद्योगिकी विभाग,*** ***द्वितीय तल, भूखंड संख्या-151,*** ***सेक्टर-44, संस्थागत क्षेत्र,*** ***गुरुग्राम– 122003*** *Email: ho.it@psb.bank.in*		***Punjab & Sind Bank*** *(A Govt. Of India Undertaking)* ***H.O. Information Technology Dept.,*** ***2nd Floor, Plot No. 151,*** ***Sector -44, Institutional Area,*** ***Gurugram - 122003*** *Email: ho.it@psb.bank.in*

Addendum 1

S. No.	RFP Section no.	RFP Page No.	RFP Clause	Modified Clause
59.	Appendix 1A, AI Security (AI Security) – 19		This must include the capability to Inspect the Web Traffic sent by CLI Commands (For ex. S3) and Thick Clients like MS Teams to enable secured transactions without any user experience issues from Day 1.	This must include the capability to Inspect the Web Traffic sent by CLI Commands (For ex. S3) and Thick Clients to enable secured transactions without any user experience issues from Day 1.
60.	Appendix 1A, AI Security (AI Security) – 20		Additional Clause	Discovery and Classification of GenAI/SaaS/Private — Discovery of sanctioned/unsanctioned cloud apps, private apps, and GenAI/LLM apps (with risk ratings) originates from a single, maintained app risk index, not a licensed third-party feed.
61.	Appendix 1A, SBOM, CBOM & AI-BOM (B. Functional and Technic		The platform shall scan the source code and generate CBOM info	The solution shall support CBOM generation through analysis of source code, binaries, firmware, software packages, VM/container images and imported CBOMs, as applicable. The solution shall support standard CBOM formats and interoperability, including CycloneDX CBOM, wherever applicable. The solution shall generate SBOM, CBOM, QBOM, AIBOM without any dependency on the vendor's proprietary source code

पंजाब एण्ड सिंध बैंक *(भारत सरकार का उपक्रम)* ***प्रधान कार्यालय: सूचना प्रौद्योगिकी विभाग,*** ***द्वितीय तल, भूखंड संख्या-151,*** ***सेक्टर-44, संस्थागत क्षेत्र,*** ***गुरुग्राम– 122003*** *Email: ho.it@psb.bank.in*		***Punjab & Sind Bank*** *(A Govt. Of India Undertaking)* ***H.O. Information Technology Dept.,*** ***2nd Floor, Plot No. 151,*** ***Sector -44, Institutional Area,*** ***Gurugram - 122003*** *Email: ho.it@psb.bank.in*

Addendum 1

S. No.	RFP Section no.	RFP Page No.	RFP Clause	Modified Clause
	al Requirements) – 11			
62.	Appendix 1A, SBOM, CBOM & AI-BOM (B. Functional and Technical Requirements) – 47		There must be a single view of vulnerabilities from scanners, VAPT, bug bounty, etc. mapped to SBOM	The solution shall provide a consolidated vulnerability view correlated with SBOM/CBOM components using global vulnerability databases, CERT-In Vulnerability Notes and Advisories, vendor/security advisories, VEX statements and imported VAPT/scanner/bug-bounty findings. It shall support identification, tracking, prioritization and remediation evidence for CERT-In-published vulnerabilities.
63.	Appendix 1A, SBOM, CBOM & AI-BOM		The solution shall discover AI model dependencies, embeddings, vector databases, plugins and external AI services.	The solution shall discover, ingest, correlate and manage AI model, framework, dependency, dataset, embedding, vector database, plugin and AI API/service metadata through supported discovery, manifests, repositories, registries, AI-BOMs and integrations.

पंजाब एण्ड सिंध बैंक *(भारत सरकार का उपक्रम)* ***प्रधान कार्यालय: सूचना प्रौद्योगिकी विभाग,*** ***द्वितीय तल, भूखंड संख्या-151,*** ***सेक्टर-44, संस्थागत क्षेत्र,*** ***गुरुग्राम– 122003*** *Email: ho.it@psb.bank.in*		***Punjab & Sind Bank*** *(A Govt. Of India Undertaking)* ***H.O. Information Technology Dept.,*** ***2nd Floor, Plot No. 151,*** ***Sector -44, Institutional Area,*** ***Gurugram - 122003*** *Email: ho.it@psb.bank.in*

Addendum 1

S. No.	RFP Section no.	RFP Page No.	RFP Clause	Modified Clause
	(B. Functional and Technical Requirements) – 66			
64.	Appendix 1A, SBOM, CBOM & AI-BOM (B. Functional and Technical Requirements) – 78		The proposed solution shall automatically discover cryptographic assets across applications, operating systems, databases, middleware and network infrastructure.	The solution shall support cryptographic asset visibility through discovery, APIs/integrations, artifact analysis and imported CBOM/QBOM information

पंजाब एण्ड सिंध बैंक *(भारत सरकार का उपक्रम)* ***प्रधान कार्यालय: सूचना प्रौद्योगिकी विभाग,*** ***द्वितीय तल, भूखंड संख्या-151,*** ***सेक्टर-44, संस्थागत क्षेत्र,*** ***गुरुग्राम– 122003*** *Email: ho.it@psb.bank.in*		***Punjab & Sind Bank*** *(A Govt. Of India Undertaking)* ***H.O. Information Technology Dept.,*** ***2nd Floor, Plot No. 151,*** ***Sector -44, Institutional Area,*** ***Gurugram - 122003*** *Email: ho.it@psb.bank.in*

Addendum 1

S. No.	RFP Section no.	RFP Page No.	RFP Clause	Modified Clause
65.	Appendix 1A, MFA – 7		The MFA server must support IETF RFC4758 (Cryptographic Token Key Initiation Protocol) protocol out-of-the-box with no additional customization required.	The MFA server must support IETF RFC4758 (Cryptographic Token Key Initiation Protocol) protocol/OATH HOTP/TOTP and FIDO2 standards protocol out-of-the-box with no additional customization required.
66.	Appendix 1A, MFA – 6		Solutions should be capable for integration with TACACS solution being used by the Bank.	Solutions should be capable for integration with RADIUS and other standard protocols being used by the Bank.
67.	Appendix 1A, MFA – 11.8		The authentication agents must support the following platforms: 11.8 Epic Hyperdrive	Clause stands deleted
68.	Appendix 1A, KMS – 3		The system should support AES(128-256), ARIA,ECC(224-512), Brainpool curves, HMAC , TDES, RSA(512-4096) and the Crypto mode (CBC, CBC-CS1,ECB,GCM) etc.	The system should support AES(128-256), ARIA,ECC(224-512), Brainpool curves, HMAC, TDES, RSA(512-4096) and the Crypto mode (FIPS-approved and industry-standard encryption modes) etc.
69.	Appendix 1A, KMS – 4		The system should support API REST (JWT),SOAP, KMIP, PKCS#11, JCE, .NET, MSCAPI, MS CNG, C,NAE,XML, Java API's and libraries for integration with custom applications.	The system should support API REST (JWT),SOAP, KMIP, PKCS#11, JCE, .NET, MSCAPI, MS CNG, C, industry-standard secure APIs/interfaces such as REST API, KMIP, PKCS#11, JCE/JCA, Microsoft CAPI/CNG or equivalent', Java API's and libraries for integration with custom applications.
70.	Appendix 1A,		The System shall support Multi-tenancy using multiple domains, Clustering, High Availability and Backup.	The System shall support multi-tenancy using multiple domains / multiple Vaults / multiple tenants, Clustering, High Availability and Backup.

पंजाब एण्ड सिंध बैंक *(भारत सरकार का उपक्रम)* ***प्रधान कार्यालय: सूचना प्रौद्योगिकी विभाग,*** ***द्वितीय तल, भूखंड संख्या-151,*** ***सेक्टर-44, संस्थागत क्षेत्र,*** ***गुरुग्राम– 122003*** *Email: ho.it@psb.bank.in*		***Punjab & Sind Bank*** *(A Govt. Of India Undertaking)* ***H.O. Information Technology Dept.,*** ***2nd Floor, Plot No. 151,*** ***Sector -44, Institutional Area,*** ***Gurugram - 122003*** *Email: ho.it@psb.bank.in*

Addendum 1

S. No.	RFP Section no.	RFP Page No.	RFP Clause	Modified Clause
	KMS – 5			
71.	Appendix 1A, KMS – 7		Solution should be capable of determining application reading data and abnormal spike in I/O are notified and blocked from Encrypting Data thus providing ransomware protection	Clause stands deleted
72.	Appendix 1A, KMS – 8		Solution should support Multi Factor Authentication (MFA) for users accessing protected path on Windows Servers either throught inbuilt feature or intergrating with the bank's MFA solution	Solution should have MFA for solution login.
73.	Appendix 1A, KMS – 14		The Key Discovery tool should be able to be managed from the KSM console and should be able to discover secrets like AES Key, AWS Key ID, Azure Storage Key, Mailchimp Access Key, Private Key, SendGrid API Key, SSH Private Key, SSH Public Key, Stripe Access Key, TDES Key, Twilio API Key, RSA Key, PGP Key, ECC Keys, Asymmetric Keys etc.	The Key Discovery capability should support the discovery of a broad range of secrets, cryptographic keys, credentials, API tokens, certificates, etc. across enterprise environments.
74.	Appendix 1A, KMS – 19		The Solution supports capability to protect data through encryption or tokenization using a FIPS 140-2 level 3 compliant solution.	The Solution supports capability to protect data through encryption or tokenization using a FIPS 140-3 level 3 compliant solution.
75.	Appendix 1A, KMS – 23		The Proposed solution should be capable of Ransomware detection and blocking capability	The Proposed solution should be capable of Ransomware “Protection or detection" and "blocking" capability

पंजाब एण्ड सिंध बैंक *(भारत सरकार का उपक्रम)* ***प्रधान कार्यालय: सूचना प्रौद्योगिकी विभाग,*** ***द्वितीय तल, भूखंड संख्या-151,*** ***सेक्टर-44, संस्थागत क्षेत्र,*** ***गुरुग्राम– 122003*** *Email: ho.it@psb.bank.in*		***Punjab & Sind Bank*** *(A Govt. Of India Undertaking)* ***H.O. Information Technology Dept.,*** ***2nd Floor, Plot No. 151,*** ***Sector -44, Institutional Area,*** ***Gurugram - 122003*** *Email: ho.it@psb.bank.in*

Addendum 1

S. No.	RFP Section no.	RFP Page No.	RFP Clause	Modified Clause
76.	Appendix 1A, KMS – 56		The HSMs must be in Secure Transport Mode (STM), to ensure HSM have not been altered while in transit	The HSMs must be in Secure Transport Mode (STM) or tamper evident packaging labels, to ensure HSM have not been altered while in transit
77.	Appendix 1A, KMS – 57		HSM should support the backup on FIPS certified hardware device, not to file in any form.	HSM should support the backup as per FIPS 140-3 guidelines
78.	Appendix 1A, Zero Day Attack Protection – 22		The proposed solution should be able to detect lateral movement (East-West) of the attack without installing agents on endpoint/server machines with least 100+ protocols for inspection.	The proposed solution should be able to detect lateral movement (East-West) of the attack without installing agents on endpoint/server machines with least 90+ protocols for inspection.
79.	Appendix 1A, Zero Day Attack Protection – 29		The proposed solution should be able to run at least 50 parallel sandboxes for analysis of payload and on premise customized sandbox solution should have the capability to allow manual submission of suspicious files for analysis	The proposed solution should be able to run at least 25 parallel sandboxes for analysis of payload and on premise customized sandbox solution should have the capability to allow manual submission of suspicious files for analysis

पंजाब एण्ड सिंध बैंक *(भारत सरकार का उपक्रम)* ***प्रधान कार्यालय: सूचना प्रौद्योगिकी विभाग,*** ***द्वितीय तल, भूखंड संख्या-151,*** ***सेक्टर-44, संस्थागत क्षेत्र,*** ***गुरुग्राम– 122003*** *Email: ho.it@psb.bank.in*		***Punjab & Sind Bank*** *(A Govt. Of India Undertaking)* ***H.O. Information Technology Dept.,*** ***2nd Floor, Plot No. 151,*** ***Sector -44, Institutional Area,*** ***Gurugram - 122003*** *Email: ho.it@psb.bank.in*

Addendum 1

S. No.	RFP Section no.	RFP Page No.	RFP Clause	Modified Clause
80.	Appendix 1A, Zero Day Attack Protection – 37		The proposed solution should support on premise centralized management for viewing information about detections	The proposed solution should support on premise centralized management or Dashboard for viewing information about detections.
81.	Appendix 1A, Zero Day Attack Protection – 44		The solution central management should include various methods of sharing threat intelligence data with other products or services including TAXII / Web services.	The solution should include various methods of sharing threat intelligence data with other products or services including TAXII / Web services.
82.	Appendix 1A, Zero Day Attack Protection – 32		Sandbox appliance should have redundant power supply, 2 TB or more storage capacity (or as per OEM recommendatin meeting the requirement mentioned in the RFP) with dedicated management port	Sandbox appliance should have redundant power supply and storage capacity as per OEM recommendation meeting the requirement mentioned in the RFP.
83.	Appendix 1A, DNS		Authoritative DNS services should be ISO 27001:2013 & ISO 27701:2019 compliant	Authoritative DNS services should be ISO 27001:2022 & ISO 27701:2019 or ISO 27018 / SOC 2 Type II compliant

S. No.	RFP Section no.	RFP Page No.	RFP Clause	Modified Clause
	Security (A. General) – 7			
84.	Appendix 1A, DNS Security (A. General) – 11		Solution must provide static name server IP for each domain used by the Bank.	The Solution shall provide authoritative DNS services with static name-server IPs wherever required for RBI/IDRBT, CERT-In, statutory, regulatory or domain-registration requirements, including the Bank's existing and future public domains. The Solution shall provide a highly available and resilient DNS infrastructure and support addition, modification, migration and reconfiguration of domains and name-server infrastructure throughout the contract period, including changes arising from future regulatory or technical requirements, without service disruption and at no additional cost to the Bank.
85.	Appendix 1A, Anti DDoS – 21		Mitigation mechanism to protecting against zero-day DoS and DDoS attacks without manual intervention. Automatic Real time signature generation	Mitigation mechanism to protect against zero-day DoS and DDoS attacks without manual intervention. Automatic Real time signature OR countermeasure generation in real-time
86.	Appendix 1A, Anti		Able to detect and protect from Zero-Day Network DDoS/DDoS flood attacks on the basis of behavioral DDoS attacks/challenge response mechanism or by an automatically created signature /	Able to detect and protect from Zero-Day Network DDoS/DDoS flood attacks on the basis of behavioral DDoS attacks/challenge response mechanism or by an automatically created signature / countermeasure within a minute.

पंजाब एण्ड सिंध बैंक *(भारत सरकार का उपक्रम)* ***प्रधान कार्यालय: सूचना प्रौद्योगिकी विभाग,*** ***द्वितीय तल, भूखंड संख्या-151,*** ***सेक्टर-44, संस्थागत क्षेत्र,*** ***गुरुग्राम– 122003*** *Email: ho.it@psb.bank.in*		***Punjab & Sind Bank*** *(A Govt. Of India Undertaking)* ***H.O. Information Technology Dept.,*** ***2nd Floor, Plot No. 151,*** ***Sector -44, Institutional Area,*** ***Gurugram - 122003*** *Email: ho.it@psb.bank.in*

Addendum 1

S. No.	RFP Section no.	RFP Page No.	RFP Clause	Modified Clause
	DDoS – 44		countermeasure within a minute and must be mentioned in data sheet. The proposed device should also support inbuilt Signatures apart from custom Signatures from Day 1.	The proposed device should also support inbuilt Signatures apart from custom Signatures OR reputation feeds from Day 1.
87.	Appendix 1B, Backup Solution and Storage – 15		The following backup and retention policy to ensure data protection, recoverability, and compliance with long-term retention needs is complied: • Daily Incremental Backup – retained for 2 weeks in disk-based appliance/backup storage • Weekly Full Backup for all data types – Retained for 4 weeks in disk-based appliance/backup storage • Monthly Full Backups – Retained for 2 Months in the same appliance/backup storage *After the 2-month period, Monthly Full backups must be migrated to long-term backup storage, where they shall be retained for the entire duration of the contract. Backup Appliance / Backup Storage Requirements * Online Backup Storage/Appliance must retain backups for a minimum period of 2 months, with each Monthly backup being preserved during this duration. * All monthly backups taken during the contract period must also be stored on long-term storage for the entire duration of the contract.	Clause Stands deleted from the Technical Specification. Refer RFP Section 15.21.4, table Retention Requirement for the requirements

पंजाब एण्ड सिंध बैंक *(भारत सरकार का उपक्रम)* ***प्रधान कार्यालय: सूचना प्रौद्योगिकी विभाग,*** ***द्वितीय तल, भूखंड संख्या-151,*** ***सेक्टर-44, संस्थागत क्षेत्र,*** ***गुरुग्राम– 122003*** *Email: ho.it@psb.bank.in*		***Punjab & Sind Bank*** *(A Govt. Of India Undertaking)* ***H.O. Information Technology Dept.,*** ***2nd Floor, Plot No. 151,*** ***Sector -44, Institutional Area,*** ***Gurugram - 122003*** *Email: ho.it@psb.bank.in*

Addendum 1

S. No.	RFP Section no.	RFP Page No.	RFP Clause	Modified Clause
			*All the data, logs, information & others must be backed up using the proposed backup and retrieval solution, in accordance with the defined backup policy and retention requirements. *Regularly test and verify the integrity of backed-up data and information by performing retrieval exercises. This process should be completed prior to overwriting or replacing any previously taken backups, to ensure that the data is recoverable, intact, and usable when required.	
88.	Appendix 1B, Backup Solution and Storage – 16		The proposed disk-based storage/appliance must interoperate with industry-leading server platforms and operating systems, and must ingest backup data over a secure, API-based disk-to-disk (D2D) connection.	The proposed disk-based storage/appliance must interoperate with industry-leading server platforms and operating systems, and must ingest backup data using standard Data protocols such as FC, ISCI, NFS, S3
89.	Appendix 1B, Backup Solution and Storage – 38		The proposed backup solution must natively support a LAN-Free architecture for all image-level VM backups to prevent performance degradation on production networks. All raw backup data payloads must stream directly from production storage to the backup appliance/storage over a dedicated Storage Area Network (SAN/Fibre Channel/iSCSI) or dedicated storage fabric. Production Ethernet/LAN infrastructure must be completely bypassed, restricting its use strictly to minor control traffic and metadata orchestration.	The proposed backup solution must natively support a "LAN-Free"/ "LAN efficient" architecture for all image-level VM backups to prevent performance degradation on production networks. All raw backup data payloads must stream directly from production storage to the backup appliance/storage over a dedicated Storage Area Network (SAN/Fibre Channel/iSCSI) or dedicated storage fabric or dedicated backup LAN. Production Ethernet/LAN infrastructure must be completely bypassed,

पंजाब एण्ड सिंध बैंक *(भारत सरकार का उपक्रम)* ***प्रधान कार्यालय: सूचना प्रौद्योगिकी विभाग,*** ***द्वितीय तल, भूखंड संख्या-151,*** ***सेक्टर-44, संस्थागत क्षेत्र,*** ***गुरुग्राम– 122003*** *Email: ho.it@psb.bank.in*		***Punjab & Sind Bank*** *(A Govt. Of India Undertaking)* ***H.O. Information Technology Dept.,*** ***2nd Floor, Plot No. 151,*** ***Sector -44, Institutional Area,*** ***Gurugram - 122003*** *Email: ho.it@psb.bank.in*

Addendum 1

S. No.	RFP Section no.	RFP Page No.	RFP Clause	Modified Clause
				restricting its use strictly to minor control traffic and metadata orchestration.
90.	Appendix 1A, DAM – 82		The solution shall support inbult authentication and integration with enterprise Identity and Access Management (IAM) platforms, including LDAP/Active Directory, RADIUS, SAML, TACACS+, and other industry-standard authentication mechanisms.	The solution shall support inbuilt authentication and integration with enterprise Identity and Access Management (IAM) platforms, including LDAP/Active Directory, RADIUS, SAML, and other industry-standard authentication mechanisms
91.	Appendix 1A, DAM – 113		The solution should expose its security capabilities through a standardized protocol-based interface (MCP) enabling AI agents and orchestration platforms to dynamically discover and invoke platform capabilities without custom integration.	Clause Stands Deleted
92.	Appendix 1A, SSLo + Packet Broker (SSL Orchestrator) – 1.3		System must have 24 x 1/10 G and 1Option of 4 x 100 G ports	System must have 16 x 1/10/25 G and 1 Option of 4 x 100 G ports
93.	Appendix 1A, SSLo + Packet		System must support resource allocation to each context including throughput, CPS, Concurrent connection,SSL throughput	System must support resource allocation to each context including Interface, Memory, SSL Card, Cores.

पंजाब एण्ड सिंध बैंक *(भारत सरकार का उपक्रम)* ***प्रधान कार्यालय: सूचना प्रौद्योगिकी विभाग,*** ***द्वितीय तल, भूखंड संख्या-151,*** ***सेक्टर-44, संस्थागत क्षेत्र,*** ***गुरुग्राम– 122003*** *Email: ho.it@psb.bank.in*		***Punjab & Sind Bank*** *(A Govt. Of India Undertaking)* ***H.O. Information Technology Dept.,*** ***2nd Floor, Plot No. 151,*** ***Sector -44, Institutional Area,*** ***Gurugram - 122003*** *Email: ho.it@psb.bank.in*

Addendum 1

S. No.	RFP Section no.	RFP Page No.	RFP Clause	Modified Clause
	Broker (SSL Orchestrator) – 3.3			
94.	Appendix 1A, SSLo + Packet Broker (SSL Orchestrator) – 6.9		System must support bump in a wire deployment mode	System must support bump in a wire/L3 deployment mode without requiring changes to the Bank's existing NAT, IP addressing, routing, or network configuration. The OEM shall mandatorily submit a written confirmation from the OEM's TAC/authorized technical team on official OEM letterhead, along with the proposed deployment architecture and traffic flow, confirming that the proposed deployment can be implemented without any changes to the Bank's existing network configuration.
95.	Appendix 1A, SSLo + Packet Broker (SSL Orchestrator) – 7.1		System must support VRRP based redundancy	System must support VRRP based redundancy or equivalent

पंजाब एण्ड सिंध बैंक *(भारत सरकार का उपक्रम)* ***प्रधान कार्यालय: सूचना प्रौद्योगिकी विभाग,*** ***द्वितीय तल, भूखंड संख्या-151,*** ***सेक्टर-44, संस्थागत क्षेत्र,*** ***गुरुग्राम– 122003*** *Email: ho.it@psb.bank.in*		***Punjab & Sind Bank*** *(A Govt. Of India Undertaking)* ***H.O. Information Technology Dept.,*** ***2nd Floor, Plot No. 151,*** ***Sector -44, Institutional Area,*** ***Gurugram - 122003*** *Email: ho.it@psb.bank.in*

Addendum 1

S. No.	RFP Section no.	RFP Page No.	RFP Clause	Modified Clause
96.	Appendix 1A, SSLo + Packet Broker (SSL Orchestrator) – 7.4		System must support dynamic VRRP priority by traffic interface, server, next hop and routes	System must support dynamic "VRRP or an equivalent mechanism" priority by traffic interface, server, next hop and routes
97.	Appendix 1A, SSLo + Packet Broker (SSL Orchestrator) – 8.5		System must support REST-style XML API (aXAPI) for all functions	System must support REST-API for all functions.
98.	Appendix 1A, WAF) – 90		The proposed WAF solution must support high availability in both Layer 2 and Layer 3 deployments. It must include either an inbuilt bypass switch or be supplied with an external bypass switch to ensure uninterrupted traffic flow during maintenance or failure.	The proposed WAF solution must support high availability in both Layer 2 and Layer 3 deployments.

पंजाब एण्ड सिंध बैंक *(भारत सरकार का उपक्रम)* ***प्रधान कार्यालय: सूचना प्रौद्योगिकी विभाग,*** ***द्वितीय तल, भूखंड संख्या-151,*** ***सेक्टर-44, संस्थागत क्षेत्र,*** ***गुरुग्राम– 122003*** *Email: ho.it@psb.bank.in*		***Punjab & Sind Bank*** *(A Govt. Of India Undertaking)* ***H.O. Information Technology Dept.,*** ***2nd Floor, Plot No. 151,*** ***Sector -44, Institutional Area,*** ***Gurugram - 122003*** *Email: ho.it@psb.bank.in*

Addendum 1

S. No.	RFP Section no.	RFP Page No.	RFP Clause	Modified Clause
99.	Appendix 1A, HIPS) – 3		The proposed server security solution must support multiple platforms of server operating systems i.e. AIX, Alma Linux, Amazon Linux, CentOS, Cloud Linux, Debian Linux, Miracle Linux, Oracle Linux, RHEL, RedHat OpenShift, Rocky Linux, Solaris, Suse, Ubuntu, Windows, Docker, Docker CE, Docker EE.	The proposed server security solution must support multiple platforms of server operating systems i.e. Windows, Linux RedHat, CentOS, Oracle, Debian, SUSE, Ubuntu, Amazon Linux, Solaris etc. for the OS versions which are under active support from respective OEM's
100.	Appendix 1A, HIPS) – 25		The solution should include a Log Inspection module capable of capturing and analyzing system logs, providing audit evidence to meet PCI DSS or internal requirements within your organization. Additionally, the solution should have the ability to forward suspicious events to an SIEM system or centralized logging server for correlation, reporting, and archiving purposes.	The HIPS solution shall provide real-time monitoring and analysis of host-level security events and generate alerts based on predefined and administrator-configurable security rules. The solution should support forwarding such events/logs depending on the severity of the event to the Bank's SIEM for monitoring, correlation, investigation, reporting, and retention
101.	Appendix 1B, Load Balancer – 23		Should support QOS for traffic prioritization, CBQ , borrow and unborrow bandwidth from queues. It should provide QOS filters based on port and protocols including TCP, UDP and ICMP Protocols. Should support rate shaping for setting user defined rate limits on critical application.	Should support QOS for traffic prioritization, borrow and unborrow bandwidth from queues. It should provide QOS filters based on port and protocols including TCP, UDP and ICMP Protocols. Should support rate shaping for setting user defined rate limits on critical application.

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
1	100	10.2	Eligibility Evaluation Criteria	The bidder should have a minimum average annual turnover of INR 1000 crore in India during the last 3 financial years (i.e. 2022-23, 2023-24 & 2024–25) along with positive net worth.	Request to modify the clause: The bidder should have a minimum average annual turnover of INR 375 crore in India during the last 3 financial years (i.e. 2022-23, 2023-24 & 2024–25) along with positive net worth.	Please refer Addendum 1 for the revised clause.
2	101	10.2	Eligibility Evaluation Criteria	Bidder must have at least enrolled manpower (on bidder's payroll) of 150 experienced employees skilled in areas of Cyber/IT security.	Request to modify the clause: Bidder must have at least enrolled manpower (on bidder's payroll) of 50 experienced employees skilled in areas of Cyber/IT security.	Please refer Addendum 1 for the revised clause.
3	100	10.2	Eligibility Evaluation Criteria	The bidder should be an authorized representative/ partner/ reseller of each of the proposed OEMs in India. MAF should be submitted from the following solution OEMs: 1. Anti-Distributed Denial of Services (Anti-DDoS) 2. SSL Orchestrator along with packet broker 3. DNS protection (Internal DNS Security) 4. Web Gateway 5. Zero-Day Attack Protection at Endpoint and network 6. Zero Trust Network Access (ZTNA) 7. Data Loss Prevention (DLP) 8. Information/Digital Right Management 9. Database Activity Monitoring 10. Mobile SDK 11. Host IPS including Application Change Control (HIPS) 12. Web Application Firewall (WAF) 13. Centralized key management solution 14. Certificate Lifecycle management 15. Identity & Access Management Solution 16. Multi Factor Authentication 17. Privilege Identity/Access Management 18. DNS Security Services (Internet-Facing DNS Security Services) 19. Cloud Access Security broker (CASB) 20. AI Security 21. SBOM/CBOM/AIBOM/QBOM	Request to modify the clause: The bidder should be an authorized representative/ partner/ reseller of atleast 5 of the below proposed OEMs in India. MAF should be submitted from the following solution OEMs: 1. Anti-Distributed Denial of Services (Anti-DDoS) 2. SSL Orchestrator along with packet broker 3. DNS protection (Internal DNS Security) 4. Web Gateway 5. Zero-Day Attack Protection at Endpoint and network 6. Zero Trust Network Access (ZTNA) 7. Data Loss Prevention (DLP) 8. Information/Digital Right Management 9. Database Activity Monitoring 10. Mobile SDK 11. Host IPS including Application Change Control (HIPS) 12. Web Application Firewall (WAF) 13. Centralized key management solution 14. Certificate Lifecycle management 15. Identity & Access Management Solution 16. Multi Factor Authentication 17. Privilege Identity/Access Management 18. DNS Security Services (Internet-Facing DNS Security Services) 19. Cloud Access Security broker (CASB) 20. AI Security 21. SBOM/CBOM/AIBOM/QBOM	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
4	101	e	Eligibility Evaluation Criteria	Bidder should have supplied, installed and maintained (or under maintenance) at least 10 of the below solutions in any one PSU/PSE/ BFSI/Government Organizations/ Regulatory & Statutory body in India: 1. Anti-Distributed Denial of Services (Anti-DDoS) 2. SSL Interception/SSL offloader 3. DNS protection (Internal DNS Security) 4. Web Gateway 5. Zero-Day Attack Protection at Endpoint and network/Anti-APT 6. Zero Trust Network Access (ZTNA)/Remote Access VPN 7. Data Loss Prevention (DLP) 8. Information/Digital Right Management 9. Database Activity Monitoring 10. Mobile SDK 11. Host IPS including Application Change Control (HIPS) 12. Web Application Firewall (WAF) (Mandatory Requirement) 13. Centralized key management solution 14. Certificate Lifecycle management 15. Identity & Access Management Solution 16. Multi Factor Authentication/2FA 17. Privilege Identity/Access Management 18. DNS Security Services (Internet-Facing DNS Security Services) Note: - a. Experience of solutions can be shown in single /multiple Clients/ work orders meeting the above criteria b. A bidder's experience in supplying and installing a solution will be considered regardless of when the installation was completed. Even if the installation was completed more than five years ago, it will still qualify, provided the bidder is currently maintaining that solution or has carried out its maintenance at any time during the five-year period preceding the RFP publication date.	Request to modify the clause: Bidder should have supplied, installed and maintained (or under maintenance) at least 3 of the below solutions in any one PSU/PSE/ BFSI/Government/Large Enterprise Organizations/ Regulatory & Statutory body in India: 1. Anti-Distributed Denial of Services (Anti-DDoS) 2. SSL Interception/SSL offloader 3. DNS protection (Internal DNS Security) 4. Web Gateway 5. Zero-Day Attack Protection at Endpoint and network/Anti-APT 6. Zero Trust Network Access (ZTNA)/Remote Access VPN 7. Data Loss Prevention (DLP) 8. Information/Digital Right Management 9. Database Activity Monitoring 10. Mobile SDK 11. Host IPS including Application Change Control (HIPS) 12. Web Application Firewall (WAF) / Network Firewall (Mandatory Requirement) 13. Centralized key management solution 14. Certificate Lifecycle management 15. Identity & Access Management Solution 16. Multi Factor Authentication/2FA 17. Privilege Identity/Access Management 18. DNS Security Services (Internet-Facing DNS Security Services)	Please be guided by the RFP
5	11	1.3 - SSL Orchestrator	Technical Specifications	System must have 24 x 1/10 G and 1Option of 4 x 100 G ports	Request to change clause as "System must have 16 x 10/25 G and 1Option of 4 x 100 G ports" Justification : OEM Specific clause. Hence request to change clause for maximum participation.	Please refer Addendum 1 for the revised clause.
6	11	2.1 - SSL Orchestrator	Technical Specifications	System must support 150 K SSL offload CPS on RSA 2 K Key and 90 K SSL offload CPS on ECDHE cipher	Request to change clause as "System must support 110 K SSL offload CPS on RSA 2 K Key and 90 K SSL offload CPS on ECDHE cipher.Proposed solution's software/firmware are architecturally capable of supporting National Institute of Standards and Technology (NIST) approved Post-Quantum Cryptography (PQC) algorithms (including but not limited to ML-KEM/FIPS 203) and Device should be ready and support NIST approved PQC algorithm as part of firmware/IOS/ hardware upgrade during its lifetime without any additional cost. " Justification : Post-Quantum Cryptography (PQC) is emerging as the mandatory security standard across the banking industry, to counteract future quantum computing threats. We strongly advise the Bank to mandate this feature to safeguard its application infrastructure. 150K SSL TPS is restricting us from participation, hence request to amend this clause.	Please be guided by the RFP
7	11	2.3 - SSL Orchestrator	Technical Specifications	System must support 64 million concurrent IP sessions and 2 M SSL sessions	Request to change clause as "System must support 64 million concurrent IP sessions and 30M HTTP request per second" Justification : OEM Specific clause. This clause is restricting leading SSL-o OEMs. Most of the leading OEMs of SSL-o does not publish SSL Sessions, once SSL is terminated device maintains either HTTP request per second or L4 connections per second. Hence request to change clause for maximum OEMs participation.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
8	11	3.1 - SSL Orchestrator	Technical Specifications	System must support 30 Partition/Virtual Context keeping in view that One virtual partition will do decryption and another will do re-encryption	Request to change clause as "System must have option of 20 Partition/Virtual Context keeping in view that One virtual partition will do decryption and another will do re-encryption" Justification : Deployment of the SSl-o should not restrictive to Virtual Context, Every OEMs had different architecture to achieve the SSl-o functionalities. Hence request to change clause for maximum OEMs participation.	Please be guided by the RFP
9	12	4.1 - SSL Orchestrator	Technical Specifications	System must support protection from Fragmented packets	These clauses are for Packet broker. Request to remove it from SSl-o section. Justification : OEM Specific clause. Only single OEM provide both Packet broker and SSL inspection solution. This solution is providing undue advantage to single OEM. Intelligent Packet Solution mostly address: Advanced L2-L4 preprocessing, including packet slicing, stripping of encapsulation tags (VLAN, MPLS, VXLAN, GRE, ERSPAN), and de-duplication before reaching security tools. While SSL-o Address below use cases: High-Capacity SSL Offload: Sustained throughput of SSL offload CPS (RSA 2K Keys) and on modern ECDHE and PQC ciphers. Deep L7 Policy Control: Supports URL category bypasses, STARTTLS protocol upgrades (SMTP, IMAP, POP3, FTPS), and programmable traffic scripting (TCL) to dynamically route traffic based on highly specific criteria. Decrypted Traffic Isolation: Mandates that decrypted plaintext traffic is strictly restricted to isolated segments facing authorized security tools and must never leak back into the production networks. As these are two different technologies and only single OEM provide the 2 technology, hence request bank to sperate the Packet Broker and SSL-o requirements.	Please be guided by the RFP. The Bank clarifies that the Packet Broker and SSL Orchestrator (SSLO) are separate solution components and may be proposed as separate products. However, the requirement for a Packet Broker solution remains mandatory and shall be complied with as specified in the RFP/tender. The Packet Broker and SSLO solutions shall comply with all applicable eligibility and OEM evaluation requirements (respectively) stipulated under Clause 18 – OEM Evaluation Criteria of the RFP. The Bidder shall remain responsible for ensuring end-to-end compatibility, tight integration, and coordinated support between the Packet Broker and SSLO components throughout the contract period.
10	12	4.2 - SSL Orchestrator	Technical Specifications	System must support protection from IP Option .The System should have in-built HSM or a third-party HSM supplied by the bidder, which must be integrated with the proposed solution		
11	12	4.3 - SSL Orchestrator	Technical Specifications	System must support protection from Land Attack		
12	12	4.4 - SSL Orchestrator	Technical Specifications	System must support protection from Packet Deformity Layer 3		
13	12	4.5 - SSL Orchestrator	Technical Specifications	System must support protection from Packet Deformity Layer 4		
14	12	4.6 - SSL Orchestrator	Technical Specifications	System must support protection from Ping of Death		
15	12	4.7 - SSL Orchestrator	Technical Specifications	System must support protection from TCP No Flag		
16	12	4.8 - SSL Orchestrator	Technical Specifications	System must support protection from TCP Syn Fin		
17	12	4.9 - SSL Orchestrator	Technical Specifications	System must support protection from TCP Syn Frag		
18	12	4.10 - SSL Orchestrator	Technical Specifications	System must support connection limit based on source IP		
19	12	4.11 - SSL Orchestrator	Technical Specifications	System must support connection rate limit based on source IP		
20	12	4.12 - SSL Orchestrator	Technical Specifications	System must support request rate limit based on source IP		
21	12	4.15 - SSL Orchestrator	Technical Specifications	SSL/TLS Orchestrator Throughput (Gbps): The proposed solution should comply with the sustained throughput figure for the decrypt-inspect-re-encrypt cycle with all security features active simultaneously (rather than throughput under idealized or feature-disabled conditions)	Request to change clause as "SSL/TLS Orchestrator Throughput (Gbps): The proposed solution should comply with the sustained throughput figure for the decrypt-inspect-re-encrypt cycle with all security features active simultaneously (rather than throughput under idealized or feature-disabled conditions). Solution must support minimum 70Gbps of SSL throughput " Justification : SSL/TLS throughput is key sizing requirement for SSL-o solution. Hence to ensure right sizing of solution we request bank to mention the SSL throughput.	Please be guided by the RFP
22	12	6.9 - SSL Orchestrator	Technical Specifications	System must support bump in a wire deployment mode	Request to change Clase as "System must support bump in a wire / L2 deployment mode" Justification : Every OEMs has different architecture to achieve the overall functionalities of SSL-o. As per best practice SSL-o must be deployed in L3 and L2 mode to act as Proxy between client and Application Server. Bump in the wire will defeat the purpose of security architecture. This clause is restricting Many OEMS from participation, hence request to change the clause for maximum OEM participation.	Please refer Addendum 1 for the revised clause.

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
23	12	6.15 - SSL Orchestrator	Technical Specifications	New Clause	Request to add new clause "The SSLV should support readymade templates for following security devices in service chain 1. Checkpoint Security Gateway - Layer 2 & Layer 3 & TAP 2. Cisco Firepower Threat defence - Layer 2 & Layer 3 & TAP 3. Fireeye NX inline - Layer 2 & TAP 4. Gigamon Inline Layer 2 5. Ixia Inline Layer 2 6. Palo Alto NGFW - Layer 3 & TP Layer 2 & TAP 7. Cisco SWA HTTP Proxy 8. Forcepoint SWG HTTP PROXY 9. Fortinet SWG HTTP PROXY 10. McAFee SWG HTTP PROXY 11. Menlo SWG HTTP PROXY 12. Digital Guardian DLP via ICAP 13. MCAfee DLP via ICAP 14. OPSWAT Metadefender via ICAP 15. SQUID ICAP 16. Symantec DLP ICAP 17. NETSCOUT TAP" Justification : This clause ensures the Bank acquires a best-of-breed SSL-O solution that integrates seamlessly and reliably, eliminating the need for complex, proprietary customization. Furthermore, because SSL-O serves as one of the Bank's most critical security controls, this approach guarantees maximum operational simplicity and ease of management for system administrators. Hence request to add this clause.	Please be guided by the RFP
24	12	7.1 - SSL Orchestrator	Technical Specifications	System must support VRRP based redundancy	Request to change clause as "System must support VRRP based redundancy or equivalent" Justification : Every OEM use different protocol to achieve the redundancy. Hence request to change this clause for maximum OEM participation.	Please refer Addendum 1 for the revised clause.
25	13	7.4 - SSL Orchestrator	Technical Specifications	System must support dynamic VRRP priority by traffic interface, server, next hop and routes	Request to change clause as "System must support dynamic VRRP priority by traffic interface, server, next hop and routes or equivalent" Justification : Every OEM use different protocol to achieve the redundancy. Hence request to change this clause for maximum OEM participation.	Please refer Addendum 1 for the revised clause.
26	36	12 - WAF	Technical Specifications	The proposed solution must support dedicated 5 Gbps of WAF throughput (HTTP/HTTPS). The bidder must provide evidence of throughput through publicly available documents /evidence based document supporting the same which needs to be submitted along with the proposal and same needs to showcased if asked by bank during Presentation & UAT (Undertaking from the OEM is not accepted in this case).	Request to change clause as "The proposed solution must support dedicated 5 Gbps of WAF throughput (HTTP/HTTPS) / L7 Throughput of 60Gbps/SSL Throughput of 30Gbps . The bidder must provide evidence of throughput through publicly available documents /evidence based document supporting from the same which needs to be submitted along with the proposal and same needs to showcased if asked by bank during Presentation & UAT " Justification : OEM Specific clause. WAF throughput depends on multiple parameters like application object size, http request per connections, type of SSL encryption/decryption etc. Also WAF throughput asked in RFP is for HTTP/HTTPS. This clause is specific to single OEM which only publish WAF throughput. This clause is restrictive to single OEM hence request to change clause for maximum OEM participation.	Please be guided by the RFP
27	36	14 - WAF	Technical Specifications	The Proposed WAF should support minimum 30000 RSA Per SEC (2048 BIT) & 10000 TPS with ECC and < 5ms latency	Request to change clause as "The Proposed WAF should support minimum 30000 RSA Per SEC (2048 BIT) & 10000 TPS with ECC and minimum latency" Justification : Latency depends on the multiple factors and providing <5ms number is difficult for every OEMs. This clause is restricting leading WAF OEMs from participation. Request to change clause for maximum participation.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
28	39	90 - WAF	Technical Specifications	The proposed WAF solution must support high availability in both Layer 2 and Layer 3 deployments. It must include either an inbuilt bypass switch or be supplied with an external bypass switch to ensure uninterrupted traffic flow during maintenance or failure.	Request to change clause as "The proposed WAF solution must support high availability in both Layer 2 and Layer 3 deployments." Justification : As solution is asked in HA mode to deploy in L3 and L2 mode. Even if single device goes down it will failover to backup appliance. Introducing Bypass switch will bypass the WAF security layer and applications will be exposed to Internet. It is highly recommend to deploy WAF in HA mode without Fail-open switch. No bank deployed WAF in Bypass mode which leads to the security breach. This clause is also specific to single OEM hence request to change clause for maximum OEM participation.	Please refer Addendum 1 for the revised clause.
29	39	92 - WAF	Technical Specifications	The solution must have bypass segments to ensure that fail open in case of hardware failure	Request to change clause as "The solution must have capability to ensure fallback to backup device in case of hardware failure. Justification : As solution is asked in HA mode to deploy in L3 and L2 mode. Even if single device goes down it will failover to backup appliance. Introducing Bypass switch will bypass the WAF security layer and applications will be exposed to Internet. It is highly recommend to deploy WAF in HA mode without Fail-open switch. No bank deployed WAF in Bypass mode which leads to the security breach. This clause is also specific to single OEM hence request to change clause for maximum OEM participation.	Please be guided by the RFP
30	39	95 - WAF	Technical Specifications	The solution shall provide built-in Vulnerability Assessment to identify web application vulnerabilities, with the WAF automatically enforcing Virtual Patching policies to protect applications without requiring application code changes. As per the guidelines by Govt Body.	Request to change clause as "The solution shall provide integration with leading Vulnerability Assessment tools to identify web application vulnerabilities, with the WAF automatically enforcing Virtual Patching policies to protect applications without requiring application code changes. As per the guidelines by Govt Body." Justification : This clause is restricting leading WAF OEM from participation and it is specific to single OEM. Request to change clause for maximum OEM participation.	Please be guided by the RFP
31	68	2 - DNS Security	Technical Specifications	DNS Platform should be purpose-built exclusively to serve DNS traffic to avoid any inter-dependency on other solutions on the provider's platform. DNS Platform to have 1000+ POPs globally with multiple POPs in India as well.	Request to change clause as "DNS Platform should be purpose-built exclusively to serve DNS traffic to avoid any inter-dependency on other solutions on the provider's platform. DNS Platform to have 30+ POPs globally with multiple POPs in India as well." Justification : With 1000+ POP is restricting many leading DNS Security solution provers from participation. As banks applications are hosted in India hence request you to reduce the global POP to 30.	Please be guided by the RFP
32	68	7 - DNS Security	Technical Specifications	Authoritative DNS services should be ISO 27001:2013 & ISO 27701:2019 compliant	Request to change clause as "Authoritative DNS services should be ISO 27001:2013 & ISO 27701:2019 or ISO 27018 / SOC 2 Type II compliant" Justification : ISO 27018 / SOC 2 addresses the rigorous data privacy, controller, and processor requirements of the General Data Protection Regulation (GDPR) and other global privacy laws. Hence request to amend the clause.	Please refer Addendum 1 for the revised clause.
33	69	43 - DNS Security	Technical Specifications	Pricing for DNS or GSLB Solution must not be dynamic or traffic consumption based e.g. Based on DNS queries or traffic served. There should not be any extra cost to absorb DDoS attack traffic handled by the DNS platform for Bank DNS Zones or GSLB. Pricing should be predictable & Flat based on the number of DNS zones or GSLB configurations as per Bank's requirement.	Request to remove this clause as every OEM have different licensing construct. Justification : This clause is restricting leading DNS Security provider from Participation. Hence Request to remove the clause.	Please be guided by the RFP
34	14	2 - Load Balancer	Technical Specifications	The Appliance should have dedicated 1x1GbE port for management and 4x10GbE SFP+ ports and multicore CPU, minimum 4 TB HDD and dual power supply.	Request to change clause as "The Appliance should have dedicated 1x1GbE port for management and 4x10GbE SFP+ ports and multicore CPU, minimum 480GB HDD and dual power supply." Justification : This clause is providing undue advantage to single OEM. Every OEM solution need storage capacity based on the underlying OS architecture e.g. for windows OS system it require more storage compare to linux. Due to this clause other leaders OEMs in ADC are unble to qualify. If bank's storage requirement is for log retention every OEMs have Management solution which can cater upto log retention of 180 days as per Cert-in guideline. Request to change this clause for fair participation all leading ADC OEMs.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
35	15	23 - Load Balancer	Technical Specifications	Should support QOS for traffic prioritization, CBQ , borrow and unborrow bandwidth from queues. It should provide QOS filters based on port and protocols including TCP, UDP and ICMP Protocols. Should support rate shaping for setting user defined rate limits on critical application.	Request to change clause as "Should support QOS for traffic prioritization, borrow and unborrow bandwidth from queues. It should provide QOS filters based on port and protocols including TCP, UDP and ICMP Protocols. Should support rate shaping for setting user defined rate limits on critical application." Justification : OEM specific clause, hence request to change clause for maximum OEM participation.	Please refer Addendum 1 for the revised clause.
36	15	35 - Load Balancer	Technical Specifications	New Clause	Proposed solution's software/firmware are architecturally capable of supporting National Institute of Standards and Technology (NIST) approved Post-Quantum Cryptography (PQC) algorithms (including but not limited to ML-KEM/FIPS 203) and Device should be ready and support NIST approved PQC algorithm as part of firmware/IOS/ hardware upgrade during its lifetime without any additional cost. " Justification : Post-Quantum Cryptography (PQC) is emerging as the mandatory security standard across the banking industry, to counteract future quantum computing threats. We strongly advise the Bank to mandate this feature to safeguard its application infrastructure. 150K SSL TPS is restricting us from participation, hence request to amend this clause.	Please be guided by the RFP
37	28	A. Perimeter & Network Security	Web Gateway Solution	Deployment Model - On Premise at DC and DR	We request to modify the clause of Deployment model as Hybrid Model now most of the security vendor provides their management module from their Meity empanneled cloud and data processing through their on-premise virtual appliance and hence data processing never leaves Bank boundaries	Please be guided by the RFP
38	18	Appendix 1A functional Specifications	Secure Web Gateway	The solution should be on premise appliance based and must Provide Web Proxy, Caching, Web based Reputation filtering, URL filtering, Antivirus, Antimalware, Enterprise Data protection control with minimum 1500 templates inbuilt with English Language support, Application Visibility & control, Detail Reporting and Management. . Load balancing should be inbuilt in the appliance or should work with Bank's existing load balancer with no additional cost.	We request you to modify the clause as "The solution should be on premise/hybrid appliance/virtual appliance based and must Provide Web Proxy, Web based Reputation filtering, URL filtering, Antivirus, Antimalware, Enterprise Data protection control with minimum 1500 templates inbuilt with English Language support, Application Visibility & control, Detail Reporting and Management. . Load balancing should be inbuilt in the appliance or should work with Bank's existing load balancer with no additional cost." Reason for Change : Physical on-premise-only mandate and inbuilt Caching unnecessarily exclude modern virtual/hybrid SWG solutions that deliver equivalent or superior security without added value from a legacy, largely-irrelevant-for-encrypted-traffic feature.	Please be guided by the RFP
39	18	Appendix 1A functional Specifications	Secure Web Gateway	The solution should provide the SSL decryption cability within the appliance itself and should be able to inspect malicious information leaks even over SSL by decrypting SSL natively and Data exfiltration control asked in the RFP should natively be applied on same hardware. The appliance should have provision of separate Network Interface for Management ports and Data ports.	We request you to modify the clause as "The solution should provide the SSL decryption cability within the appliance itself and should be able to inspect malicious information leaks even over SSL by decrypting SSL natively and Data exfiltration control asked in the RFP should natively be applied on same hardware/virtual appliance. " Reason for Change Native SSL decryption and data exfiltration control are functional security requirements, not tied to physical form factor — restricting them to hardware-only, with mandatory separate NICs, unnecessarily excludes equally capable virtual appliance solutions and limits competition without adding security value.	Please be guided by the RFP
40	18	Appendix 1A functional Specifications	Secure Web Gateway	Single solution or combination of solution proposed should have proxy & caching with URL filtering. Also provides Real time content classification, categorization and security scanning in built with proxy solution. Proxy filtering and Web Data security for on prem bank user's must run on same appliance.	We request you to modify the clause as " Single solution or combination of solution proposed should have proxy with URL filtering. Also provides Real time content classification, categorization and security scanning in built with proxy solution. Proxy filtering and Web Data security for on prem bank user's must run on same appliance." Reason for Change - Caching is a legacy bandwidth-optimization feature unrelated to security efficacy, and with most web traffic now encrypted (HTTPS), caching benefits are minimal; mandating it restricts participation to legacy on-prem proxy appliances and excludes modern cloud-native/SASE-based secure web gateway solutions without any corresponding security benefit.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
41	18	Appendix 1A functional Specifications	Secure Web Gateway	The solution should provide proxy, caching, content filtering, SSL inspection, inline AV(Anti-Virus) protocol filtering. The solution should have more than 1500+ predefined templates to prevent the confidential information in block mode with the visibility to provide the sanctioned and unsanctioned application visibility and control. Solution should provide the details and reports for the data exfiltration happening in the password and encrypted files uploads over the web natively.	We request you to modify the clause as " The solution should provide proxy, content filtering, SSL inspection, inline AV(Anti-Virus) protocol filtering. The solution should have more than 1500+ predefined templates to prevent the confidential information in block mode with the visibility to provide the sanctioned and unsanctioned application visibility and control. Solution should provide the details and reports for the data exfiltration happening in the password and encrypted files uploads over the web natively. Reason for Change - Removing "caching" as a mandatory requirement broadens vendor eligibility to solutions that deliver proxy-based security functions without a dedicated caching engine, since caching is largely obsolete for modern SSL-encrypted traffic	Please be guided by the RFP
42	19	Appendix 1A functional Specifications	Secure Web Gateway	The proposed solution's proxy gateway should be a hardware appliance for Secure Web Gateway solution and should not be dependent on virtualization platforms. However any other component required to run the solution like management, DB, etc. can be provided as software but bidder to provision the required compute.	We request you to modify the clause as " The proposed solution's proxy gateway should be a hardware/virtual appliance for Secure Web Gateway solution. However any other component required to run the solution like management, DB, etc. can be provided as software but bidder to provision the required compute." Reason for Change - Allowing a virtual appliance option gives flexibility to leverage existing virtualization infrastructure, reducing hardware costs and deployment time without compromising security functionality.	Please be guided by the RFP
43	19	Appendix 1A functional Specifications	Secure Web Gateway	The proposed solution should store and Process all Proxy policies and configurations locally on the proposed hardware appliances or in the solution and should not leave bank's premises at any point of time.	We request you to modify the clause as " The proposed solution should store and Process all Proxy policies and configurations locally on the proposed hardware/virtual appliances or in the solution and should not leave bank's premises at any point of time" Reason for Change - Adding "virtual" accommodates virtual appliance deployments (not just physical hardware) while still keeping all data processing strictly on-premises.	Please be guided by the RFP
44	41	7.3.2 Information/Digital Right Management	Key Deliverables	1.(i) Data Classification Rules	Kindly clarify, if the DRM solution is expected to have in built capability to classify documents as part of its functionality. Additionally, since 200 licenses are requested for the DRM solution, please confirm that the document classification capability—if required—will apply only to these 200 users.	The proposed DRM solution shall also support integration with the Bank's data/document classification mechanisms and shall be capable of applying protection policies based on classification labels generated by such mechanisms.
45	42	7.3.2 Information/Digital Right Management	Key Deliverables	10. Pre-built query options for non-technical users	Kindly clarify the expected use case, as the requirement is not clear	The proposed DRM solution shall provide pre-built reports, queries, and dashboards covering commonly required access, usage, policy, and security activities, enabling non-technical users to generate and view reports through a user-friendly interface.
46	104	10.2 Eligibility Evaluation Criteria	18. OEM Evaluation Criteria	Note: Experience should be during the five-year period preceding the RFP publication date. Even if the installation was completed more than five years ago, it will still qualify, provided the product is currently under maintenance or has been maintained at any time during the five-year period preceding the RFP publication date	We request bank to clarify the minimum contract duration that OEM should have completed. We request bank to consider minimum 3 years deployment period, further we will request bank to specify minimum user count to be mentioned for such reference.	Please be guided by the RFP
47	209	15.21.4 Deployment & Data Retention	8. Information/ Digital Rights Management	Admin/Policy & Rules Creator License for 200 users. Any number of users can apply the created policy if provided access to by admin.	We wish to highlight that the DRM licencing is based on number of users, there is no licencing for admin/policy & rule creator. Hence only 200 named users will be able to apply/create policy. Kindly confirm number of users who will be protecting/applying policies to the documents.	The Bank has specifically mentioned a requirement for 200 Administrator Licenses. Accordingly, the proposed solution should provide 200 Licenses for users responsible for administration, policy creation, and rule management.
48	Appendix 1A	DRM Functional Specification	A6	The solution does not have any dependency on software from other vendor for its working.	Kindly clarify, the banks requirement from this clause. The RFP asks for deployment and integration capabilities (like DLP. SIEM etc.) this will have dependency on those software's from other vendors.	Bidder is proposing a consolidated comprehensive IT sEcurity Solution which includes both DLP and DRM, so bidder to identify identify the solution accordingly. The bidder is required to integrate the solution with SIEM
49	Appendix 1A	DRM Functional Specification	A7	The Solution is having integration capability with DLP (Data Loss Prevention) solution and able to apply Keyword based / File Classification based document protection.	The REST APIs/SDK are available for integration with DLP and classification tools to enable automatic protection at the endpoint level. However, for this integration to be feasible, the existing / proposed DLP or classification tool must be capable of consuming these REST APIs/SDK to apply DRM policies. Kindly confirm bank DLP/classification OEM supports consumption of REST APIs/SDK for integrations. Additionally, since DRM licenses required is 200, please confirm that integration capabilities are required only for these 200 users.	Bidder is proposing a consolidated comprehensive IT security Solution which includes both DLP and DRM, so bidder to identify identify the solution accordingly.
50	Appendix 1A	DRM Functional Specification	A14	The solution to deploy latest / strong encryption standards (AES 256) on Email/Documents/Other Files Formats. Bidder shall provide details regarding encryption/algorithm techniques being used in the solution.	Kindly clarify if bank Is looking for integration with its exchange for automatic encryption for emails body and attachments.	The solution to deploy latest / strong encryption standards (AES 256) on Email attachments /Documents/Other Files Formats. Bidder shall provide details regarding encryption/algorithm techniques being used in the solution as a part of the technical proposal and response to the requirement.

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
51	Appendix 1A	DRM Functional Specification	A15	The solution is having document protection capability on various devices i.e. desktops, laptops, tablets, iOS mobile devices fileservers and Android Mobile.	Kindly delete tablets, iOS and Android mobile devices, the user can view protected document on mobile devices but cannot protect them.	The solution is having document protection/ viewing capability on various devices i.e. desktops, laptops, tablets, iOS mobile devices fileservers and Android Mobile.
52	Appendix 1A	DRM Functional Specification	A26	The Solution is supporting all MS Office versions offered by Microsoft and supports dominant MS Office formats (e.g., docx, doc, pptx, xlsx etc.) and pdf with advance permission controls.	Kindly clarify that none of the MS version being used by bank are declared EOL by Microsoft, we support all the versions which are currently under active support from Microsoft	Please be guided by the RFP
53	Appendix 1A	DRM Functional Specification	A30	The solution shall automatically preserve a real-time, immutable and cryptographically verifiable copy of every document protected by the solution and their subsequent versions, either natively or through seamless integration with an bidder proposed on-premise repository solution. The solution shall maintain complete version history, bank-defined retention policies, and a tamper-evident audit trail to ensure document authenticity, integrity and chain of custody for audit, regulatory, legal and forensic purposes.	Kindly delete, the file versioning is not a DRM feature, This is an OEM specific capability. Once the document is protected by DRM no third party solution will be able to decrypt it to provide versioning capabilities.	Bidder is free to propose the DRM solution however file versioning (preserve a real-time, immutable and cryptographically verifiable copy of every document protected by the solution and their subsequent versions) is the mandatory requirement and can be achieved by proposing a separate solution or through seamless integration with an bidder proposed on-premise repository solution.
54	Appendix 1A	DRM Functional Specification	A46	The solution shall support automated folder-based protection for files stored on central file servers or banks-approved repositories. The solution shall automatically apply protection policies to files based on existing data classification labels or other bank-defined labels, without requiring user intervention. The solution shall continuously monitor designated folders and automatically apply or update protection policies for newly created, modified, or reclassified files	Kindly delete "existing data classification labels or other bank-defined labels, and reclassified files" the automatic folder protection is independent of labels and is driven by pre defined policies on the folder. Kindly clarify, if this capability is also needed for 200 users only as per DRM requirement. please specify the type of file server in use at bank (e.g., Windows, Linux, NetApp, EMC, etc.).	Please be guided by the RFP All features and capabilities sought in the RFP shall be for the number of defined users sought.
55	Appendix 1A	DRM Functional Specification	F89	The system should be able to interface with Office365 & Outlook online and seamlessly.	Kindly clarify, interface, ideally any unprotected data which is being shared via any of these tools should be automatically protected based on pre defined policies. Instead of interface, we suggest bank should ask for integration, interface has no practical relevance. Additionally, since 200 licenses are requested for the DRM solution, if required—will apply only to these 200 users.	Please be guided by the RFP All features and capabilities sought in the RFP shall be for the number of defined users sought.
56	Appendix 1A	DRM Functional Specification	F90	The system should be able to interface with MS Teams.		Please be guided by the RFP all features and capabilities sought in the RFP shall be for the number of defined users sought.
57	Appendix 1A	DRM Functional Specification	F91	The system should be able to interface with SharePoint.		Please be guided by the RFP all features and capabilities sought in the RFP shall be for the number of defined users sought.
58	Appendix 1A	DRM Functional Specification	F92	The system should be able to interface with OneDrive.		Please be guided by the RFP all features and capabilities sought in the RFP shall be for the number of defined users sought.
59	Appendix 1A	DRM Functional Specification	F94	The system should be integrated with DLP system of Bank.	The REST APIs/SDK are available for integration with DLP and classification tools to enable automatic protection at the endpoint level. However, for this integration to be feasible, the existing / proposed DLP or classification tool must be capable of consuming these REST APIs/SDK to apply DRM policies. Kindly confirm bank DLP/classification OEM supports consumption of REST APIs/SDK for integrations. Additionally, since DRM licenses required is 200, please confirm that integration capabilities are required only for these 200 users.	Bidder is proposing a consolidated comprehensive IT security Solution which includes both DLP and DRM, so bidder to identify identify the solution accordingly.
60	Appendix 1A	DRM Functional Specification	F95	Interface able to handle exceptions (e.g. will output to log files, retries) when unsuccessful. Able to handle continual processing or gracefully terminated.	Kindly clarify the requirement	Please be guided by the RFP
61	Appendix 1A	DRM Functional Specification	H103	Pre-built query feature for non-programmers	Kindly clarify the expected use case, as the requirement is not clear	Please be guided by the RFP
62	22	6.11	Performance Bank Guarantee/Security Deposit (PBG)	Security Deposit / Performance Guarantee should be submitted by way of Bank Guarantee in favor of Punjab & Sind Bank payable at Delhi / Bank Guarantee may be obtained from any of the Scheduled Commercial Banks (except Cooperative Bank, RRB & Punjab & Sind Bank) for an amount as mentioned in Section 1	As per the latest amendment in GFR 2017 dated 02-02-2022 (Rule 171 of GFR 2017), Performance Security may be obtained in the form of insurance surety bonds, account payee demand draft, banker's cheque, or bank guarantee. Therefore, it is requested to accept an Insurance Surety Bonds or Bank Guarantee towards Perfromance Security.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
63	159	15.5 Annexure 5	Pre-Qualification Criteria	Bidder should have supplied, installed and maintained (or under maintenance) at least 10 of the below solutions in any one PSU/PSE/ BFSI/Government Organizations/ Regulatory & Statutory body in India: 1. Anti-Distributed Denial of Services (Anti-DDoS) 2. SSL Interception/SSL offloader 3. DNS protection (Internal DNS Security) 4. Web Gateway 5. Zero-Day Attack Protection at Endpoint and network/Anti-APT 6. Zero Trust Network Access (ZTNA)/Remote Access VPN 7. Data Loss Prevention (DLP) 8. Information/Digital Right Management 9. Database Activity Monitoring 10. Mobile SDK 11. Host IPS including Application Change Control (HIPS) 12. Web Application Firewall (WAF) (Mandatory Requirement) 13. Centralized key management solution 14. Certificate Lifecycle management 15. Identity & Access Management Solution 16. Multi Factor Authentication/2FA 17. Privilege Identity/Access Management 18. DNS Security Services (Internet-Facing DNS Security Services)	Bidder should have supplied, installed and maintained (or under maintenance) at least 10 of the below solutions in any one PSU/PSE/ BFSI/Government Organizations/ Regulatory & Statutory body / Private Organizations in India: 1. Anti-Distributed Denial of Services (Anti-DDoS) 2. SSL Interception/SSL offloader 3. DNS protection (Internal DNS Security) 4. Web Gateway 5. Zero-Day Attack Protection at Endpoint and network/Anti-APT 6. Zero Trust Network Access (ZTNA)/Remote Access VPN 7. Data Loss Prevention (DLP) 8. Information/Digital Right Management 9. Database Activity Monitoring 10. Mobile SDK 11. Host IPS including Application Change Control (HIPS) 12. Web Application Firewall (WAF) (Mandatory Requirement) 13. Centralized key management solution 14. Certificate Lifecycle management 15. Identity & Access Management Solution 16. Multi Factor Authentication/2FA 17. Privilege Identity/Access Management 18. DNS Security Services (Internet-Facing DNS Security Services)	Please be guided by the RFP
64					OR Bidder should have supplied, installed and maintained (or under maintenance) at least 10 of the below solutions in any one PSU/PSE/ BFSI/Government Organizations/ Regulatory & Statutory body in India: 1. Anti-Distributed Denial of Services (Anti-DDoS) 2. SSL Interception/SSL offloader 3. DNS protection (Internal DNS Security) 4. Web Gateway 5. Zero-Day Attack Protection at Endpoint and network/Anti-APT 6. Zero Trust Network Access (ZTNA)/Remote Access VPN 7. Data Loss Prevention (DLP) 8. Information/Digital Right Management 9. Database Activity Monitoring 10. Mobile SDK 11. Host IPS including Application Change Control (HIPS) 12. Web Application Firewall (WAF) (Bidder / OEM) (Mandatory Requirement) 13. Centralized key management solution 14. Certificate Lifecycle management 15. Identity & Access Management Solution 16. Multi Factor Authentication/2FA 17. Privilege Identity/Access Management 18. DNS Security Services (Internet-Facing DNS Security Services)	
65	116	11 PAYMENT TERMS	11.1 Product (Software) Cost	Product License Cost & Subscription Cost 1) On successful delivery of the licenses which would be considered delivered once the software (with OOTB features) is made available for view and review of the bank on the proposed hardware. The Bidder is required to submit the required to submit the following: □ Delivery proof □ OOTB Installation Proof □ Invoice of the Product = 50%	Considering the OEM paymnet term, it is requested to revise this payment term as : Product License Cost & Subscription Cost 1) On successful delivery of the licenses which would be considered delivered once the software is made available for the bank. The Bidder is required to submit the required to submit the following: □ Delivery proof & Invoice of the product = 70% of product cost with 100% GST of the Invoice	Please be guided by the RFP
66	116	11 PAYMENT TERMS	11.1 Product (Software) Cost	On successful UAT Signoff of the respective product = 20%	On successful installation & UAT Signoff of the respective product = 20% of the product cost	Please be guided by the RFP
67	116	11 PAYMENT TERMS	11.1 Product (Software) Cost	On successful Go-live of the respective product = 30%	On successful Go-live of the respective product = 10% of the product cost.	Please be guided by the RFP
68	117	11 PAYMENT TERMS	11.3 Hardware Cost	Appliance Cost On successful Delivery of the Appliance which would be considered delivered once the solution (with OOTB features) is made available for view and review of the bank. The Bidder is required to submit the required to submit the following: □ Delivery proof □ OOTB Installation Proof □ Invoice of the Product = 50%	Considering the OEM paymnet term, it is requested to revise this payment term as: On successful Delivery of the Appliance which would be considered delivered the bank. The Bidder is required to submit the required to submit the following: □ Delivery proof & Invoice of the Product = 70% of the product cost with 100% GST of the invoice.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
69	117	11 PAYMENT TERMS	11.3 Hardware Cost	On successful UAT Signoff of the respective product = 20%	On successful UAT Signoff of the respective product = 20% of product cost	Please be guided by the RFP
70	117	11 PAYMENT TERMS	11.3 Hardware Cost	On successful Go-live of the respective product = 30%	On successful Go-live of the respective product = 10% of the product cost	Please be guided by the RFP
71	1	Appendix 1A Functional Specification-DAM	13	The solution shall integrate with database encryption technologies where applicable and continue to monitor database activities on encrypted databases	We understand this clause requires the solution to continue monitoring activity on encrypted databases, and that it is met by a host-based agent capturing activity at the database process/memory level — independent of native TDE, file/volume-level encryption and SSL/TLS-encrypted sessions — without requiring encryption keys, keystore or HSM integration. Kindly confirm this interpretation, and confirm that encryption, tokenization and key management, where required, may be delivered through a separately licensed and certified component of the same OEM's data security stack rather than being native to the DAM module. Request the Bank to also share the encryption products and database platforms in use, so co-existence can be confirmed at bid stage.	Please be guided by the RFP
72	1	Appendix 1A Functional Specification-DAM	52	Solution should have capability to track execution of stored procedures, including who executed a procedure, what procedure name and when, which tables were accessed.	We understand this clause is met where the solution records every stored procedure execution — procedure name, executing database user with the correlated application/OS user and source host, timestamp, and input parameters — and provides table/object-level visibility by parsing the SQL and mapping the procedure to the database objects it references, with policy-based alerting and reporting on such executions. Kindly confirm this interpretation, and confirm that objects accessed through dynamic SQL generated at runtime inside a procedure body are outside the scope of this clause. Request the Bank to also share the database platforms and versions in scope.	Please be guided by the RFP
73	1	Appendix 1A Functional Specification-DAM	113	The solution should expose its security capabilities through a standardized protocol-based interface (MCP) enabling AI agents and orchestration platforms to dynamically discover and invoke platform capabilities without custom integration.	We understand this clause is met where the OEM provides an MCP-compliant server/connector that exposes the platform's security capabilities over its documented REST APIs and SDK, deployed alongside the solution, and that the protocol interface need not be embedded within the database security module itself — this being the prevailing implementation pattern across the industry. Given that MCP support in data security products is a very recent introduction, request the Bank to confirm whether the offered MCP capability must be generally available as on the bid date, and whether BFSI production references and deployment counts for this specific capability are required to be submitted. Request the Bank to also confirm that the interface, and any associated AI processing, must be deployed on-premise within the Bank's network, with no data traversing an OEM-hosted or third-party LLM service, and to share the intended AI/orchestration platforms and use cases.	Please refer Addendum 1 for the revised clause.
74		Appendix 1A Functional Specification-DAM	3	The solution shall support horizontal and/or vertical scalability without requiring architectural redesign.	Kindly confirm that scalability will be evaluated in conjunction with the Total Cost of Ownership (TCO), including software, underlying hardware/infrastructure, and associated services such as solution deployment. Also, kindly confirm whether solutions offering the lowest overall TCO for the required scalability will be given preference during evaluation.	Please be guided by the RFP
75	1	Appendix 1A Functional Specification-DAM	105	The Risk Analytics Solution must provide behavior analytics algorithm to establish behavioral baseline and find deviations.	Kindly confirm whether the solution's built-in User and Entity Behavior Analytics is also required to automatically establish behavioral baselines for normal database activity and identify deviations such as unusual access volumes, atypical query patterns, off-hours activity, and privilege misuse, with prioritized and risk-scored anomalies rather than only raw alerts.	Please be guided by the RFP
76	1	Appendix 1A Functional Specification-DAM	119	The Risk Analytics Solution must be able to integrate with Active Directory (AD) to enhance forensics and provide line of sight into user identity.	Kindly confirm whether this requirement extends to attributing database activity to the actual end-user identity (e.g., AD/LDAP user), including scenarios where access is through connection pooling or shared/generic service accounts.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
77	1	Appendix 1A Functional Specification-DAM	97	The solution should automate and simplify regulatory compliance activities and provides superior long-term retention of live audit data in the DAM. It should enable long-term data estate and forensic records retention policies (e.g., fast access, live audit data, length of retention timeframes).	Kindly confirm the Bank's required retention period for long-term archived data. While the RFP specifies a minimum of 1 month of online/searchable audit data, we request the Bank to also specify the required archival retention period (e.g., up to 10 years) to be supported by the solution, with archived data maintained in secure, tamper-proof storage and available for timely retrieval for audit and investigation purposes.	Please be guided by the RFP
78	1	Appendix 1A Functional Specification-DAM	16	The solution shall be able to integrate with leading Next-Gen SOC solutions such as SIEM, S-BDL, SOAR etc. to generate meaningful correlated events. Also, it should be capable of sending all format logs to SIEM/S-BDL	Kindly confirm whether the requirement also includes configurable and automated response playbooks covering alerting, session blocking/quarantine, and ticketing, triggered directly by detected risk events, in addition to standard log/event forwarding to SIEM/SOAR platforms	Bank is in the process of procuring SOAR solution, bidder proposed solution should be integrated with SOAR
79	1	Appendix 1A Functional Specification-DAM	2	The proposed DAM solution should be able to monitor databases in scope without dropping any log.	Kindly confirm the Bank's expected peak sustained transaction throughput (e.g., 60,000+ TPS) that the solution must monitor without dropping any privileged or non-privileged database activity, including adequate capacity for future growth.	Please be guided by the RFP
80	1	Appendix 1A Functional Specification-DAM	75	The proposed solution shall support monitoring of all databases covered under the procured licenses and shall support future expansion. Solution should support the deployment modes i.e. monitoring / blocking separately for each database.	kindly confirm whether the solution must be offered on a SUBSCRIPTION (term) basis rather than a perpetual license, with predictable, usage-based pricing that includes software updates and support for the subscription term, and without large upfront capital outlay or separately priced maintenance.	Please be guided by the RFP
81	203	15.21 Annexure 21: Sizing/Volumetrics, Data Retention and Current Infrastructure	1	Non-Production Environment: For appliance-based solutions, the bidder shall design and propose an appropriate non-production environment to support testing, validation, upgrades, patching, configuration changes, policy tuning, rule testing, and other activities during the contract period without impacting production services. For VM-based solutions, the non-production environment shall be sized at a minimum of 10% of the Production (DC) environment unless otherwise specified in the RFP.	Query for Non-production environment:Kindly clarify the DAM license Volumetrics and availability requirements for the Non-Production environment, including whether the solution is required at the DC, DR, or both locations, and whether a standalone deployment or an HA deployment is required for both locations	Please be guided by the RFP Non-Production environment sizing shall follow the generic methodology prescribed in Annexure 21: for appliance-based solutions, bidder to design and propose an appropriate non-production environment; for VM-based solutions, minimum 10% of Production (DC) environment.
82	162	15.5 Annexure 5: Pre-Qualification Criteria	18	OEM Evaluation Criteria: The proposed OEM solution/product should have been successfully implemented in least two Scheduled bank (including financial regulators). 31. Database Access Management (DAM)	Query: Considering the mission-critical nature of the DAM solution and the scale of the Bank's proposed deployment, we request that the OEM qualification criteria be enhanced to require successful implementation of the proposed DAM solution in at least two Indian banking customers, with each deployment covering 300 or more databases. This would help ensure demonstrated scalability, proven performance, and operational maturity in comparable banking environments. Requesting Bank to change the clause to: "31. Database Access Management (DAM) –with each deployment covering 300 or more databases.	Please be guided by the RFP
83	97	9 - Project Timelines	Overall Implementation period	"Overall Implementation period shall be 5 Months (Start Date is T0) for all solution & services."	what is the timeline for PIM Pam project completion?	Refer Section 9 – Project Timelines: the overall Implementation Period is 5 months from T0 for all solutions and services, including PIM/PAM. Detailed phase-wise/solution-wise milestones shall be part of the Project Plan to be submitted by the bidder
84		ZTNA	Appendix 1A Functional Specification	The ZTNA solution should have device posture validation across multiple parameters like Device Encryption, Registry Check, Process Check, AD Domain Check, OPSWAT and Certificates etc. to provide specific URL or Internet Access based on granular policy controls. The device posture check should be recurring and check the compliance of the posture periodically to maintain the Device Trust.	OPSWAT by product/vendor name makes the requirement implementation-specific rather than outcome-basedAs a vendor neutral Suggested Change The ZTNA solution should have device posture validation across multiple parameters like Device Encryption status, Registry Check, Process Check, AD Domain Check, OPSWAT or Third party posture and certificates/Machine identity etc. to provide specific URL or Internet Access based on granular policy controls. The device posture check should be recurring and check the compliance of the posture periodically to maintain the Device Trust	Please refer Addendum 1 for the revised clause.
85		ZTNA	Appendix 1A Functional Specification	Any component installed in DC's (On-premise) must not need any inbound ACL rule in customer DC/DR Firewall to provide access to Private Application.	If the on-prem gateway is behind another customer perimeter firewall, that perimeter firewall will normally need an ACL/NAT/publishing rule allowing the required Remote Access traffic to reach the gateway.This claue is technically not feasible Suggested Change Remove the clause	Please refer Addendum 1 for the revised clause.

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
86		ZTNA	Appendix 1A Functional Specification	The Solution should have the capability to authenticate users and enroll/log in to the service using their Email Address. This capability should not need any SAML/SSO Integration and admin should be able to send invite links to the user's email to enable this functionality.	The exact email-address-based self-enrollment workflow—where an administrator enters an email address, sends an invitation link, and the user activates an account without SAML/SSO—is natively available in SASE capabilities. It is not the standard workflow of an on-premises Suggested Changes The solution should have the capability to authenticate and enroll users into the service using user id or certificate-based authentication without requiring SAML/SSO integration and admin should be able to send an enrollment invitation, certificate or registration key to the user's registered email address to enable this functionality.	Please be guided by the RFP
87		ZTNA	Appendix 1A Functional Specification	Solution should have Zero trust security and Digital Experience Management (DEM) from Day 1 using the same Endpoint Agent and single management console for both capabilities.	For a on-premises architecture, we provide Zero Trust-style access, session monitoring and operational visibility through:Quantum Security Gateway,VPN Agent, Smart Management,SCV Posture Validation etc. However, the on-premises Remote Access agent does not provide a complete, dedicated Digital Experience Management DEM capability—such as application response time, hop-by-hop path analysis etc (Its available in Cloud platform) and is redirecting to particular vendor. Suggested Changes The solution should have Zero Trust security and centralized user-access and connectivity monitoring from Day 1, using the same endpoint agent and single management console for both capabilities	Please be guided by the RFP
88		ZTNA	Appendix 1A Functional Specification	Connectivity between remote users' devices and private applications should be secured by an end-to-end TLS encrypted tunnel.	We support encrypted IPSEC Tunnels Suggested Changes Connectivity between remote users' devices and private applications should be secured by an TLS or IPSEC encrypted tunnel.	Please be guided by the RFP
89		ZTNA	Appendix 1A Functional Specification	The solution should have Granular policies for blocking or allowing access to private applications that can be built on criteria including User, Group or Organizational Unit (OU), Device Classification and Operating System.	The clause should be modified to avoid tying access control to specific directory constructs or OEM-specific policy attributes. Organizational Unit (OU) is primarily an administrative structure in Active Directory and is not always the most appropriate authorization object. Similarly, Device Classification and Operating System may be consumed by different OEMs as device identity, computer groups, posture attributes, or compliance status rather than as direct rule-base fields. Suggested Change The solution should have granular policies for blocking or allowing access to private applications that can be built on criteria including User, Group or directory attributes such as Organizational Unit, Device Identity/Classification and Operating System.	Please be guided by the RFP
90		ZTNA	Appendix 1A Functional Specification	The solution should provide the capability to add any number of connector in DC without any additional price or license.	We have a different onprim architecture SuggestedChanges The solution should provide the capability to add any number of connector or gateway in DC without any additional price or license.	Please refer Addendum 1 for the revised clause.
91		ZTNA	Appendix 1A Functional Specification	The End-user should not be able to see the Application Local IP even if they are authorized to access the application (application access based on FQDN but real Application IP is masked)	Suggested Changes The End-user should not be able to see the web Application Local IP even if they are authorized to access the application (application access based on FQDN but real Application IP is masked)	Please be guided by the RFP
92		ZTNA	Appendix 1A Functional Specification	The ZTNA components including ZTNA broker, App Connector should be deployed on-premises in SDC	"ZTNA Broker" and "App Connector" are vendor-specific architectural terminologies.We have a different onprim architecture SuggestedChanges The ZTNA components including ZTNA broker, App Connector or Gateway should be deployed on-premises in SDC	Please refer Addendum 1 for the revised clause.
93		ZTNA	Appendix 1A Functional Specification	Solution should be able to provide client/clientless Browser based access to Internal Web Applications from Day 1. It should also support the capability to enforce DLP policies on the access to Internal Web Applications.	The security objective is to prevent unauthorized movement of sensitive information during private application access. Different OEMs may implement this using dedicated DLP, content inspection, data classification or content-aware access controls. SuggestedChanges Solution should be able to provide client/clientless Browser based access to Internal Web Applications from Day 1. It should also support the capability to enforce DLP or content awareness policies on the access to Internal Web Applications.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
94		ZTNA	Appendix 1A Functional Specification	The End point Agent should support multi-user mode installation (for ex. Installing agent on VDI/Thin Clients).	VDI, Terminal Server and Thin Client are different endpoint architectures with different agent deployment models. SuggestedChanges The Endpoint Agent should support multi-user mode installation	Please be guided by the RFP
95		ZTNA	Appendix 1A Functional Specification	The solution should have a single Policy Engine with ZTNA and DEM in a unified/separate console. At any point in time, ZTNA features, and functionality sought should not be compromised. However, ZTNA and DEM should have “single agent deployment” in case agent-based solution deployment is proposed	Referring to Vendor specific as Point no-7- Please remove this clause	Please be guided by the RFP
96		ZTNA	Appendix 1A Functional Specification	The solution should support if required all endpoint- and server-initiated apps, like-to-like VPN replacement adding traffic optimization capabilities for enhanced performance and security.	The term “all server-initiated applications” is technically absolute,connectivity depends on protocol behavior, addressing, routing and endpoint security traffic optimization” should be defined through measurable capabilities such as dynamic split tunneling, QoS, traffic prioritization SuggestedChanges The solution should support,if required, all supported endpoint and supported server-initiated/back-connection applications to provide VPN-equivalent private application connectivity, along with traffic optimization/steering capabilities for enhanced performance and security.”	Please be guided by the RFP
97		ZTNA	Appendix 1A Functional Specification	Solution must support Connector Dashboard provides insight into application traffic,app connector health, and utilization, enabling decision on resource allocation, connection optimization, and troubleshooting.	Suggested ChangesSolution must support Connector or gateway Dashboard provides insight into application traffic,app connector or gateway health, and utilization, enabling decision on resource allocation, connection optimization, and troubleshooting.	Please refer Addendum 1 for the revised clause.
98		ZTNA	Appendix 1A Functional Specification	Solution should support extensive coverage with in-built Data types like Aadhar card, PII, etc with different File Types etc. Solution should support extensive coverage with 100+ in-built Data types with minimum 200 File Types.	Suggested Changes: Solution should support extensive coverage with in-built or customized Data types like Aadhar card, PII, etc with different File Types etc. Solution should support extensive coverage with 100+ in-built Data types with minimum 200 File Types.	Please refer Addendum 1 for the revised clause.
99		ZTNA	Appendix 1A Functional Specification	Connectivity between remote users’ devices and private applications should be secured by an end-to-end TLS encrypted tunnel and optimally routed through with a low latency, high-capacity, scalable network infrastructure.	For an on-premises ZTNA solution, we controls:Endpoint VPN → Quantum Gateway → Security policy but it does not control the entire network path since it depends on the underlying backbone or Infrastructure like ISP,MPLS WAN etc Suggested Changes “Connectivity between remote users’ devices and private applications should be secured using TLS/SSL or IPsec encrypted tunnels. The solution should support optimized gateway/path selection, high availability and load sharing across the available network infrastructure for enhanced performance and scalability.”	Please be guided by the RFP
100		ZTNA	Appendix 1A Functional Specification	The solution should have Granular policies for blocking or allowing access to private applications that can be built on criteria including User, Group or Organizational Unit (OU), Device Classification and Operating System.	The clause should be modified to avoid tying access control to specific directory constructs or OEM-specific policy attributes. Organizational Unit (OU) is primarily an administrative structure in Active Directory and is not always the most appropriate authorization object. Similarly, Device Classification and Operating System may be consumed by different OEMs as device identity, computer groups, posture attributes, or compliance status rather than as direct rule-base fields. Suggested Cheange The solution should have granular policies for blocking or allowing access to private applications that can be built on criteria including User, Group or directory attributes such as Organizational Unit, Device Identity/Classification and Operating System.	Please be guided by the RFP
101		AI Security	Appendix 1A Functional Specification	Allow administrators to permit lower-risk activities (e.g., 'ask a question') while blocking higher-risk activities (e.g., 'upload file', 'paste source code', 'share screen') within the same AI application.	Screen Share is not covered Suggested Change Allow administrators to permit lower-risk activities (e.g., 'ask a question') while blocking higher-risk activities (e.g., 'upload file', 'paste source code') within the same AI application.	Please be guided by the RFP
102		AI Security	Appendix 1A Functional Specification	Maintain and auto-update a cloud/AI application risk-rating database covering data handling, certifications and known incidents for thousands of AI/SaaS apps.	Suggested Change Maintain and auto-update a cloud/AI application risk-rating database covering data handling and known incidents for thousands of AI/SaaS apps.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
103		AI Security	Appendix 1A Functional Specification	The proposed solution should not be dependent on any on-premise device/NGFW to provide SaaS or Gen AI app activity controls such as upload, share, post, AI post, comment, send, create, modify, download, etc , nor by any DLP solution for data at rest it has to be inline	We support allow, ask, block, prevent, detect and redact controls for chat, prompt and paste. Additionally, allow and block access controls and tool controls. Suggested Change The proposed solution should not be dependent on any on-premise device/NGFW to provide SaaS or Gen AI app activity controls such as upload, share, post, send etc , nor by any DLP solution for data at rest it has to be inline	Please be guided by the RFP
104		AI Security	Appendix 1A Functional Specification	The proposed solution should provide DLP-level controls to block and monitor data exfiltration over Gen-AI apps, including detailed user coaching that redirects users to corporate Gen AI apps, with an option for users to justify business use case before interacting further.	We have DLP level controls but no user coaching and redirecting. We can instead block or allow access to apps and websites. We also provide the ask option for users to provide justification. Suggested Changes The proposed solution should provide DLP-level controls to block and monitor data exfiltration over Gen-AI apps, with an option for users to justify business use case before interacting further	Please refer Addendum 1 for the revised clause.
105		AI Security	Appendix 1A Functional Specification	The proposed solution should inspect Model Context Protocol (MCP) servers for bi-directional data sharing between apps, agents, and LLMs (including via CLI), and provide visibility/granular activity controls for public MCP servers — detecting and inspecting message types such as CallToolRequest/Result, CreateMessageRequest/Result, Elicit Result, GetPromptRequest/Result, Initialize Request/Result, ListPromptsResult, ListResourceResult, ListToolsResult, ReadResourceRequest/Result, etc. — for real-time policy enforcement, DLP, and threat scanning, in accordance with the Bank's performance and scalability requirements	It is requested that large number of MCP protocol message types be removed to keep the requirement technology-neutral, outcome-oriented and future-ready. The Bank's security objective is to obtain visibility and granular control over bidirectional MCP interactions, including prompts, responses, tool calls, resources and associated data exchanges, with real-time DLP, threat inspection and policy enforcement. Suggested Changes The proposed solution should inspect Model Context Protocol (MCP) servers for bi-directional data sharing between apps, agents, and LLMs (including via CLI), and provide visibility/granular activity controls for public MCP servers — detecting and inspecting message for real-time policy enforcement, DLP, and threat scanning, in accordance with the Bank's performance and scalability requirements	Please be guided by the RFP
106		AI Security	Appendix 1A Functional Specification	The solution must provide a real-time inspection engine capable of detecting and mitigating Generative AI-specific threats, including prompt injection, jailbreaking, and leakage of copyrighted or patented material/	Suggested Change : In Committed Roadmap	Please be guided by the RFP
107		AI Security-Posture	Appendix 1A Functional Specification	Posture Check including Certificate check, Domain check, AV agent check, customer's Custom apps check, process and registry check on endpoints.	This is a part of ZTNA solution and Hence request you to remove it from AI security to prevent any duplicacy or ambiguity Change Suggested Remove this Clause from AI Security since its already covered under ZTNA	Please refer Addendum 1 for the revised clause.
108		AI Security-Posture	Appendix 1A Functional Specification	The Posture assessment must be periodic in nature and repeat in every 15 minutes or less to ensure continued compliance"	This is a part of ZTNA solution and Hence request you to remove it from AI security to prevent any duplicacy or ambiguity Change Suggested Remove this Clause from AI Security since its already covered under ZTNA	Please refer Addendum 1 for the revised clause.
109		AI Security-Posture	Appendix 1A Functional Specification	This must include the capability to Inspect the Web Traffic sent by CLI Commands (For ex. S3) and Thick Clients like MS Teams to enable secured transactions without any user experience issues from Day 1.	This is a part of ZTNA solution and Hence request you to remove it from AI security to prevent any duplicacy or ambiguity Change Suggested Remove this Clause from AI Security since its already covered under ZTNA	Please refer Addendum 1 for the revised clause.
110		AI Guardrail	Appendix 1A Functional Specification	The proposed solution should provide detailed visibility, granular activity control, and protection for both Gen-AI prompts and responses — blocking content that bypasses LLM safety protocols, constitutes prompt injection/jailbreaking attempts, or is harmful/ hateful/ biased/ inappropriate/ risky — with policies mapped to MITRE ATLAS and OWASP Top 10 for LLMs.	We provide the Risk mapping to MITRE ATLAS and OWASP Top 10 for LLMs is supported on Workforce AI and AI Red teaming by which you can create policies. Suggested Changes The proposed solution should provide detailed visibility, granular activity control, and protection for both Gen-AI prompts and responses — blocking content that bypasses LLM safety protocols, constitutes prompt injection/jailbreaking attempts, or is harmful/ hateful/ biased/ inappropriate/ risky — with Risk mapped to MITRE ATLAS and OWASP Top 10 for LLMs.	Please refer Addendum 1 for the revised clause.
111		AI Guardrail	Appendix 1A Functional Specification	The solution must provide the capability to block or allow the download of MCP server code from public repositories (e.g., GitHub) based on repository age, stars, or security reputation.	Suggested Changes This is currently not supported under Guardrails hence request you to remove the clause	Please be guided by the RFP
112		General	Appendix 1A Functional Specification	Discovery of Embedded AI browser extensions, plug-ins and connectors using AI with Agent and Agentless	Suggested Changes Discovery of Embedded AI browser extensions, plug-ins and connectors using AI with Agent OR Agentless	Please refer Addendum 1 for the revised clause.

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
113		General	Appendix 1A Functional Specification	Enterprise-wide protection across Email, SaaS, Files, Endpoints and AI prompts.	Email protection is not part of AI security framework and we support SAAS for the a list of supported platfom (Eg Copilot, Salesforce agent etc) Suggested Changes Enterprise-wide protection across supported SaaS, Files, Endpoints and AI prompts.	Please refer Addendum 1 for the revised clause.
114		General	Appendix 1A Functional Specification	Configurable enforcement actions including Content Moderation, Coach in addition to Block/Monitor.	Coaching feature is not part of core AI security feature set Suggested Change Configurable enforcement actions including Content Moderation, in addition to Block/Monitor.	Please refer Addendum 1 for the revised clause.
115		General	Appendix 1A Functional Specification	Agent based controls with activity controls (Visit, Copy, Paste, Share, Upload, Post).	We support activity control for access, Prompts,paste and file upload Suggested Change Agent based controls with activity controls (Visit,Paste, Share, Upload, Post).	Please be guided by the RFP
116		General	Appendix 1A Functional Specification	Detection and control of non-browser AI interactions (Cursor, Claude Desktop, CLI, local AI tools, etc.) with Data and Threat , Guardrails	Guardrails are in roadmap for public AI applications on desktop. Fo rother applications which support API integration, guardarials support this natively. Suggested Change Detection and control of non-browser AI interactions (Cursor, Claude Desktop, CLI, local AI tools, etc.) with Data and Threat	Please be guided by the RFP
117		General	Appendix 1A Functional Specification	Context-aware user coaching with safer alternatives.	Coaching feature is not part of AI security and refer to the particular vendor Suggested Change Remove the clause	Please refer Addendum 1 for the revised clause.
118		General	Appendix 1A Functional Specification	Single control plane for multiple LLM providers (like Azure OpenAI, Bedrock, Vertex AI, Anthropic, etc.).	This is a part of AI gateways which does not provide security feature but is a Infrastructure component which is not required as per the Bank usecases. Suggested Changes Remove the Clause	Please refer Addendum 1 for the revised clause.
119		General	Appendix 1A Functional Specification	API or Inline compatibility with OpenAI, Anthropic, Bedrock and Vertex AI schemas without application code changes.	Native Support for Open AI chat completion is available, Anthropic format is in road and Bedrock & Vertex Ai schemas can be supported with minimal code changes at API integration Suggested Changes API or Inline compatibility with OpenAI, Anthropic, Bedrock and Vertex AI schemas with minor code changes.	Please refer Addendum 1 for the revised clause.
120		General	Appendix 1A Functional Specification	Secure API key abstraction through AI Gateway (application never stores provider keys).	This is a part of AI gateways which does not provide security feature but is a Infrastructure component which is not required as per the Bank usecases. Suggested Changes Remove the Clause	Please be guided by the RFP
121		General	Appendix 1A Functional Specification	Policy-based model routing/weighted load balancing/automatic failover and token/ request rate limiting.	This is a part of AI gateways which does not provide security feature but is a Infrastructure component which is not required as per the Bank usecases. Suggested Changes Remove the Clause	Please refer Addendum 1 for the revised clause.
122		General	Appendix 1A Functional Specification	AI Gateway dashboards for request, response and token consumption.	This is a part of AI gateways which does not provide security feature but is a Infrastructure component which is not required as per the Bank usecases. Suggested Changes Remove the Clause	Please be guided by the RFP
123		General	Appendix 1A Functional Specification	Centralized System Prompt Repository injected by the Gateway.	This is a part of AI gateways which does not provide security feature but is a Infrastructure component which is not required as per the Bank usecases. Suggested Changes Remove the Clause	Please be guided by the RFP
124		General	Appendix 1A Functional Specification	Detailed operational dashboards and exportable reports (tokens, prompts, models, providers, users, streaming, tool usage).	Streaming is generally not part of AI security and is refeering to particular vendor hence requesting you to modify the clause Suggested Change Detailed operational dashboards and exportable reports (tokens, prompts, models, providers, users tool usage).	Please refer Addendum 1 for the revised clause.
125		General	Appendix 1A Functional Specification	Control on MCP server capabilities (Tools, Resources, Prompts, Schemas).	We provide control on tools & Prompts which are necessary feature set from day 1 Suggetsed Changes Control on MCP server capabilities (Tools, Prompts).	Please refer Addendum 1 for the revised clause.

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
126		General	Appendix 1A Functional Specification	Gateway-terminated authentication for MCP with OAuth/Dynamic Client Registration/API Keys.	This is a part of AI gateways which does not provide security feature but is a Infrastructure component which is not required as per the Bank usecases. Suggested Changes Remove the Clause	Please be guided by the RFP
127		General	Appendix 1A Functional Specification	Enforcement across MCP protocol primitives (initialize, tools/list, tools/call, resources/read, prompts/get, etc.).	Allowing and blocking tools per mcp with RBAC is supported. Please change the clause neutrally for all vendors	Please be guided by the RFP
128		General	Appendix 1A Functional Specification	Gateway latency and scalability requirements.	This is a part of AI gateways which does not provide security feature but is a Infrastructure component which is not required as per the Bank usecases. Suggested Changes Remove the Clause	Please be guided by the RFP
129		AI Gateway	Appendix 1A Functional Specification	All Points related to AI Gateway	AI Gateway is not security productand is not required to ful fill the Bank's usecases revolving around employee usage & applications.	Please be guided by the RFP
130	105	10.2	Eligibility Evaluation Criteria	The proposed OEM solution/product should have been successfully implemented in at least 2 verifiable clients in India.	Since AI security is a new Technology and is in evaluation stage by cutomers in India Hence requesting the change to provide gloval reference Suggested Change The proposed OEM solution/product should have been successfully implemented in at least 2 verifiable clients in India or globally.	Please be guided by the RFP
131	149	Appendix 1A	DNS Security	A.11 : Solution must provide static name server IP for each domain used by the Bank.	Please change to : Auth DNS Solution must provide static name server IP for punjabandsind.bank.in domain for IDRBT compliance & registration. Dedicated Static IPs cannot be provided for each single domains, nor are needed by any bank or organization. This is only needed for new bank.in domains (as per IDRBT mandate). For other domains, PSB shall get Six Name Servers Anycast IPs with 100% uptime SLA. Same Setup is already deployed successfully across Many top indian banks.	Please refer Addendum 1 for the revised clause.
132	149	Appendix 1A	DNS Security	C. Cloud Based Load Balancing Solution - GSLB	Please confirm on how Domains may require this GSLB functionality (for Load balancing between DC DR Purposes). For now, we are considering 20 Domain Properties - Same as Auth DNS Zones. Please confirm the final no. as per bank's requirement so it can be included while submitting the RFP response.	Please be guided by the RFP, Refer Annexure 21, clause 15.21.4
133	17	Appendix 1A Functional Specification.xlsx	Clause F-98	The Solution should have integrated GSLB functionality to provide DC-DR Failover.	Requesting Bank to share : Number of FQDN to be considered for sizing	Please be guided by the RFP, Refer Annexure 21, clause 15.21.4
134	Instruction to Bidders - 1787133915.pdf- Page No 7	SSL Orchestrator with Packet Broker (NETWORK VISIBILITY DEVICES or Network Packet Broker Solution)	Packet Broker/A/11	Packet Grooming: Adds a set of traffic-optimization capabilities beyond basic filtering and load balancing before packets reach security tools — including de-duplication of repeated packets, packet slicing (trimming packets to only the relevant portion, e.g., headers), stripping of encapsulation headers/tags (VLAN, MPLS, VXLAN, GRE, ERSPAN), payload masking of sensitive data, and generation of flow metadata. This reduces the bandwidth and processing load placed on downstream security tools while improving the relevance of what they actually inspect.	Request to Delete as We observes that the requirement combines several advanced Packet Broker functions, including de-duplication, packet slicing, encapsulation stripping, payload masking, and flow-metadata generation. Mandating the complete set of these functions may unnecessarily narrow the solution landscape and could favor specific OEM implementations rather than the underlying operational requirement. We request the Authority to define the mandatory business outcome rather than prescribing a particular feature set. Accordingly, the bidder requests that the requirement permit equivalent mechanisms capable of delivering the required traffic optimization and security-tool efficiency, irrespective of the OEM's implementation methodology. This will ensure broader participation while maintaining the required technical outcome.	Please be guided by the RFP
135	Instruction to Bidders - 1787133915.pdf- Page No 7	SSL Orchestrator with Packet Broker (NETWORK VISIBILITY DEVICES or Network Packet Broker Solution)	Packet Broker/A/12	Secure Configuration Backup: Removes FTP as an allowed method for scheduled configuration backups, since it transmits data (including credentials) in plaintext, and mandates the use of secure alternatives only — SFTP, SCP, or FTPS. This closes off a common insecure-by-default configuration pathway and ensures backup data is protected in transit.	We seeks clarification on this clause due to an apparent contradiction within the RFP. While this clause excludes FTP and requires SFTP/SCP/FTPS, FTP appears to be specified under Point No. 27. Such conflicting provisions create uncertainty regarding the mandatory compliance criteria and may result in different interpretations during technical evaluation. We request the Authority to harmonize the relevant clauses and clearly identify the protocols that shall constitute mandatory compliance. The final requirement should be technology-neutral and should permit any industry-standard secure backup mechanism providing equivalent or higher security, thereby avoiding an unintended preference for a particular OEM implementation.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
136	Instruction to Bidders - 1787133915.pdf- Page No 9	SSL Orchestrator with Packet Broker (NETWORK VISIBILITY DEVICES or Network Packet Broker Solution)	Packet Broker/E/57	The Solution must support the Government Security Compliances not limited to FIPS 140-2 (Level 1) or The Solution must support the use of standards-aligned cryptographic module	We requests that this requirement be aligned with the regulatory and technical characteristics of the proposed Packet Broker solution. MTCTE certification, wherever applicable to the proposed equipment/category, should be considered as the relevant Government of India mandatory certification requirement. In contrast, mandating FIPS 140-2 Level 1 or equivalent cryptographic-module certification for a Packet Broker may not be technically relevant where the appliance does not generate, store, or manage cryptographic keys as part of its packet-brokering function. Such a requirement could unnecessarily exclude otherwise technically compliant solutions solely because they do not employ a cryptographic module in their Packet Broker architecture. We therefore request that the Authority remove the FIPS/cryptographic-module-specific requirement and instead specify applicable Indian regulatory certifications, including MTCTE wherever mandated, along with functional security requirements. This would ensure technology neutrality, regulatory relevance, and participation by all technically qualified OEMs.	Please be guided by the RFP
137	63	Instruction to Bidders - 1787133915.pdf	11	The platform shall scan the source code and generate CBOM info	The current requirement limits CBOM generation to source-code scanning. In practical enterprise environments, many software assets including legacy systems, COTS applications, vendor-supplied software, firmware and containerized workloads do not provide source-code access. To ensure comprehensive coverage and alignment with CERT-In CBOM guidance, Request modification: The platform should support generation of CBOM information through analysis of source code/ binaries/ firmware/ software packages/ VM/container images and imported CBOMs. Source-code cryptographic analysis, where required, may be performed using supported third-party tools and imported in CycloneDX CBOM format.	Please refer Addendum 1 for the revised clause.
138	64	Instruction to Bidders - 1787133915.pdf	44	The solution must be able to scan and generate Cryptographic Bill of Materials (CBOM) & Software Bill of Materials (SBOM) for software deployments, based on a list of target machines provided by the organization. This includes: · Remote Discovery & Access · Comprehensive Inventory Collection	As per CERT-In SBOM guidance, SBOM/CBOM generation should be based on source code, binaries, firmware, software packages, VM images and container images. Enterprise-wide discovery through SSH, WinRM or agent-based inventory collection falls under Asset Management/Endpoint Management platforms and is outside the scope of SBOM generation. Request modification. The solution shall generate SBOM and CBOM information through artifact-based analysis of supplied source code, binaries, firmware, software packages, VM images and container images.	The Bank requires both BOM generation and appropriate discovery/inventory capabilities. The solution shall support agentless discovery/scanning, API-based integrations and scheduled/on-demand/continuous discovery, as applicable. BOMs shall be generated from source code, binaries, firmware, packages, VM images and container images.
139	64	Instruction to Bidders - 1787133915.pdf	47	There must be a single view of vulnerabilities from scanners, VAPT, bug bounty, etc. mapped to SBOM	Enterprise-wide cryptographic asset discovery across infrastructure is outside the scope of standard CBOM management. Request modification. The solution shall provide a consolidated view of vulnerabilities correlated to SBOM components using supported vulnerability databases, advisories, VEX statements and imported findings, aligned with CERT-In vulnerability tracking recommendations.	Please refer Addendum 1 for the revised clause.
140	64	Instruction to Bidders - 1787133915.pdf	53	The proposed solution shall automatically discover all cryptographic assets deployed across enterprise applications and infrastructure.	Enterprise-wide cryptographic asset discovery across infrastructure is outside the scope of standard CBOM management. Request modification. The proposed solution shall generate and manage cryptographic asset information from analyzed software/firmware artifacts and imported CBOM data	Please be guided by the RFP. Both QBOM and CBOM shall meet this requirement. The solution shall support generation, discovery, ingestion, consolidation and correlation of cryptographic asset information through artifact analysis, agentless discovery, APIs/integrations and imported CBOM data. Please refer addendum 1 for the revised clause
141	64	Instruction to Bidders - 1787133915.pdf	55	The solution shall identify cryptographic usage across applications, APIs, operating systems, databases and middleware.	Request modification. The solution shall identify and manage cryptographic artifacts and findings available through analyzed software artifacts and imported CBOM data, aligned with CERT-In CBOM objectives.	Please be guided by the RFP. The solution shall identify and manage cryptographic usage through source/artifact analysis, CBOM ingestion and supported integrations/discovery mechanisms. It shall provide relationship/dependency information wherever technically available.
142	64	Instruction to Bidders - 1787133915.pdf	56	The solution shall discover TLS, SSL, SSH, IPSec and VPN cryptographic implementations.	Request modification. The solution shall identify or flag weak/deprecated cryptographic algorithms and protocols when such information is available within analyzed artifacts or imported CBOM data.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
143	64	Instruction to Bidders - 1787133915.pdf	62	The proposed solution shall automatically discover all AI, Machine Learning and Generative AI assets deployed across the enterprise.	As per CERT-In AIBOM guidance, Enterprise-wide AI asset discovery is outside standard AIBOM scope. Request modification. The solution should support centralized AI-BOM inventory through ingestion of AI model and dataset metadata, including supported model repositories.	Please be guided by the RFP. The solution shall support centralized AI-BOM inventory through discovery, supported repositories/registries, integrations, artifact analysis and imported AI-BOM metadata.
144	65	Instruction to Bidders - 1787133915.pdf	66	The solution shall discover AI model dependencies, embeddings, vector databases, plugins and external AI services.	Request modification. The solution shall ingest and manage AI model, framework and dependency metadata available through supported AI-BOM inputs, model repositories and dataset sources, aligned with CERT-In AIBOM recommendations.	Please refer Addendum 1 for the revised clause.
145	65	Instruction to Bidders - 1787133915.pdf	78	The proposed solution shall automatically discover cryptographic assets across applications, operating systems, databases, middleware and network infrastructure.	Discovery across operating systems, middleware and network infrastructure is beyond the scope of SBOM/CBOM platforms. Request modification. The proposed solution shall generate and manage cryptographic asset information derived from analyzed software/firmware artifacts and imported CBOM data.	Please refer Addendum 1 for the revised clause.
146	65	Instruction to Bidders - 1787133915.pdf	82	The proposed solution shall discover TLS, SSL, SSH, IPSec and VPN cryptographic implementations.	Request modification. The proposed solution shall identify or flag weak/deprecated cryptographic protocol usage where detected within analyzed artifacts or imported CBOM data.	Please be guided by the RFP
147	65	Instruction to Bidders - 1787133915.pdf	87	The proposed solution shall generate cryptographic risk scores based on algorithm strength, usage and exposure.	Kindly clarify risk-scoring methodology. CERT-In guidance focuses on visibility and vulnerability management and does not prescribe a specific cryptographic risk-scoring model. Request modification. The solution should support prioritization using available risk indicators such as CVSS, EPSS and exploitability information.	The solution shall provide cryptographic risk/ prioritization based on factors including algorithm strength, vulnerability status, exposure, asset criticality, exploitability and quantum vulnerability, with configurable scoring/weighting.
148	65	Instruction to Bidders - 1787133915.pdf	89	The proposed solution shall automatically discover all Artificial Intelligence (AI), Machine Learning (ML), Generative AI and Agentic AI assets deployed across the enterprise.	Enterprise-wide AI asset discovery is outside standard AIBOM scope. Request modification. The proposed solution shall support centralized inventory and management of AI, ML, Generative AI and Agentic AI assets through AI-BOM ingestion and metadata management.	Please be guided by the RFP. The solution shall support centralized AI-BOM inventory through discovery, supported repositories/registries, integrations, artifact analysis and imported AI-BOM metadata.
149	65	Instruction to Bidders - 1787133915.pdf	93	The proposed solution shall identify AI frameworks, SDKs and model dependencies used by enterprise applications.	Request modification. The proposed solution shall ingest and display AI framework, SDK and model dependency metadata where such information is available through supported AI-BOM inputs and associated sources.	Please be guided by the RFP. The solution shall identify, ingest and display AI framework, SDK, model and dependency information through supported artifact analysis, AI-BOM inputs and associated repositories/integrations.
150	65	Instruction to Bidders - 1787133915.pdf	94	The proposed solution shall discover vector databases, embeddings, plugins and AI APIs associated with deployed AI applications.	Request modification. The proposed solution shall ingest and manage metadata describing vector databases, embeddings, plugins and AI APIs where available through AI-BOM inputs, model manifests or related metadata sources.	Please be guided by the RFP. The solution shall discover or ingest and manage metadata for vector databases, embeddings, plugins and AI APIs/services through supported application/artifact analysis, manifests, AI-BOMs and integrations.
151	65	Instruction to Bidders - 1787133915.pdf	100	The proposed solution shall generate AI asset risk scores based on model exposure, dependency and business impact.	Kindly clarify AI risk-scoring methodology. CERT-In AIBOM guidance focuses on AI inventory, metadata management and dependency transparency and does not prescribe a standard business-impact-based risk-scoring framework.	Please be guided by the RFP. The solution shall support AI risk prioritization using configurable factors including model criticality, exposure, dependency vulnerabilities, data sensitivity, business criticality and other Bank-defined factors.
152	66	Instruction to Bidders - 1787133915.pdf	124	The solution shall automatically discover cryptographic and quantum-related assets across on-premises, cloud, virtualized, containerized, and hybrid environments.	Request removal. As per CERT-In QBOM guidance, discovery of cryptographic and quantum-related assets across enterprise environments pertains to PQC readiness and cryptographic posture assessment and is outside the scope of the proposed SBOM/CBOM solution.	Please be guided by the RFP
153	66	Instruction to Bidders - 1787133915.pdf	125	Applications, Servers, Databases, APIs, PKI, Certificates, HSMs, KMS, Containers, Kubernetes, Network Devices, VPNs, IoT, Cloud Services.	Request removal. Discovery of applications, servers, databases, PKI, certificates, HSMs, KMSs, network devices, VPNs, IoT and cloud services is associated with Cryptographic Posture Management and QBOM readiness solutions rather than SBOM management.	Please be guided by the RFP
154	66	Instruction to Bidders - 1787133915.pdf	126	Automatically identify RSA, ECC, DSA, Diffie-Hellman, ML-KEM,ML-DSA AES, SHA, TLS, SSH, IPSec, PQC algorithms, and hybrid implementations.	Request removal. Enterprise-wide identification of RSA, ECC, DSA, Diffie-Hellman, AES, SHA, TLS, SSH, IPSec, PQC and hybrid cryptographic implementations falls under QBOM and cryptographic posture assessment functions rather than SBOM generation.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
155	66	Instruction to Bidders - 1787133915.pdf	127	Agent-based, Agentless, API-based, Scheduled, Continuous Discovery.	CERT-In BOM guidance focuses on BOM generation, sharing, management and transparency. Continuous discovery mechanisms such as agent-based, agentless and scheduled infrastructure discovery are outside standard SBOM/CBOM requirements. Request modification. The solution shall support artifact-based analysis and API-based BOM ingestion and management.	Please be guided by the RFP
156	66	Instruction to Bidders - 1787133915.pdf	128	Maintain centralized QBOM repository with configurable metadata.	Request removal. Maintenance of a centralized QBOM repository is associated with quantum-risk management and PQC readiness activities and is outside the scope of the proposed SBOM solution.	Please be guided by the RFP
157	66	Instruction to Bidders - 1787133915.pdf	129	Discover relationships between applications, cryptographic libraries, certificates, protocols, APIs, and infrastructure components.	Discovery of relationships involving certificates, infrastructure assets and runtime environments aligns more closely with Cryptographic Posture Management platforms. Request Modification. The solution supports dependency analysis and relationship mapping among software components and cryptographic libraries identified through artifact analysis.	Please be guided by the RFP
158	66	Instruction to Bidders - 1787133915.pdf	131	Automatically identify quantum-vulnerable cryptographic implementations.	Request removal. Identification of quantum-vulnerable cryptographic implementations falls under QBOM and post-quantum readiness assessment and is outside the scope of the proposed solution.	Please be guided by the RFP
159	66	Instruction to Bidders - 1787133915.pdf	132	Identify assets containing long-term confidential data susceptible to future quantum attacks.	Request removal. Assessment of readiness for migration to post-quantum cryptography is a QBOM/PQC readiness requirement and not a standard SBOM capability.	Please be guided by the RFP
160	66	Instruction to Bidders - 1787133915.pdf	133	Assess readiness for migration to post-quantum cryptography.	Request removal. Assessment of readiness for migration to post-quantum cryptography is a QBOM/PQC readiness requirement and not a standard SBOM capability.	Please be guided by the RFP
161	66	Instruction to Bidders - 1787133915.pdf	134	Evaluate algorithm abstraction, hybrid support, dynamic algorithm replacement, and migration capability.	Request removal. Evaluation of algorithm abstraction, hybrid support, dynamic algorithm replacement and migration capability pertains to PQC transformation and migration planning rather than SBOM management.	Please be guided by the RFP
162	66	Instruction to Bidders - 1787133915.pdf	135	Detect hybrid deployments combining classical and PQC algorithms.	Request removal. Detection of hybrid deployments combining classical and post-quantum cryptography falls within QBOM and PQC readiness assessment scope.	Please be guided by the RFP
163	66	Instruction to Bidders - 1787133915.pdf	136	Generate migration plans based on business criticality and quantum risk.	Request removal. Generation of migration plans based on business criticality and quantum risk is a governance and consulting activity associated with PQC readiness programs and not a capability of SBOM/CBOM management platforms.	Please be guided by the RFP
164	57	Instruction to Bidders - 1787133915.pdf	:DAM:1	Creation of an inventory through auto discovery of all databases and database users, deployed across the bank.	Request to remove this clause	Please be guided by the RFP
165	57	Instruction to Bidders - 1787133915.pdf	:DAM:2	The proposed DAM solution should be able to monitor databases in scope without dropping any log.	Request to make this clause more flexible to optimise storage and reduce signal to noise ratio- The solution must support granular auditing/logging capability to monitor different types of operations on sensitive and non sensitive data as well as include or exclude users from these policies	Please be guided by the RFP
166	57	Instruction to Bidders - 1787133915.pdf	:DAM:4	The solution should have the capability to detect vulnerabilities including behavioral vulnerabilities such as excessive administrative logins, account sharing and unusual after-hours' activity by scanning databases, data warehouses and big data environments. The solution should identify issues such as missing patches, weak passwords, unauthorized changes and misconfigured privileges. Further, comprehensive reports should be provided along with suggestions to address all vulnerabilities.	Request to change to the following: - The solution should have the capability to detect vulnerabilities including behavioral vulnerabilities such as excessive administrative logins, account sharing and unusual after-hours' activity by scanning databases, data warehouses and big data environments.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
167	57	Instruction to Bidders - 1787133915.pdf	:DAM:5	The solution should provide capability to detect DB attacks and prevent attacks such as SQL injection, leakage of sensitive data etc. and should be able to detect and alert unauthorized or unusual queries, access to sensitive and confidential data etc. for various database including big database.	Request to change to the following: - The solution should provide capability to detect DB attacks such as leakage of sensitive data etc. and should be able to detect and alert unauthorized or unusual queries, access to sensitive and confidential data etc. for various database including big database.	Please be guided by the RFP
168	57	Instruction to Bidders - 1787133915.pdf	:DAM:6	The solution should support installation manager on each database server to avoid manual efforts to coordinate agent activities along with up-gradation and configuration changes.	Request to allow agentless next generation DAM: - The solution should be either be agentless or support installation manager on each database server to avoid manual efforts to coordinate agent activities along with up-gradation and configuration changes.	Please be guided by the RFP
169	57	Instruction to Bidders - 1787133915.pdf	:DAM:7	The solution should be able to monitor, detect and prevent breaches/anomalies for following databases: a) MySQL b) MS SQL c) PostgreSQL d) Oracle DB e) Maria DB f) any other DBs	Request to change to the following: - The solution should be able to monitor and detect breaches/anomalies for following databases: a) MySQL b) MS SQL c) PostgreSQL d) Oracle DB	Please be guided by the RFP
170	57	Instruction to Bidders - 1787133915.pdf	:DAM:9	The solution should audit all types of database access across the organization regardless of database type or operating system of the host without relying on native auditing.	Please provide the location-wise count of different types of databases to be supported.	Relevant details shall be shared with the succesfull bidder
171	57	Instruction to Bidders - 1787133915.pdf	:DAM:12	The solution should be able to inspect SQL statements going to the database and determine with high accuracy whether to allow, log, audit, substitute or block the SQL.	Request to remove this clause	Please be guided by the RFP
172	57	Instruction to Bidders - 1787133915.pdf	:DAM:13	The solution shall integrate with database encryption technologies where applicable and continue to monitor database activities on encrypted databases	Request to remove this clause	Please be guided by the RFP
173	57	Instruction to Bidders - 1787133915.pdf	:DAM:16	The solution shall be able to integrate with leading Next-Gen SOC solutions such as SIEM, S-BDL, SOAR etc. to generate meaningful correlated events. Also, it should be capable of sending all format logs to SIEM/S-BDL	Requestt to change this cluase to the following: - The solution shall be able to integrate with leading Next-Gen SOC solutions such as SIEM, S-BDL, SOAR etc. to generate meaningful correlated events.	Please be guided by the RFP
174	57	Instruction to Bidders - 1787133915.pdf	:DAM:18	The solution should be capable of generating reports on policy console including usage of agents, pushing, upgrades, push updates, configurations updates, policy updates, startup/restart etc.	Requestt to change this cluase to the following: - The solution should be capable of generating reports on policy console including usage of agents, pushing, upgrades, push updates, configurations updates, policy updates, startup/restart etc or support viewing the status and updaing the agentless proxies from the central console.	Please be guided by the RFP
175	57	Instruction to Bidders - 1787133915.pdf	:DAM:19	The solution should have the capability to build an inventory by discovery of all databases and database users. The discovery capability by itself should be near real-time and on-demand discovery.	Request to change ro the following to make it security relevant: - The solution should have the capability to build an inventory of all sensitive database tables and columns.	Please be guided by the RFP
176	57	Instruction to Bidders - 1787133915.pdf	:DAM:20	The solution should have the ability to generate reports consisting of the details of all database-level IP addresses, database type, Agent versions, status, etc. (active/inactive) and timestamp.	Request to change to the following: - The solution should have the ability to generate reports consisting of the details of all database-level IP addresses/hostnames, database type, Agent versions/agentless proxy, status, etc. (active/inactive) and timestamp.	Please be guided by the RFP
177	58	Instruction to Bidders - 1787133915.pdf	:DAM:23	The solution should have various notification mechanisms like Mails, SNMP traps etc. for security monitoring and health monitoring and the notification mechanism must be real time. Specify the notification mechanisms the solution supports.	Request to change to the following: - The solution should have various notification mechanisms like Mails, Slack etc. for security monitoring and health monitoring and the notification mechanism must be real time. Specify the notification mechanisms the solution supports.	Please be guided by the RFP
178	58	Instruction to Bidders - 1787133915.pdf	:DAM:24	The solution should be capable of identifying the missing patches and report the same and should have capabilities of virtual patching or protecting through security policies of known vulnerabilities till the patch is installed.	Request to remove this clause	Please be guided by the RFP
179	58	Instruction to Bidders - 1787133915.pdf	:DAM:26	The solution should have the ability to generate report showing the access of each user to the tables of each database along with the user who granted them the permission.	Request to remove this clause	Please be guided by the RFP
180	58	Instruction to Bidders - 1787133915.pdf	:DAM:29	The proposed solution required monitoring should be delivered while solution is enabled and in blocking mode.	Request to change to the following The proposed solution required monitoring should be delivered while solution is enabled.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
181	58	Instruction to Bidders - 1787133915.pdf	:DAM:30	The solution should support creation of policies/rules for enforcing access control and proper rights management on databases.	Request to remove this clause	Please be guided by the RFP
182	58	Instruction to Bidders - 1787133915.pdf	:DAM:33	Solution must monitor privileged user access or local SQL activity that does not cross the network such as Bequeath, IPC, Shared Memory, or Named Pipes.	Request to remove this clause	Please be guided by the RFP
183	58	Instruction to Bidders - 1787133915.pdf	:DAM:35	Solution must support filtering/hiding of the bind variables of all the SQL activities captured.	Request to remove this clause	Please be guided by the RFP
184	58	Instruction to Bidders - 1787133915.pdf	:DAM:43	The solution should be able to auto discover privilege users in the database and should support user entitlement reviews on database accounts.	Request to remove this clause	Please be guided by the RFP
185	58	Instruction to Bidders - 1787133915.pdf	:DAM:44	The solution should identify insecure default accounts and weak/default credentials through database security assessment capabilities.	Request to remove this clause	Please be guided by the RFP
186	58	Instruction to Bidders - 1787133915.pdf	:DAM:45	Solution tracks the dormant accounts as per defined rule.	Request to remove this clause	Please be guided by the RFP
187	59	Instruction to Bidders - 1787133915.pdf	DAM 47	Solution should detect attacks on network protocols, as well as application layer DB activity.	Request to remove this clause	Please be guided by the RFP
188	59	Instruction to Bidders - 1787133915.pdf	:DAM:49	Solution should detect attacks attempting to exploit known vulnerabilities as well as common threat vectors and can be configured to issue an alert and/or "terminate the session in real time or policy-based blocking"	Request to remove this clause	Please be guided by the RFP
189	59	Instruction to Bidders - 1787133915.pdf	:DAM:50	The solution should discover misconfigurations in the database and its platform and suggest remedial measures.	Request to remove this clause	Please be guided by the RFP
190	59	Instruction to Bidders - 1787133915.pdf	:DAM:51	The solution should be capable of reporting missing patches and report the details of such patches and vulnerabilities associated with.	Request to remove this clause	Please be guided by the RFP
191	59	Instruction to Bidders - 1787133915.pdf	:DAM:52	Solution should have capability to track execution of stored procedures, including who executed a procedure, what procedure name and when, which tables were accessed.	Request to modify this cluase to the following: - Solution should have capability to track execution of stored procedures, including who executed a procedure, what procedure name and when.	Please be guided by the RFP
192	59	Instruction to Bidders - 1787133915.pdf	:DAM:53	Solution should also be able to detect any change happens in stored procedure.	Request to remove this clause	Please be guided by the RFP
193	59	Instruction to Bidders - 1787133915.pdf	:DAM:57	Ability to kill sessions for accessing sensitive data/policy violations and keeping all activity in the logs.	Request to remove this clause	Please be guided by the RFP
194	59	Instruction to Bidders - 1787133915.pdf	:DAM:58	The solution should be capable of blocking access real time, execution of commands which violate the rules/policies, store the events securely and report the same in real time.	Request to modify this cluase to the following: - The solution should be capable of alerting in real time, execution of commands which violate the rules/policies, store the events securely and report the same in real time.	Please be guided by the RFP
195	59	Instruction to Bidders - 1787133915.pdf	:DAM:59	The Proposed solution should support monitoring mode and blocking mode of deployment. In monitoring mode, solution can generate alerts for unauthorized activity. In blocking mode, solution must proactively block malicious queries including blocking of matching signatures for known attacks like SQL injection.	Request to remove this clause	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
196	59	Instruction to Bidders - 1787133915.pdf	:DAM:60	The solution should support installation of agents, update of agents, configurations updates, policy updates, start/stop/restart etc. at all the databases from management server centrally.	Request to allow agentless next generation DAM: - The solution should be either be agentless or support installation of agents, update of agents, configurations updates, policy updates, start/stop/restart etc. at all the databases from management server centrally.	Please be guided by the RFP
197	59	Instruction to Bidders - 1787133915.pdf	:DAM:65	The solution should be able to support/monitor all database activities in OS like all flavors of Linux (Solaris, CentOS, Ubuntu, RHEL) and Windows for databases like MS SQL, MySQL, PostgreSQL, Oracle DB, Maria DB, any other DBs etc. at a minimum provided that DB vendors still support the versions in scope.	Request to change to the following: - The solution should be able to support/monitor all database activities in OS like all flavors of Linux (Solaris, CentOS, Ubuntu, RHEL) and Windows for databases like MS SQL, MySQL, PostgreSQL, and Oracle DB at a minimum provided that DB vendors still support the versions in scope.	Please be guided by the RFP
198	59	Instruction to Bidders - 1787133915.pdf	:DAM:66	The solution should provide information of DB links and should have capability to monitor the activity of DB links.	Request to remove this clause	Please be guided by the RFP
199	59	Instruction to Bidders - 1787133915.pdf	:DAM:69	The solution should discover all the databases with details i.e. IP, type, OS, available in the bank network.	Request to remove this clause	Please be guided by the RFP
200	60	Instruction to Bidders - 1787133915.pdf	:DAM:75	The proposed solution shall support monitoring of all databases covered under the procured licenses and shall support future expansion. Solution should support the deployment modes i.e. monitoring / blocking separately for each database.	Request to modify to the following: - The proposed solution shall support monitoring of all databases covered under the procured licenses and shallmsupport future expansion.	Please be guided by the RFP
201	60	Instruction to Bidders - 1787133915.pdf	:DAM:76	The solution shall provide mechanisms to optimize resource utilization and configurable resource consumption	Request to modify to the following: - The solution shall provide mechanisms to optimize resource utilization.	Please be guided by the RFP
202	60	Instruction to Bidders - 1787133915.pdf	:DAM:77	The solution should have capability to facilitate rule creation at a very granular level. Example: Which user can connect from which source, access what objects, have which rights, at what time window etc.	Request to remove this clause	Please be guided by the RFP
203	60	Instruction to Bidders - 1787133915.pdf	:DAM:78	Rules also should allow blocking access depending upon different parameters like above.	Request to remove this clause	Please be guided by the RFP
204	60	Instruction to Bidders - 1787133915.pdf	:DAM:82	The solution shall support inbult authentication and integration with enterprise Identity and Access Management (IAM) platforms, including LDAP/Active Directory, RADIUS, SAML, TACACS+, and other industry-standard authentication mechanisms.	Request to modify to the following: - The solution shall support inbult authentication and integration with enterprise Identity and Access Managemen (IAM) platforms, like LDAP/Active Directory and SAML and native MFA for console login.	Please refer Addendum 1 for the revised clause.
205	60	Instruction to Bidders - 1787133915.pdf	:DAM:87	The solution must support generation of both predefined as well as custom-built reports as per Bank's requirements with both tabular views, PDF and data analysis graphical views.	Request the requirement of data analysis graphical views	Please be guided by the RFP
206	60	Instruction to Bidders - 1787133915.pdf	:DAM:91	The solution should be able to generate the reports in PDF, Excel & CSV formats.	Request to modify to the following: - The solution should be able to generate the reports in PDF, Excel & JSON formats.	Please be guided by the RFP
207	60	Instruction to Bidders - 1787133915.pdf	:DAM:93	The solution shall store audit logs in a secure, tamper-evident repository supporting integrity verification and efficient retrieval.	Request to modify to the following: - The solution shall store audit logs in a secure, tamper-evident repository supporting efficient retrieval.	Please be guided by the RFP
208	61	Instruction to Bidders - 1787133915.pdf	:DAM:100	The Solution must have in-built Risk Analytics module/engine.	Request to remove this vendor specific module	Please be guided by the RFP
209	61	Instruction to Bidders - 1787133915.pdf	:DAM:101	The Risk Analytics module/engine must be purposefully built and be self-contained	Request to remove this vendor specific module	Please be guided by the RFP
210	61	Instruction to Bidders - 1787133915.pdf	:DAM:102	The Risk Analytics module/engine should provide unified console which aggregates threat indicators across the enterprise databases.	Request to remove this vendor specific module	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
211	61	Instruction to Bidders - 1787133915.pdf	:DAM:103	The Risk Analytics module/engine should provide an intuitive dashboard page containing widgets that give a quick informative and drill-down capability view of the following: a) Protected Assets b) Open Issues c) Security Events Over Time d) Entities With Most Severe Incidents e) Events Analyzed f) System Health Status	Request to remove this vendor specific module	Please be guided by the RFP
212	61	Instruction to Bidders - 1787133915.pdf	:DAM:104	The Risk Analytics Solution must be able to support the identification of anomalous activity on databases including: a) MS SQL b) MySQL c) PostgreSQL d) Oracle DB e) Maria DB f) any other DB deployed in Bank	Request to remove this vendor specific module	Please be guided by the RFP
213	61	Instruction to Bidders - 1787133915.pdf	:DAM:105	The Risk Analytics Solution must provide behavior analytics algorithm to establish behavioral baseline and find deviations.	Request to remove this vendor specific module	Please be guided by the RFP
214	61	Instruction to Bidders - 1787133915.pdf	:DAM:106	The Risk Analytics Solution must be able to differentiate between suspicious behavior from risky/abusive behavior (anomaly vs incident).	Request to remove this vendor specific module	Please be guided by the RFP
215	61	Instruction to Bidders - 1787133915.pdf	:DAM:107	The Risk Analytics Solution should be able to assess user's risk potential.	Request to remove this vendor specific module	Please be guided by the RFP
216	61	Instruction to Bidders - 1787133915.pdf	:DAM:108	The solution should support real-time monitoring and policy enforcement/blocking for Cloud DB/DBaaSenvironments, including databases deployed on Kubernetes/container platforms.	Request to modify to the following: - The solution should support real-time monitoring and policy for Cloud DB/DBaaSenvironments, including databases deployed on Kubernetes/container platforms.	Please be guided by the RFP
217	61	Instruction to Bidders - 1787133915.pdf	:DAM:109	The solution should provide a Compliance Smart Assistant capable of automatically deploying industry-standard compliance policies (PCI DSS, SOX, GDPR, HIPAA, etc.) with minimal manual configuration.	Request to remove this clause	Please be guided by the RFP
218	61	Instruction to Bidders - 1787133915.pdf	:DAM:110	The solution should automatically terminate, quarantine, or block suspicious database sessions based on configurable security policies.	Request to remove this clause	Please be guided by the RFP
219	61	Instruction to Bidders - 1787133915.pdf	:DAM:111	The solution should identify database user privileges, review excessive permissions, and detect inactive/dormant privileged accounts.	Request to remove this clause	Please be guided by the RFP
220	61	Instruction to Bidders - 1787133915.pdf	:DAM:112	The solution should provide Data Risk Analytics by correlating activities, vulnerabilities, identities, and sensitive data across all monitored databases.	Request to remove this vendor specific module	Please be guided by the RFP
221	61	Instruction to Bidders - 1787133915.pdf	:DAM:114	The Risk Analytics Solution should automatically detect the following: a) Nature of accounts which connect to the database (Service Account, DBA User Account, etc.) b) Purpose of database tables (Business Critical Tables, System Tables, etc.) c) Data access habits (working hours, amount of data retrieved)	Request to remove this vendor specific module	Please be guided by the RFP
222	62	Instruction to Bidders - 1787133915.pdf	:DAM:115	The Risk Analytics Solution must be able to detect Abnormal Behavior such as: a) Database Access at Non-Standard Time b) Database Service Account Abuse c) Excessive Database Record Access d) Excessive Failed Logins e) Excessive Failed Logins from Application Server f) Excessive Multiple Database Access g) Machine Takeover h) Suspicious sensitive system tables scan i) Suspicious Application data access j) Suspicious Database command execution k) Suspicious Dynamic SQL activity	Request to remove this vendor specific module	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
223	62	Instruction to Bidders - 1787133915.pdf	:DAM:116	The Risk Analytics Solution must be able to identify/detect the following: a) Typical end point information b) Typical database access patterns	Request to remove this vendor specific module	Please be guided by the RFP
224	62	Instruction to Bidders - 1787133915.pdf	:DAM:117	The Risk Analytics Solution should be able to detect suspicious activity including scans for sensitive and valuable data, which may indicate the reconnaissance phase of a potential breach.	Request to remove this vendor specific module	Please be guided by the RFP
225	62	Instruction to Bidders - 1787133915.pdf	:DAM:119	The Risk Analytics Solution must be able to integrate with Active Directory (AD) to enhance forensics and provide line of sight into user identity.	Request to remove this vendor specific module	Please be guided by the RFP
226	62	Instruction to Bidders - 1787133915.pdf	:DAM:120	The Risk Analytics Solution should be able to perform analysis when integrated with Active Directory.	Request to remove this vendor specific module	Please be guided by the RFP
227	62	Instruction to Bidders - 1787133915.pdf	:DAM:121	The Risk Analytics module shall provide user-centric dashboards with drill-down capabilities for incidents, anomalies, user behaviour and endpoint activity.	Request to remove this vendor specific module	Please be guided by the RFP
228	62	Instruction to Bidders - 1787133915.pdf	:DAM:122	The Risk Analytics Solution must support REST API to enable extraction of Security Events.	Request to remove this vendor specific module	Please be guided by the RFP
229	62	Instruction to Bidders - 1787133915.pdf	:DAM:124	The Risk Analytics Solution should be able to whitelist behavior which is authorized or acknowledge behavior that cannot be remediated immediately.	Request to remove this vendor specific module	Please be guided by the RFP
230	62	Instruction to Bidders - 1787133915.pdf	:DAM:125	The Risk Analytics Solution must be able to send logs to SIEM or other Risk Analytics Solution for seamless incident management.	Request to remove this vendor specific module	Please be guided by the RFP
231	62	Instruction to Bidders - 1787133915.pdf	:DAM:126	The Risk Analytics Solution must give incidents details which include Username, Source, Destination, Related/Correlated Issues, Type, Time, Severity and Priority.	Request to remove this vendor specific module	Please be guided by the RFP
232	62	Instruction to Bidders - 1787133915.pdf	:DAM:127	The Risk Analytics Solution should automatically assign a Priority Score (a more granular threat score, on a defined scale) to each incident for easier classification of important events.	Request to remove this vendor specific module	Please be guided by the RFP
233	62	Instruction to Bidders - 1787133915.pdf	:DAM:128	The Risk Analytics Solution should include comprehensive incident details when investigating an incident. Details should include: a) Description b) Severity Influencing Reasons c) Client and Server Details d) Incident Details e) Typical Behavior	Request to remove this vendor specific module	Please be guided by the RFP
234	62	Instruction to Bidders - 1787133915.pdf	:DAM:129	The Risk Analytics Solution must be able to export detected incidents and anomalies to an Excel file for offline review.	Request to remove this vendor specific module	Please be guided by the RFP
235	62	Instruction to Bidders - 1787133915.pdf	:DAM:130	The Risk Analytics Solution must be able to send email notification on detecting an issue/incident.	Request to remove this vendor specific module	Please be guided by the RFP
236		Instruction to Bidders - 1787133915.pdf	:DAM:		Request to add the following clause: - For SaaS soltions, the SaaS tenant must be hosted in India	Please be guided by the RFP
237		Instruction to Bidders - 1787133915.pdf	:DAM:		Request to add the following clause: - The proposed DAM solution must provide a dedicated SaaS tenant model and not a shared SaaS tenant for increased security	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
238		Instruction to Bidders - 1787133915.pdf	:DAM:		Request to add the following clause: - The proposed DAM solution must be SOC2 Type 2 and SOC 3 certified	Please be guided by the RFP
239		Instruction to Bidders - 1787133915.pdf	:DAM:		Request to add the following clause: - The proposed DAM solution must be ISO/IEC 27001:2022, 27018:2019 and 27017:2015 compliant	Please be guided by the RFP
240		Instruction to Bidders - 1787133915.pdf	:DAM:		Request to add the following clause: - The proposed DAM solution must be PCI:DSS compliant	Please be guided by the RFP
241		Instruction to Bidders - 1787133915.pdf	:DAM:		Request to add the following clause: - The proposed DAM solution should map every query to industry standard CRUDS model for easy security investigations	Please be guided by the RFP
242		Instruction to Bidders - 1787133915.pdf	:DAM:		Request to add the following clause: - The proposed DAM solution should capture the number of records returned by the database query for threat detection and triage	Please be guided by the RFP
243		Instruction to Bidders - 1787133915.pdf	:DAM:		Request to add the following clause: - The proposed DAM solution should correlate data sensitivity to every query to help reduce signal to noise ratio	Please be guided by the RFP
244		Instruction to Bidders - 1787133915.pdf	:DAM:		Request to add the following clause: - The proposed DAM solution should provide target context within the database for every query	Please be guided by the RFP
245		Instruction to Bidders - 1787133915.pdf	:DAM:		Request to add the following clause: - The proposed DAM solution should capture query success or failure status	Please be guided by the RFP
246		Instruction to Bidders - 1787133915.pdf	:DAM:		The proposed DAM solution should also log the raw query data.	Please be guided by the RFP
247		Instruction to Bidders - 1787133915.pdf	:DAM:		Request to add the following clause: - The proposed DAM solution should provide data classification policies based on regex patterns, positive and negative keywords as well as algorithmic validators like Luhn, GST Checksum, Verhoef and BIN where possible to discover and classify sensitive columns.	Please be guided by the RFP
248		Instruction to Bidders - 1787133915.pdf	:DAM:		Request to add the following clause: - The proposed DAM solution should deploy a local scanner/crawler in customer's cloud environment and/or data centers to scan data and not move data outside of the customer environment.	Please be guided by the RFP
249		Instruction to Bidders - 1787133915.pdf	:DAM:		Request to add the following clause: - The proposed DAM solution must provide customizable pre-built data classification policies for various privacy (like DPDP and GDPR), regulatory(like PCI and SOX), statutory(like ITAR) and data security(like credentials and access tokens) requirements.	Please be guided by the RFP
250		Instruction to Bidders - 1787133915.pdf	:DAM:		Request to add the following clause: - The proposed DAM solution should have various pre-built data classification patterns for Indian Banks like PAN, Aadhaar, GST, Indian Passport Number, Indian Driving License, Indian Mobile Phone Number, Indian Address, Credit Card Number, Credit Card Pin, Credit Card CVV, SWIFT, and IBAN.	Please be guided by the RFP
251		Instruction to Bidders - 1787133915.pdf	:DAM:		Request to add the following clause: - The proposed DAM solution should also allow creation of custom data classification policies	Please be guided by the RFP
252		Instruction to Bidders - 1787133915.pdf	:DAM:		Request to add the following clause: - The proposed DAM solution should provide functionality to test data classification policies before enabling them	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
253		Instruction to Bidders - 1787133915.pdf	:DAM:		Request to add the following clause: - The proposed DAM solution should support threat models/alerting policies that take data sensitivity into consideration	Please be guided by the RFP
254			RFP Document 7.2.1.3.Data Security 7.2.1.3.Database Activity Monitoring Features & modules:2. Page 34	The Proposed DAM Solution should support automatic updates to the signature database and based on global threat intelligence, ensuring complete protection against the latest threats.	Request to remove this clause	Please be guided by the RFP
255			RFP Document 7.2.1.3.Data Security 7.2.1.3.Database Activity Monitoring Features & modules:3. Page 34	"In The proposed DAM solution, audit policy and security policy should be mutually exclusive. The solution should be capable of generating security alerts even if an audit policy is not assigned to a given DB."	Request to remove this clause	Please be guided by the RFP
256			RFP Document 7.2.1.3.Data Security 7.2.1.3.Database Activity Monitoring Features & modules:5. Page 34	Solutions must have audit log feature to detect any changes in the tool and same should be integrated with SIEM for real time alerts.	Request to remove this clause	Please be guided by the RFP
257			RFP Document 7.2.1.3.Data Security 7.2.1.3.Database Activity Monitoring Bidder/OEM Responsibility:5 Page 35	The OEM must enable real-time monitoring, blocking of unauthorized access, and sensitive data discovery/masking, with policies tailored to the Bank's specific needs.	Request to rmeove the blocking and masking requirements and change the clause to the following: - The OEM must enable real-time monitoring of unauthorized access, and sensitive data discovery, with policies tailored to the Bank's specific needs.	Please be guided by the RFP
258			RFP Document 7.2.1.3.Data Security 7.2.1.3 7.2.3.1.1 Key Deliverables:1.iv Page 35	Vulnerability assessment and patch management reports	Request to remove this clause	Please be guided by the RFP
259			RFP Document 7 Scope of Work C. Data Security (DAM)Database Activty Monitoring Page 27	Deployment Model: On-Premises	Request to allow SaaS solutions	Please be guided by the RFP
260	31	E. Management Layer and Security	AI Security	Deployment Model - On Premise at DC and DR	Most of the AI Security solution uses a hybrid architecture by design: an on-premise inline component inspects and protects all data flowing between agents and the LLM — so sensitive Bank data never leaves the premises — while cloud-based control plane handles only non-sensitive policy management, orchestration, and real-time threat-intelligence updates. This will fully meet the data sovereignty intent behind the RFP's on-prem clause while still delivering the continuously updated threat protection, which a fully air-gapped deployment would not support. We're requesting the clause be revised to reflect this hybrid model so that PSB gets the best of the breed solution without compromising the Bank's security or compliance requirements.	Please refer Addendum 1 for the revised clause.
261	70	Instruction to Bidders - 1787133915.pdf	CASB	If any component of the proposed solution is hosted on a cloud platform, indicate whether the Product OEM/Cloud Service Provider (CSP) has submitted CSP compliance functional specifications and supporting documentation demonstrating compliance with all applicable requirements of this RFP. If the dropdown is not selected, the product will be considered NON COMPLIANT.	Some of the OEMs operates as the Product OEM/CSP for its SaaS-based AI Security platform, and maintains and can furnish current ISO 27001 and SOC 2 Type II attestations, along with DPDPA-aligned data handling practices, covering the cloud control/management plane. We request that these independently audited, industry-recognized certifications be accepted as the compliance functional specification for this clause, since they demonstrate equivalent or stronger assurance than data-center-level ownership documentation, which is not applicable to a SaaS delivery model built on certified hyperscaler/co-location infrastructure.	Please be guided by the RFP
262	74	Instruction to Bidders - 1787133915.pdf	AI Security	Solution is available as a lightweight virtual appliance for public cloud deployments in AWS, or private cloud deployments with Vmware ESXi.	We request you to modify this clause as " Solution is available as a lightweight virtual appliance for public cloud deployments in AWS, or private cloud deployments with Vmware ESXi or Microsoft Hyper-V.	Please refer Addendum 1 for the revised clause.
263	73	Instruction to Bidders - 1787133915.pdf	AI Security	The Posture assessment must be periodic in nature and repeat in every 15 minutes or less to ensure continued compliance"	We request you to modify this clause as " The Posture assessment must be periodic in nature and should repeat in every 5 minutes to ensure continued compliance"	Please refer Addendum 1 for the revised clause.
264	149	14.2 APPENDIX 1B: Technical Compliance Sheet DDoS S. No. 2	System should have 5 Gbps of clean/legitimate throughput which can scale upto 10 Gbps on the same H/w. System should support more then 20 MPPS. System should be factored on clean/legitimate license throughput.	Suggetsed Clause: System should have 5 Gbps of clean/legitimate throughput which can scale upto 10 Gbps on the same H/w. Mitigation Throughput 10Gbps from day1 and scale to 20Gbps. System should support more then 12 MPPS. System should be factored on clean/legitimate license throughput.	If we consider an average packet size of 64 bytes (minimum packet size), 9 Mpps is equivalent to approximately 5 Gbps of throughput handling. Based on our experience deploying our solution at major Public Sector Banks, including leading/top-tier banks, 12–14 Mpps is more than sufficient to cater to a 10 Gbps clean traffic environment. Additionally, the mitigation throughput should also be considered to ensure effective mitigation of attacks in both ingress and egress traffic directions.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
265	149	14.2 APPENDIX 1B: Technical Compliance Sheet DDoS S. No. 73		The proposed solution shall support PQC readiness and migration capability, including identification of quantum-vulnerable cryptographic algorithms and support for PQC-enabled or quantum-resistant cryptographic standards, wherever applicable to the solution.	The technical specifications requested for TLS inspection already cover full SSL/TLS inspection as an in-built capability of the DDoS mitigation hardware. Therefore, specifying the latest cipher suites and TLS 1.3 with hardware-based acceleration should be considered as a technology-neutral requirement to enable wider OEM participation, rather than mandating any specific requirement. Suggested Clause: The proposed solution shall support TLS 1.3 with hardware acceleration for encrypted traffic protection.	PQC readiness is intended to cover applicable cryptographic functions, communication interfaces, authentication mechanisms, APIs, certificates and other security components of the proposed solution and support migration to quantum-resistant standards. DDoS vendor need to submit their roadmap or approach on PQC
266	149	14.2 APPENDIX 1B: Technical Compliance Sheet WAF S. No. 12		The proposed solution must support dedicated 5 Gbps of WAF throughput (HTTP/HTTPS). The bidder must provide evidence of throughput through publicly available documents /evidence based document supporting the same which needs to be submitted along with the proposal and same needs to showcased if asked by bank during Presentation & UAT (Undertaking from the OEM is not accepted in this case).	Not every OEM publishes WAF throughput as a standard performance parameter. However, leading vendors in the WAF and API Protection space do publish Layer-7 throughput capabilities as part of their product specifications. Therefore, vendors that can demonstrate equivalent L7/WAF and API protection performance should also be considered to ensure wider OEM participation and a technology-neutral evaluation process. Suggested Clause: The proposed solution must support dedicated 5 Gbps of WAF throughput (HTTP/HTTPS) or 25 Gbps of L7 throughput. The bidder must provide evidence of throughput through publicly available documents (Undertaking from the OEM is also accepted in this case).	Please be guided by the RFP
267	149	14.2 APPENDIX 1B: Technical Compliance Sheet WAF S. No. 81		The client component (JavaScript) should be downloaded from the same domain as the application (first party). It is not allowed to use external locations to upload the script.	Every OEM may use its own architecture and methodology to achieve the required functionality. Therefore, the evaluation should be functionality- and outcome-based rather than implementation-method-based. The specified clause should not be restrictive, provided that the proposed solution meets the intended security and functional requirements. Suggested Clause: The client component (JavaScript) should be downloaded from the same domain as the application (first party).	Please be guided by the RFP
268	149	14.2 APPENDIX 1B: Technical Compliance Sheet WAF S. No. 90		The proposed WAF solution must support high availability in both Layer 2 and Layer 3 deployments. It must include either an inbuilt bypass switch or be supplied with an external bypass switch to ensure uninterrupted traffic flow during maintenance or failure.	Fail-open/Bypass is not relevant in the context of a stateful security solution, as maintaining session and connection state is essential to its intended operation. If fail-open functionality is considered a mandatory requirement, it should be applied consistently across the complete network security architecture and applicable network devices. Specifying fail-open only for a single stateful solution does not provide meaningful operational value and may unnecessarily restrict wider OEM participation. Suggested Clause: The proposed WAF solution must support high availability in both Layer 2 and Layer 3 deployments.	Please refer Addendum 1 for the revised clause.
269	149	14.2 APPENDIX 1B: Technical Compliance Sheet WAF S. No. 92		The solution must have bypass segments to ensure that fail open in case of hardware failure	Fail-open/Bypass is not relevant in the context of a stateful security solution, as maintaining session and connection state is essential to its intended operation. If fail-open functionality is considered a mandatory requirement, it should be applied consistently across the complete network security architecture and applicable network devices. Specifying fail-open only for a single stateful solution does not provide meaningful operational value and may unnecessarily restrict wider OEM participation. Suggested Clause: The solution must support high availability	Please be guided by the RFP
270	149	14.2 APPENDIX 1B: Technical Compliance Sheet WAF	New Clause Request	Suggested Clause: The solution should provide comprehensive protection against API-based attacks, including the OWASP API Security Top 10 and Broken Object Level Authorization (BOLA) attacks. It should also provide comprehensive bot management and mitigation capabilities, covering Gen 1 through Gen 4 bot attacks, to ensure effective protection against both automated and sophisticated application-layer threats.	The solution should also support next-generation security features and emerging threat-protection capabilities to ensure effective protection against evolving cyber threats.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
271	40	Appendix 1A Functional Specification Centralised key management solution (KMS)	3	The system should support AES(128-256), ARIA,ECC(224-512), Brainpool curves, HMAC , TDES, RSA(512-4096) and the Crypto mode (CBC, CBC-CS1,ECB,GCM) etc.	The requirement specifies CBC-CS1 as a mandatory cryptographic mode. Please clarify the specific use case and security/compliance rationale for mandating CBC-CS1. As cryptographic implementations may use different standards-compliant modes depending on the data type and encryption architecture, we request that this vendor/implementation-specific reference be removed and the requirement be amended to accept equivalent FIPS-approved and industry-standard encryption modes providing an equivalent or higher level of security.	Please refer Addendum 1 for the revised clause.
272	40	Appendix 1A Functional Specification Centralised key management solution (KMS)	4	The system should support API REST (JWT),SOAP, KMIP, PKCS#11, JCE, .NET, MSCAPI, MS CNG, C,NAE,XML, Java API's and libraries for integration with custom applications.	The requirement specifies NAE/XML as an integration interface. Please clarify the business or technical requirement necessitating NAE/XML specifically. We request that the requirement be made interface/vendor neutral by replacing NAE/XML with 'industry-standard secure APIs/interfaces such as REST API, KMIP, PKCS#11, JCE/JCA, Microsoft CAPI/CNG or equivalent'. This will allow equivalent solutions to participate without mandating a specific vendor interface.	Please refer Addendum 1 for the revised clause.
273	40	Appendix 1A Functional Specification Centralised key management solution (KMS)	7	Solution should be capable of determining application reading data and abnormal spike in I/O are notified and blocked from Encrypting Data thus providing ransomware protection	The requirement for ransomware protection appears to require process-level behavioural monitoring and analysis, including identification of abnormal process behaviour, suspicious file-access/encryption activity, detection of ransomware-like processes, and blocking/termination of such processes. This functionality is generally associated with EDR/XDR or endpoint anti-ransomware solutions and is distinct from encryption, key management and access-control functionality. We therefore request that the Bank mitigate this requirement through integration with the Bank's existing EDR/XDR solution. Please amend the clause to native process-level ransomware detection and blocking should be done by EDR/XDR where logs from the solutions are forwarded to the SIEM/SOC to identify anomalies.	Please refer Addendum 1 for the revised clause.
274	40	Appendix 1A Functional Specification Centralised key management solution (KMS)	8	Solution should support Multi Factor Authentication (MFA) for users accessing protected path on Windows Servers either throught inbuilt feature or intergrating with the bank's MFA solution	The requirement specifies Multi-Factor Authentication (MFA) for users accessing protected resources/paths. Protecting a storage path is what the encryption solution + KMS will achieve , however accessing the path with MFA is primarily an Identity and Access Management (IDAM) capability involving user identity verification, authentication factors, authentication policies and access control, rather than a core encryption or Key Management System (KMS) functionality. Since the scope of the proposed solution is focused on data encryption, key management and protection of data, please clarify whether the MFA requirement can be reclassified under the IDAM section of the RFP and addressed through the Bank's existing enterprise MFA/IDAM solution as per the RFP.	Please refer Addendum 1 for the revised clause.
275	40	Appendix 1A Functional Specification Centralised key management solution (KMS)	23	The Proposed solution should be capable of Ransomware detection and blocking capability	The requirement for ransomware protection appears to require process-level behavioural monitoring and analysis, including identification of abnormal process behaviour, suspicious file-access/encryption activity, detection of ransomware-like processes, and blocking/termination of such processes. This functionality is generally associated with EDR/XDR or endpoint anti-ransomware solutions and is distinct from encryption, key management and access-control functionality. We therefore request that the Bank mitigate this requirement through integration with the Bank's existing EDR/XDR solution. If integration is acceptable, please amend the requirement accordingly and confirm that native process-level ransomware detection and blocking should be done by EDR/XDR where logs from the solutions are forwarded to the SIEM/SOC to identify anomalies.	Please refer Addendum 1 for the revised clause.
276	104	OEM Evaluation Criteria	18	The proposed OEM solution/product should have been successfully implemented in least two Scheduled bank (including financial regulators).	Please relax the clause and change it to "The proposed OEM solution/product should have been successfully implemented in least two Scheduled bank (including financial regulators) or a PSU.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
277	101	10.2	Eligibility Evaluation Criteria	Bidder should have supplied, installed and maintained (or under maintenance) at least 10 of the below solutions in any one PSU/PSE/ BFSI/Government Organizations/ Regulatory & Statutory body in India:	We request the Bank to allow technical experience of the bidding entity's branch office/ parent/ sister/member of same network or member of same global firm as well. Rationale: We understand that project experience sought in this technical evaluation criteria stipulates to provide credentials of solutions mentioned. The global assignments are of similar nature and have been undertaken by the entities in the corresponding geography. These entities are separate legal and independent entities and are referred as a network of member firms. Additionally, as a general practice followed by most of the PSUs/ Ministries, technical experience and resources of the bidding entity's branch office/ parent/ sister/member of same network or member of same global firm is considered.	Please be guided by the RFP
278	101	10.2	Eligibility Evaluation Criteria	Copy of Purchase Order/Work Order/ Contract AND In addition to the above, bidder to provide the following: a) Client credential/reference letter specifying the product deployed and the current status/stage of the project; OR b) Email confirmation from the client specifying the product deployed and the current status/stage of the project; OR c) Client-signed implementation signoff/ report confirming successful implementation of the solution; Note: The submitted documentary evidence must clearly identify the customer, the product/solution deployed, and the implementation and/or maintenance status relevant to the criterion for each of the products.	We request the Bank to kindly add a clause as under. ""In case where the bidder cites the reasons of Non-Disclosure Agreement (NDA) for its inability to submit necessary documents in support of meeting the experience criteria, Bidder has to submit letter / certificate, certifying all the required information, issued by CEO / CFO / Authorized Signatory of the bidder, with an endorsement by Chartered Accountant/ Statutory Auditor/ Certified Public Accountant (not being an employee or a Director or not having any interest in the bidder company / firm). The endorsement by Chartered Accountant / Statutory Auditor/ Certified Public Accountant should clearly specify their UDIN as well." Rationale: As an industry practice, the tenders floated by Indian PSUs allow the bidders to certify the project experience by CEO/ CFO/ Head of bidding entity/ MD/Partner of the company along with an endorsement by Chartered Accountant/ Statutory Auditor/ Certified Public Accountant/ TPIA/ Chartered Engineer (not being an employee or a Director or not having any interest in the bidder(s) company / firm) (Please refer to above clause from GeM bid number GEM/2026/B/7408393 of Indian Oil Corporation Limited which got submitted recently for your kind consideration)	Please be guided by the RFP
279	116	11.1	Product (Software) Cost	Product License Cost: 50% on successful delivery of licenses and OOTB installation proof, 20% on successful UAT Sign-Off, 30% on successful Go-Live of the respective product Subscription Cost (One time license Cost): 50% on successful delivery of the licenses and OOTB installation proof, 20% on successful UAT Sign-Off, 30% on successful Go-Live of the respective product.	Request the Bank to revise the payment milestone for Product License Cost and Subscription cost (One time License cost) to 80% upon successful delivery of licenses and OEM entitlement/activation confirmation, and 20% upon successful UAT Sign-Off, considering that software licenses are supplied upfront and ownership transfers to the Bank upon delivery. Justification: Software license costs are incurred by the bidder/OEM at the time of procurement and delivery. Aligning 80% payment against delivery and 20% against UAT will facilitate timely OEM payment obligations while ensuring adequate performance protection to the Bank through the balance payment linked to successful UAT.	Please be guided by the RFP
280	120	12.1	Service Level Agreement	Total penalties due Service level and liquidated damages shall not exceed 10% of the Total contract value.	We request Bank to consider capping the Liquidated Damages at a maximum of 5% of the value of the undelivered/unperformed portion of the contract instead of 10% of the total contract value. Justification: Liquidated Damages should be proportionate to the delayed or affected portion of the scope. Applying LD on the total contract value, including completed and accepted portions of work/services, may not adequately reflect the actual impact of the delay. Capping LD at 5% of the undelivered/unperformed portion is a widely accepted industry practice.	Please be guided by the RFP
281	209-9	15.21.4 Deployment & Data Retention	Point 9. DAM	150 Applications Database at DC and 150 Application Database at DR	Please confirm whether the DR environment is expected to handle application requests independently during normal operations, or only in the event of DC failure/failover, when application requests are redirected to DR.	Refer Annexure 21 – Deployment & Data Retention table. Deployment requirement is solution-specific and stated therein

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
282	209-10	15.21.4 Deployment & Data Retention	Point 9. DAM	Bank's DC - HA (N+N Active-Active) deployment Bank's DR - HA (N+N Active-Active) deployment	As per our understanding for collector deployment it is a N+1 architecture and for Central Manager/Any other pplication components deployment should be in a N+N architecture at each location	Please be guided by the RFP. The proposed solution shall comply with the HA (N+N Active-Active) deployment at both DC and DR
283	206	15.21.3 Current IT assets	Current Asset Description	Database 300	Please provide the complete inventory of in-scope databases, including database location (DC/DR/NDR), deployment model (On-Premises/IaaS/PaaS/DBaaS), database type, version, and CPU cores of the associated servers.	The details shall be shared with the successful bidder
284	206	15.21.3 Current IT assets	Current Asset Description	Database 300	The RFP specifies 300 application databases. We are assuming this represents 300 database servers(total count of database server physical/virtual). Please confirm whether this assumption is correct.	Please be guided by the RFP
285	209-10	15.21.4 Deployment & Data Retention	Point 9. DAM	1 Month (Logs and Data Storage on Appliance / Primary Storage)	Please confirm the expected daily database activity log volume (GB/day) across DC and DR, to enable sizing for the specified one-month log and data retention requirement.	Details shall be shared with the Successful bidder.
286	42	7.3.3.1 Database Activity Monitoring Appendix 1A Functional Specification.pdf Sheet Name: DAM. Point 75		1. Proposed solution should comply with the requirement mentioned in Appendix 1: Functional compliance sheet, Sheet Name: DAM.	Please confirm whether the solution is expected to support future growth in the number of databases beyond the currently stated 300 databases. If so, please provide the expected database growth over the proposed solution lifecycle. The proposed solution shall support monitoring of all databases covered under the procured licenses and shall support future expansion	Please be guided by the RFP
287	42	7.3.3.1 Database Activity Monitoring Appendix 1A Functional Specification.pdf Sheet Name: DAM. Point 47	1. Proposed solution should comply with the requirement mentioned in Appendix 1: Functional compliance sheet, Sheet Name: DAM.	Solution should detect attacks on network protocols, as well as application layer DB activity.	We understand the requirement for detection of attacks on network protocols is limited to database-related network traffic/protocol activity .Please confirm	Yes, and please be guided by the RFP
288	42	7.3.3.1 Database Activity Monitoring Appendix 1A Functional Specification.pdf Sheet Name: DAM. Point 61	1. Proposed solution should comply with the requirement mentioned in Appendix 1: Functional compliance sheet, Sheet Name: DAM.	The agent deployment/activation should not require a reboot of OS and DB services (except in case database is using native encryption feature) after installation/configuration. Only one OEM DAM agent to be installed, if required. All agents regardless of deployment mode should be managed from the centralized management console	As per our understanding the solution inherently does not require a restart . However, for OS platforms where a restart is inherently required for agent installation (e.g., AIX), the applicable OS restart requirement would apply to the DAM agent installation as well. Please confirm this	Yes, and please be guided by the RFP
289	42	7.3.3.1 Database Activity Monitoring Appendix 1A Functional Specification.pdf Sheet Name: DAM. Point 82	1. Proposed solution should comply with the requirement mentioned in Appendix 1: Functional compliance sheet, Sheet Name: DAM.	The solution shall support inbult authentication and integration with enterprise Identity and Access Management (IAM) platforms, including LDAP/Active Directory, RADIUS, SAML, TACACS+, and other industry-standard authentication mechanisms	Please clarify whether the TACACS+ requirement is applicable to the DAM solution, as TACACS+ is primarily used for authentication and access control of network devices. We understand that TACACS+ is not applicable to the DAM solution and that the requirement is intended for network devices. Please confirm that TACACS+ support is therefore not required as a mandatory part of the DAM scope.	Please refer Addendum 1 for the revised clause.

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
290	42	7.3.3.1 Database Activity Monitoring Appendix 1A Functional Specification.pdf Sheet Name: DAM. Point 114	1. Proposed solution should comply with the requirement mentioned in Appendix 1: Functional compliance sheet, Sheet Name: DAM.	The Risk Analytics Solution should automatically detect the following: a) Nature of accounts which connect to the database (Service Account, DBA User Account, etc.) b) Purpose of database tables (Business Critical Tables, System Tables, etc.) c) Data access habits (working hours, amount of data retrieved)	We understand that one-time customer-defined classification of accounts and tables, followed by automated classification and behavioral analysis of access patterns, would be an acceptable approach. Please confirm.	Bidder to propose the approach to meet the requirement
291	100	10.2	Eligibility Criteria Clause	The bidder should have a minimum average annual turnover of INR 1000 crore in India during the last 3 financial years (i.e. 2022-23, 2023-24 & 2024–25) along with positive net worth.	Kindly check if minimum averga turnover can be reducced to 500 Crore instead of 1000 crore	Please refer Addendum 1 for the revised clause.
292	104	10.2 Eligibility Evaluation Criteria	18	OEM Evaluation Criteria "In addition to the above, bidder to provide the following:"	Clarification required: Its mentioned as Bidder, however We understand its OEM to provide the Eligibility documents	OEM documentation need to be sought and collated by the bidder and submitted as part of the Bidder's proposal.
293	62	Training	7.5.8	At a minimum, the following training programs shall be conducted for each proposed solution/OEM:	The training requirements are quite high, its coming to be 40 days per solution. Please re-consider	Please refer Addendum 1 for the revised clause.
294	18	Web Gateway		The solution should be on premise appliance based and must Provide Web Proxy, Caching, Web based Reputation filtering, URL filtering, Antivirus, Antimalware, Enterprise Data protection control with minimum 1500 templates inbuilt with English Language support, Application Visibility & control, Detail Reporting and Management. . Load balancing should be inbuilt in the appliance or should work with Bank's existing load balancer with no additional cost.	The clause currently specifies support only for the English language. However, sensitive and confidential data in the banking sector may also be available in Hindi. Therefore, the solution should support Hindi language content to ensure effective data protection and avoid potential compliance gaps like DPDPA. Hence, Hindi must be included.	Please be guided by the RFP
295	20	Web Gateway		The proposed solution shall support PQC readiness, including support for secure cryptographic mechanisms and standards that facilitate future migration to quantum-resistant cryptography, wherever applicable to the solution	Current industry-wide PQC adoption in proxy/TLS-inspection appliances is still maturing, with hybrid key-exchange mechanisms (e.g., ML-KEM) emerging as the near-term path rather than full production deployment. We understand the requirement is for the OEM to have a defined PQC roadmap and support for hybrid/quantum-resistant TLS key-exchange mechanisms as they become available/standardised, rather than mandating PQC algorithms from day1. Kindly confirm if the understanding is correct.	Please be guided by the RFP
296	27	DLP		The solution should be capable to fingerprint the data generated from specific applications, Web URLs, Data Repositories, Network Shares	Need clarity on the use-case of fingerprinting data generated from specific applications, Web URLs, Data Repositories, and Network Shares. DLP fingerprints data via discovery crawls of structured (databases) and unstructured (file shares, repositories) data sources, irrespective of where the data is generated. Hope the same is expected here, kindly confirm.	Yes, and please be guided by the RFP
297	21	Appendix 1A Functional Specs :Zero Day	Clause 10 "Zero-Day Attack Protection for Endpoint and Network"	Solution must be a custom built on premise dedicated Anti-APT solution	We Request to amend this clause as below "Solution should be a purpose-built dedicated hardware appliance and must not be part or component of devices like NGFW, IDS/IPS, DDOS, UTM etc and The proposed solution shall be from different OEM than the existing OEMs of firewalls and IPS to ensure the multi layer security controls in the network and to utilize threat intelligence from different OEMs." Justification:Purpose-built architecture eliminates security risks associated with multi-function integration and ensures the solution is optimally engineered specifically for sophisticated threat detection and sandbox analysis, not as a secondary component of broader security platforms. The addition of "hardware" specification guarantees a dedicated appliance with isolated processing and memory resources, eliminating resource contention and ensuring consistent, high-fidelity threat detection independent of other workloads.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
298	21	Appendix 1A Functional Specs :Zero Day	Clause 29 Zero-Day Attack Protection for Endpoint and Network	The proposed solution should be able to run at least 50 parallel sandboxes for analysis of payload and on premise customized sandbox solution should have the capability to allow manual submission of suspicious files for analysis	We request to amend this clause as below "The proposed solution should be able to run at least 30 sandboxes for analysis of payload and on premise customized sandbox solution should have the capability to allow manual submission of suspicious files for analysis" Justification: 30 sandboxes provide sufficient concurrent analysis capacity for enterprise-scale payload examination while optimizing on-premises infrastructure costs and resource utilization without compromising threat detection throughput. This aligns with industry standards for mid-to-large deployments and allows for prioritized analysis of critical threats while maintaining manual submission and review capabilities for suspicious files.	Please refer Addendum 1 for the revised clause.
299	208	15.21.4 Deployment & Data Retention	Clause : 5	Bank's DC - HA (N+N Active-Active) deployment 2. Bank's DR - HA (N+N Active-Active) deployment 3. The sandboxing environment a. HA (N+N Active-Passive) deployment at DC b. HA (N+N Active-Passive) deployment at DR	We request to amend this clause as below " "Bank's DC - HA (N+N Active-Passive) deployment 2. Bank's DR - HA (N+N Active-Passive) deployment 3. The sandboxing environment (on the same box) a. HA (N+N Active-Passive) deployment at DC b. HA (N+N Active-Passive) deployment at DR" Justification: Solution architected to support Active-Passive HA deployment with integrated Virtual Analyzer sandboxing on the same appliance, reducing capital expenditure and operational complexity while maintaining high availability and disaster recovery capabilities. Co-locating the sandbox environment eliminates unnecessary hardware duplication, simplifies failover orchestration, and reduces the overall footprint and management overhead in both DC and DR environments. This architecture aligns with native design principles and industry best practices for dedicated security appliances, delivering equivalent threat detection and analysis performance with improved cost efficiency and operational manageability.	Please be guided by the RFP
300	210	15.21.4 Deployment & Data Retention	Clause 11	1. Bank's DC - HA (N+N Active-Active) deployment 2. Bank's DR - HA (N+N Active-Active) deployment	We request to amend this clause as below 1. Bank's DC - HA (N+N Active-Passive) deployment 2. Bank's DR - HA (N+N Active-Passive) deployment Justification: Agent-based architecture inherently provides distributed protection across workloads, eliminating the need for Active-Active manager redundancy while maintaining high availability through Active-Passive configuration with synchronized database replication. Active-Passive deployment reduces infrastructure complexity, operational overhead, and licensing costs while delivering equivalent resilience and failover protection in both DC and DR environments.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
301		Appendix 1A Functional Specs :Zero Day	Recommended clause to be added		We request to add this clause as part of HIPS Solution should have the capabilities to shield vulnerabilities until the actual patch is deployed. There should not be any new rules that should be enabled or disable for shielding a vulnerability. Justification Technical: Provides a compensating control (virtual patch/shield) that blocks exploitation of a known vulnerability at the network/host layer without altering the underlying OS or application configuration, and without requiring new rules to be toggled on/off for each shielding action. This removes the change-control and regression-testing burden that comes with pushing every rule change through the bank's server hardening process. Business: Production servers cannot always be patched immediately (vendor patch cycles, application compatibility testing, maintenance-window constraints). Virtual patching closes the exposure window between vulnerability disclosure and actual patch deployment, reducing risk of exploitation while avoiding unplanned downtime to revenue-generating systems. This is consistent with CERT-In's guidance (ref. CISG-2026-03, cert-in.org.in) that recommends virtual patching/shielding as a compensating control until the permanent patch is applied. Reference link of Cert-in Guidelines URL: https://www.cert-in.org.in/s2cMainServlet?pageid=GUIDLNVIEW02&refcode=CISG-2026-03 Reference: page 5 of 12	Please be guided by the RFP, the clause reference is with respect to HIPS and not Zero Day Attack
302		Appendix 1A Functional Specs :Zero Day	Recommended clause to be added		We request to add this clause as below "HIPS solution should support policies creation based on - User defined and Recommendation scan." Justification Technical: Recommendation-scan based policy creation automatically profiles each server (OS, installed applications, open ports) and proposes the applicable security policy, while still allowing security teams to author custom, user-defined policies for non-standard servers. Business: Reduces manual policy-authoring effort and the risk of human error across the bank's large and heterogeneous server estate (branches, DR site, data centre), speeding up onboarding of new servers and ensuring a consistent security baseline is applied bank-wide, which supports audit and regulatory reporting. Reference link of Cert-in Guidelines URL: https://www.cert-in.org.in/s2cMainServlet?pageid=GUIDLNVIEW02&refcode=CISG-2026-03 Reference: page 4 of 12 (b) Immediate Disclosure of Critical and High-Severity Vulnerabilities"	Please be guided by the RFP, the clause reference is with respect to HIPS and not Zero Day Attack

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
303		Appendix 1A Functional Specs :Zero Day	Recommended clause to be added		We request to add this clause as part of RFP ask "Proposed HIPS solution should support virtual patching of both known and unknown vulnerabilities." Justification Technical: Combines signature-based protection for known CVEs with behaviour/anomaly-based IPS detection for zero-day and unknown vulnerabilities, giving layered protection that does not rely solely on vendor patches or signature updates. Business: Protects revenue-critical banking applications from exploitation even before a vendor patch or signature exists, minimising both financial and reputational risk from a breach. This directly aligns with CERT-In's guideline referenced at cert-in.org.in (ref. CISG-2026-03), which calls out virtual patching as the recommended compensating control for both known and unknown/zero-day vulnerabilities. Reference link of Cert-in Guidelines URL: https://www.cert-in.org.in/s2cMainServlet?pageid=GUIDLNVIEW02&refcode=CISG-2026-03 Reference: page 5 of 12	Please be guided by the RFP, the clause reference is with respect to HIPS and not Zero Day Attack
304	1	Appendix 1A Functional Specification	2	The system should support an easy way to centrally store and manage key & secret lifecycle tasks	Kindly clarify whether "secret lifecycle tasks" is expected to include advanced enterprise secrets-management capabilities such as automated secret creation and rotation, dynamic/just-in-time secret generation, secret expiry and revocation, centralized policy-based access control, audit logging, and secure delivery of secrets to applications, DevOps tools, containers and cloud-native environments. If confirmed, we request the Bank to revise the clause as, "The system should support an easy way to centrally store and manage key & shall provide centralized management of static and dynamic secrets, including secure storage, automated rotation, expiry/revocation, policy-based access control, audit logging, and secure delivery to applications, containers, Kubernetes and cloud-native environments."	Please be guided by the RFP. Bidder to design the solution, including all the components, complying with the requirement stated in the RFP with respect to deployment, retention and other terms
305	1	Appendix 1A Functional Specification	6	The encryption of file/folders should be as per with FIPS approved & certified mechanisms & optionally , should not require any downtime while data encryption occurs.	Kindly clarify whether the Bank requires the proposed file/folder encryption solution to have an independently FIPS-validated cryptographic module, separate from the KMS FIPS certification, and to support online encryption of existing data without application or business downtime. If confirmed, we request the Bank to revise the clause as "The file and folder encryption solution shall use an independently FIPS approved cryptographic mechanism. The OEM shall submit the applicable FIPS certificate covering the proposed file/folder encryption product other than KMS FIPS certificate. The solution shall support uninterrupted encryption mechanism to encrypt existing data online without requiring application or business downtime, while maintaining continuous data availability throughout the encryption process."	Please be guided by the RFP
306	1	Appendix 1A Functional Specification	7	Solution should be capable of determining application reading data and abnormal spike in I/O are notified and blocked from Encrypting Data thus providing ransomware protection	Kindly clarify whether the Bank requires the solution to provide real-time, process-level ransomware detection using behavioural or machine-learning analysis, with automatic alerting and blocking of the offending process from accessing protected data. If confirmed, we request the Bank to revise the clause as, "The solution shall provide real-time, process-level ransomware detection using behavioural or machine-learning analysis, with automatic alerting and blocking of the offending process from accessing protected data. The capability shall provide proactive prevention and shall not rely solely on signature-based detection or post-incident recovery mechanisms."	Please refer Addendum 1 for the revised clause.

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
307	1	Appendix 1A Functional Specification	9	The Block Cipher Encryption software should incorporate the encryption without having dependency on the native encryption capabilities of storage, database, cloud or Hypervisor. Well versed and adaptable with latest deployment technologies like Kubernetes, docker etc.	The Kubernetes requirement is broad and does not clearly define the expected level of Kubernetes support. Kindly clarify whether native Kubernetes integration is required for transparent encryption and access control of persistent data without application modification or reliance on native storage encryption. If confirmed, we request the Bank to revise the clause as, "The Block Cipher Encryption software should incorporate the encryption without having dependency on the native encryption capabilities of storage, database, cloud or Hypervisor. The solution shall natively support Kubernetes for transparent encryption and policy-based access control of persistent data, without application modification."	Please be guided by the RFP
308	1	Appendix 1A Functional Specification	10	The solution should provide capabilities for key discovery, vulnerability assessment, centralized inventory, key management and provisioning, as well as alerting, logging, and reporting. It should also include a powerful dashboard to monitor the status of all activities.	Vulnerability assessment is generally a separate infrastructure/application security function, we request the Bank to consider removing this requirement from the scope of the Key Management and revise the clause as, "The solution should provide capabilities for key discovery, centralized inventory, key management and provisioning, as well as alerting, logging, reporting, and a centralized dashboard to monitor the status of all activities."	Please be guided by the RFP
309	1	Appendix 1A Functional Specification	22	The solution should have the capability to support bulk encryption and transformation from File to file , File to DB , DB to DB and DB to file	Kindly clarify whether the proposed solution is required to natively support bulk data encryption and transformation across all four workflows through the OEM-provided solution, without custom development or dependency on third-party tools.	Please be guided by the RFP
310	1	Appendix 1A Functional Specification	23	The Proposed solution should be capable of Ransomware detection and blocking capability	Kindly clarify whether the proposed solution is required to provide real-time, process-level ransomware detection using behavioural or machine-learning analysis, with automatic alerting and blocking of the offending process from accessing protected data.	Please refer Addendum 1 for the revised clause.
311	1	Appendix 1A Functional Specification	42	Security between HSM and the HSM client includes Message authentication	The term “message authentication” does not define whether authentication is required at the transport layer or through a cryptographic message-authentication mechanism. The requirement should focus on ensuring the authenticity and integrity of communications between the HSM client and the HSM. Requesting Bank to revise this clause as, "The HSM shall provide mutually authenticated and integrity-protected communication between the HSM client and the HSM using a secure communication mechanism, ensuring protection against unauthorized access."	Please be guided by the RFP
312	1	Appendix 1A Functional Specification	44	HSM should have FIPS 140-3 Level 3 security certification (with certification in the name of OEM)	The FIPS certification requirement should ensure that the proposed HSM is a complete, OEM-manufactured and supported security solution, rather than an appliance assembled or bundled using cryptographic hardware from another OEM. This will ensure single-OEM accountability for the HSM appliance, cryptographic hardware, firmware, and security certification. Requesting Bank to revise this clause as, "The HSM shall have a valid FIPS 140-3 Level 3 certification in the name of the OEM. The proposed HSM appliance and its cryptographic card shall be from the same OEM as an integrated HSM solution. Bundled, assembled, or integrated solutions using cryptographic cards from a different OEM shall not be considered compliant."	HSM should have FIPS 140-3 Level 3 security certification (with certification in the name of OEM). Rebranded, private label, or third party sourced cryptographic modules are not permitted. The FIPS 140-3 security policy of the HSM should not have any references to a third party certified firmware.
313	1	Appendix 1A Functional Specification	49	HSM must have containerization to allows granular control of key material for applications requiring high assurance by providing segregation of partition traffic for each applications	The term “containerization” is ambiguous in the context of an HSM. Kindly clarify whether the requirement is intended to mandate cryptographically isolated logical partitions for separate applications.	Please be guided by the RFP
314	1	Appendix 1A Functional Specification	51	HSM must support clustering of HSMs and load balancing without the need of external load balancer , The HSM should be capable of forming HA with existing HSM	Kindly clarify whether the HSM HA architecture is required to provide native active-active load balancing, automatic failover and recovery, without requiring any external load balancer or application changes, with automatic synchronization of cryptographic objects when an HSM is added or recovered. If confirmed, request the Bank to revise the clause as, "The HSM shall support native active-active High Availability with automatic load balancing, failover and recovery without requiring an external load balancer. Cryptographic requests shall be dynamically distributed across active HSM members, and upon failure, pending operations shall automatically fail over to available members. The solution shall support automatic synchronization of cryptographic objects when an HSM member is added or recovered."	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
315	1	Appendix 1A Functional Specification	53	The HSM must support the latest containerized technology that allows multiple independent containerized HSM to run in a single HSM machine. Each containerized HSM is independent and isolated from others, they can be started, stop and upgrade firmware without affecting the rest of containerized HSMs in the machine.	Kindly clarify whether the requirement for multiple independently running containerized HSM instances is mandatory for the proposed HSM when its intended role is to act as the Root of Trust for the KMS. If the objective is segregation and isolation of cryptographic keys and applications, we request the Bank to revise the requirement to logical/cryptographic partitioning instead, such as, "The HSM shall support multiple logically and cryptographically isolated partitions within a single physical HSM, providing strong segregation of keys, applications, administrators, and cryptographic operations. Each partition shall operate as an independent logical security domain with separate access controls and key material."	Please be guided by the RFP
316	1	Appendix 1A Functional Specification	54	The HSM shall provide supported Software Development Kit (SDK) and standard cryptographic interfaces/ APIs to enable application integration, cryptographic operations, and development of supported extensions without compromising the security certification of the HSM.	The term “development of supported extensions” imply modification or development of custom functionality within the HSM, which could affect the HSM's validated security boundary and certification. Kindly clarify whether “development of supported extensions” refers to the use of OEM-supported SDKs, APIs, and documented extensions for application integration. If confirmed, we request the Bank to revise the clause as, "The HSM shall provide supported Software Development Kit (SDK) and standard cryptographic interfaces/ APIs to enable application integration, cryptographic operations, and use of supported SDK extensions and APIs without compromising the security certification of the HSM."	Please be guided by the RFP
317	1	Appendix 1A Functional Specification	55	The HSM shall support secure lifecycle management of cryptographic keys, including backup, restore, replication, and distribution mechanisms for secure management of Post-Quantum Cryptographic algorithms, including stateful algorithms	The requirement for backup, restore, replication, and distribution of keys used with stateful PQC algorithms shouldn't be applicable, as duplication or restoration of stateful key material can create security risks due to potential reuse of state. Requesting Bank to revise this clause as, "The HSM shall support secure lifecycle management of cryptographic keys, including backup, restore, replication, and distribution mechanisms for secure management of Post-Quantum Cryptographic algorithms. For stateful algorithms, lifecycle operations shall preserve the required cryptographic state and prevent unsafe duplication, rollback, or reuse of state."	Please be guided by the RFP
318	1	Appendix 1A Functional Specification	57	HSM should support the backup on FIPS certified hardware device, not to file in any form.	Kindly clarify whether the Bank requires the HSM backup device to be FIPS 140-3 Level 3 validated. If confirmed, we request the Bank to revise the clause as, "HSM should support the backup on FIPS certified hardware device, not to file in any form."	Please refer Addendum 1 for the revised clause.
319	211	15.21.4 Deployment & Data Retention	19	S-BOM, C-BOM, AI-BOM & QBOM Volumetrics: HSM – 16 Qty	Kindly clarify the intended use case and technical specifications for the 16 HSMs mentioned under the volumetrics requirement to enable appropriate sizing and solution proposal.	Bidder to right size as per the RFP
320	203	15.21 Annexure 21: Sizing/Volumetrics, Data Retention and Current Infrastructure	1	Non-Production Environment: For appliance-based solutions, the bidder shall design and propose an appropriate non-production environment to support testing, validation, upgrades, patching, configuration changes, policy tuning, rule testing, and other activities during the contract period without impacting production services. For VM-based solutions, the non-production environment shall be sized at a minimum of 10% of the Production (DC) environment unless otherwise specified in the RFP.	Kindly clarify the deployment and availability requirements for the Non-Production environment, including whether the solution is required at the DC, DR, or both locations, and whether a standalone appliance or an HA deployment is required.	Please refer Annexure 21 of the RFP
321	1	Appendix 1A Functional Specification	6	The encryption of file/folders should be as per with FIPS approved & certified mechanisms & optionally , should not require any downtime while data encryption occurs.	Please clarify the number of servers/VMs in scope for file/folder encryption?	Bidder to right size and design the solution. Further details should be discussed with the successful bidder during the SRS Stage
322	1	Appendix 1A Functional Specification	21	The Key Management solution must have KMIP support to enable the solution to store the encryption keys of solutions providing native encryption ensuring that even if the disk drives (physical or virtual) are stolen, the data stored within them remains protected against unauthorized access.	Please clarify the total number of KMIP clients will be in scope?	Bidder to right size and design the solution. Further details should be discussed with the successful bidder during the SRS Stage
323	1	Appendix 1A Functional Specification	22	The Bidder should support separate key management from CSP provider-controlled encryption; this key management component should be fully managed and owned by NIC. The Bidder shall support generation, storage and import/export of keys in BYOK scheme for multiple CSPs including: AWS, Azure, GCP, Oracle and Salesforce etc.	Please clarify the number of accounts/subscription/project/tenancy will be in scope for this requirement.	Bidder to right size and design the solution. Further details should be discussed with the successful bidder during the SRS Stage
324	1	Appendix 1A Functional Specification	9	The Block Cipher Encryption software should incorporate the encryption without having dependency on the native encryption capabilities of storage, database, cloud or Hypervisor. Well versed and adaptable with latest deployment technologies like Kubernetes, docker etc.	Please clarify the number of Kubernetes and docker will be in scope for this requirement.	Bidder to right size and design the solution. Further details should be discussed with the successful bidder during the SRS Stage

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
325	1	Appendix 1A Functional Specification	22	The solution should have the capability to support bulk encryption and transformation from File to file , File to DB , DB to DB and DB to file	Please clarify the number of bulk encryption targets will be in scope for this requirement.	Bidder to right size and design the solution. Further details should be discussed with the successful bidder during the SRS Stage
326	1	Appendix 1A Functional Specification	12	The solution should be able to perform the secrets management capability (SSH,API keys, tokens) , including but not limited to secrets of AWS, Azure, Docker ,Kubernetes and should support authentication methods like SAML , API key, Oauth etc.	Please clarify the number of clients will be in scope for secret management.	Bidder to right size and design the solution. Further details should be discussed with the successful bidder during the SRS Stage
327	162	15.5 Annexure 5: Pre-Qualification Criteria	18	OEM Evaluation Criteria: The proposed OEM solution/product should have been successfully implemented in least two Scheduled bank (including financial regulators). 29. Centralized key management solution	Kindly confirm whether the OEM is required to provide reference implementations for key capabilities specifically sought under Centralized key management solution, such as file/folder encryption, BYOK, etc. Further, to ensure that the proposed capabilities are proven in real-world deployments and not limited to product claims, request the Bank to consider providing additional technical weightage to OEMs providing successful reference implementations for these specific requirements.	Please be guided by the RFP
328	1	Appendix 1A Functional Specification-WAF	41	The solution must be able to protect web applications that include Web services (API) content.	Kindly clarify the expected monthly API traffic volume for the bank environment, including projected requirements for future expansion (e.g., 50 million API requests per month)	Details will be discussed with the successfull bidder in the SRS Stage
329	1	Appendix 1A Functional Specification-WAF	77	The solution should be able to block even the most advanced bots that try to emulate standard client behavior and pretend to be web browsers.	Kindly clarify the expected monthly bot traffic volume for the bank environment, including projected requirements for future expansion (e.g., 50 million bot requests per month)	Please be guided by the RFP
330	1	Appendix 1A Functional Specification-WAF	78	Client Identification and Behavioral Analysis Requirement: The solution must support client identification by injecting JavaScript into the browser to collect detailed runtime environment data	Query: Effective client identification and behavioral analysis require sufficient browser-side telemetry to distinguish legitimate users from automated or evasive activity. We request the Bank to enhance the clause to specify collection of at least 150 runtime attributes, including detection of automation tools, unusual screen resolutions, atypical user behavior, and suspicious drivers or browser modifications, to strengthen bot detection and client identification. Requesting Bank to change the clause to: "Client Identification and Behavioral Analysis Requirement: The solution must support client identification by injecting JavaScript into the browser to collect detailed runtime environment data—capturing at least 150 attributes. It should detect anomalies such as: - Presence of automation tools - Unusual screen resolutions - Atypical user behavior (e.g., erratic or absent mouse movements) - Suspicious drivers or browser modifications"	Please be guided by the RFP
331	1	Appendix 1A Functional Specification-WAF	79	The client component (JavaScript) should be resistant to reverse-engineering techniques through advanced code obfuscation techniques and frequent script changes	Query:Client-side JavaScript interrogation is critical for detecting sophisticated bots that attempt to reverse-engineer and emulate legitimate browser behavior. Frequent script rotation, combined with code obfuscation, reduces the effectiveness of such evasion techniques.We request the Bank to specify a minimum JavaScript interogation frequency of once every 10 minutes. Requesting Bank to change the clause to:"The client component (JavaScript) should be resistant to reverse-engineering techniques through advanced code obfuscation techniques and frequent script changes(at least once every 10 minutes)"	Please be guided by the RFP
332	1	Appendix 1A Functional Specification-WAF	80	The system should provide the ability to apply the following actions against traffic classified as BOT: · blocking · monitoring · displaying a captcha	Query: To strengthen bot mitigation, Delay can disrupt automated request patterns without immediate blocking, while Custom Page enables adaptive security responses based on bot risk and behavior. We request the Bank to include Delay and Custom Page as additional actions for traffic classified as BOT, enhancing protection against automated and evasive bot activity. Requesting Bank to change the clause to:The system should provide the ability to apply the following actions against traffic classified as BOT: · blocking · monitoring · displaying a captcha · delay · Custom Page	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
333	1	Appendix 1A Functional Specification-WAF	81	The appliance must be a purpose built WAF with its own custom specialized hardened OS integrated with the proposed hardware.	Query:A hypervisor layer can introduce virtualization overhead and resource contention, resulting in performance throttling and variable latency under high traffic and intensive security inspection workloads. To ensure predictable and consistent WAF performance, we request the Bank to specify that the purpose-built WAF appliance must not use hypervisors and should be purpose build for WAF. Requesting Bank to change the clause to:The appliance must be a purpose built WAF with its own custom specialized hardened OS integrated with the proposed hardware and appliance must not use hypervisors.	Please be guided by the RFP
334	1	Appendix 1A Functional Specification-WAF	95	The solution shall provide built-in Vulnerability Assessment to identify web application vulnerabilities, with the WAF automatically enforcing Virtual Patching policies to protect applications without requiring application code changes. As per the guidelines by Govt Body.	Query:Reference to Clause 43, wherein integration of the WAF solution with Vulnerability Assessment tools is required, we request the Bank to also allow WAF solutions that integrate with Vulnerability Assessment tools to identify vulnerabilities and enforce corresponding Virtual Patching Requesting Bank to change the clause to: "The solution shall provide built-in/integration with Vulnerability Assessment to identify web application vulnerabilities, with the WAF automatically enforcing Virtual Patching policies to protect applications without requiring application code changes. As per the guidelines by Govt Body."	Please be guided by the RFP
335	1	Appendix 1A Functional Specification-WAF	96	The WAF solution should be capable to store all logs for at least one month on appliance itself. Bidder to enusre that bidder right size the same. Bidder to submit the detailed calculation of Hard Disk and RAM requirement to meet the bank RFP ask of storage on-appliance and Response along with any bottleneck mitigation and SLA compliance. If any stage the same is observed bidder is required to provide the additional hardware/component to mitigate the same at no additional cost to the bank	Query: Log forwarding to a SIEM/syslog server, along with archival to external storage, provides scalable long-term retention, centralized access, and avoids dependency on the WAF appliance's local storage capacity. We request the Bank to consider this approach for maintaining the required minimum one-month log retention, while also enabling seamless expansion of the retention period in the future to meet evolving compliance requirements. Requesting Bank to change the clause to:"The WAF solution should be capable to store all logs for at least one month on the appliance or forwarding the logs to a SIEM/syslog server, with logs archived to external storage for at least one month.Bidder to enusre that bidder right size the same. Bidder to submit the detailed calculation of Hard Disk and RAM requirement to meet the bank RFP ask of log retention on-appliance or through supported external storage, along with response to any bottleneck mitigation and SLA compliance. If at any stage the same is observed, bidder is required to provide the additional hardware/component to mitigate the same at no additional cost to the bank."	Please be guided by the RFP
336	203	15.21 Annexure 21: Sizing/Volumetrics, Data Retention and Current Infrastructure	1	Non-Production Environment: For appliance-based solutions, the bidder shall design and propose an appropriate non-production environment to support testing, validation, upgrades, patching, configuration changes, policy tuning, rule testing, and other activities during the contract period without impacting production services. For VM-based solutions, the non-production environment shall be sized at a minimum of 10% of the Production (DC) environment unless otherwise specified in the RFP.	Query for Non-production environment:Kindly clarify the deployment and availability requirements for the Non-Production environment, including whether the solution is required at the DC, DR, or both locations, and whether a standalone appliance or an HA deployment is required for both locations	Please be guided by the RFP Non-Production environment sizing shall follow the generic methodology prescribed in Annexure 21: for appliance-based solutions, bidder to design and propose an appropriate non-production environment; for VM-based solutions, minimum 10% of Production (DC) environment.
337	162	15.5 Annexure 5: Pre-Qualification Criteria	18	OEM Evaluation Criteria: The proposed OEM solution/product should have been successfully implemented in least two Scheduled bank (including financial regulators). 28. Web Application Firewall (WAF)	Query: Considering the mission-critical nature of WAF solution and the performance requirements of the Bank, we request that the OEM qualification criteria be enhanced to require successful implementation of the proposed WAF solution in at least two Indian banking customers, with deployments using 5 Gbps or higher pure WAF throughput appliances.This would help ensure demonstrated experience, proven performance, and operational maturity in comparable banking environments. Requesting Bank to change the clause to: "28. Web Application Firewall (WAF) with 5 Gbps or higher pure WAF throughput appliances for atleast 2 indian banking customers"	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
338	1	Primary Storage	5	Proposed storage solution should be offerred with minimum 2 controllers with minimum 256 GB DRAM Cache memory on the entire storage Solution. The solution should scale to atleast 512GB Cache memory by adding additional controller.	Change To: Proposed storage solution should be offerred with minimum 2 controllers with minimum 128 GB DRAM Cache memory on the entire storage Solution. The solution should scale to atleast 256GB Cache memory by adding additional controller. Explaination: Cache ask should be Reduced as cache of 64GB or less per controller (128GB total) is enough as the latest CPUs, high-speed memory, and Gen 5 PCIe cards deliver the required performance efficiently. Modern storage controllers optimize cache usage, and industry benchmarks confirm that asked performance can be achieved with lower memory. This reduction not only meets technical needs but also decreases hardware, power, and cooling costs, resulting in a lower TCO for the solution	Please be guided by the RFP
339	4	Backup Solution	16	The proposed disk-based storage/appliance must interoperate with industry-leading server platforms and operating systems, and must ingest backup data over a secure, API-based disk-to- disk (D2D) connection.	Change To: The proposed disk-based storage/appliance must interoperate with industry-leading server platforms and operating systems, and must ingest backup data using standard Data protocolos such as FC, ISCI, NFS, S3 Expalination: This specific ask qulifies only specific backup appliance not any target storage as enterprise storage do not support data ingestion using API rather laverage protocols such as FC, ISCI, NFS , S3.	Please be guided by the RFP
340	4	Backup Solution	25	The Proposed Appliance/Backup Storage must provide verification of the Metadata and actual data of the file with strong Checksum Mechanism	Change To:The Proposed Appliance/Backup Solution must provide verification of the Metadata and actual data of the file with strong Checksum Mechanism Explaination: Proposed ask should be from Solution instead of storage as any storage does not offer file-level checksum reporting for backup files. This is typically a function of the backup software (e.g., Commvault, Veeam) that stores backups on storage.	Please be guided by the RFP
341	2	Long Term Storage	4	Addititional Point Request	Point to be written as: Long Term Storage should support WORM (Wrte Once, Read Many) capability to have Data Immutability. Explaination: We recommend implementing WORM (Write Once, Read Many) capability for long-term backup storage to ensure data is protected against accidental deletion and ransomware attacks. Additionally, WORM functionality is required to comply with regulatory guidelines for banking institutions. Since backup storage is expected to provide WORM capability, long-term backup storage should also comply with this requirement to maintain robust data protection .	Please be guided by the RFP
342	1,2,4	Primary Storage Backup Storage Long Term Storage		New Point request	Point to be written as: The proposed storage systems (for all 3 storage requirements), should have launch dates within past 3 years Explainations: We recommend qualifying storage systems with a launch date within the past three years. This approach ensures a better return on investment and reliable long-term support for a period of 7 to 10 years, as required by the bank. Some OEMs are currently offering systems that are over six years old and lack a clear roadmap or support commitment, which poses a risk to long-term operational stability and longitivity.	Please be guided by the RFP
343	GPU Server	ITEM	Form Factor	1U/2U rack mounted with sliding rails	As the server is going to cater Double width high TDP GPU's management of Heat dissipation is key aspect for better GPU performance. Hence we request Bank to allow up to 4U Server.	Please be guided by the RFP
344	GPU Server	ITEM	GPU Memory	94 Gb or higher	We seek clarity from Bank to specify the how many GPU's are needed per system. Also bank should also specify the max GPU Handling/population capability of the system.	Bidder to design based on the deployment requirement of the solution and sizing
345		General	Appendix 1A Functional Specification	Policy-based model routing/weighted load balancing/automatic failover and token/request rate limiting.	This is a part of AI gateways which does not provide security feature but is a Infrastructure component which is not required as per the Bank usecases. Suggested Changes Remove the Clause	Please refer addendum 1 for the revised Clause

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
346				Suggestions & Recommendation for AI Security Stack	Considering the Bank's current stage of enterprise AI adoption and the evolving nature of AI architectures, The solution shall provide comprehensive security controls for enterprise AI applications, including AI discovery, AI Guardrails, prompt/response inspection, Data leakage protection, threat prevention, access control, policy enforcement, monitoring and audit logging. The capabilities may be delivered through an integrated AI Security platform or a dedicated AI Gateway, provided that all specified security outcomes are met	Please be guided by the RFP
347				Suggestions & Recommendation for AI Security Stack		Please be guided by the RFP
348				Suggestions & Recommendation for AI Security Stack		Please be guided by the RFP
349				Suggestions & Recommendation for AI Security Stack	The Bank Specifies an AI gateway as a mandatory component for inspection and control for AI application traffic however considering the current usecase of bank for next 5 years, AI Gateway will introduce complexity and latency only and is not required. Modern AI Security platform provide capabilities such as AI application,Guardrails,Prompt & response inspection,Data leakage protection and monitoring with out requiring dedicated AI gateway.	Please be guided by the RFP
350				Suggestions & Recommendation for AI Security Stack		Please be guided by the RFP
351				Suggestions & Recommendation for AI Security Stack	AI Gateway is an architecture, not a security outcome, NIST AI RMF focuses on the outcomes of Govern, Map, Measure and Manage, rather than prescribing a mandatory gateway product. Requesting the Bank team to reconsider and re-evaluate the requirement for AI Gateway since this RFP belongs to the usecase for AI security.	Please be guided by the RFP
352				Suggestions & Recommendation for AI Security Stack		Please be guided by the RFP
353				Suggestions & Recommendation for AI Security Stack	We request removal of the mandatory standalone AI Gateway requirement because an AI Gateway represents one possible deployment architecture and not a complete AI-security control framework. Employee AI usage, AI-enabled applications and autonomous agents operate through multiple channels, including browsers, SaaS applications, copilots, APIs, private models and tool integrations, which may not traverse a centralized gateway. The requirement should therefore be based on demonstrable security outcomes such as shadow-AI discovery, prompt and response inspection, sensitive-data protection, prompt-injection prevention, agent tool-call control, runtime policy enforcement, audit logging, scalability and high availability	Please be guided by the RFP
354				Suggestions & Recommendation for AI Security Stack		Please be guided by the RFP
355				Suggestions & Recommendation for AI Security Stack	Current asked AI security solution in RFP is oversized for bank requirement and will add huge commercial impact on the overall budget	Please be guided by the RFP
356	3	Functional Specs-Anti DDOS	2	System should have 5 Gbps of clean/legitimate throughput which can scale upto 10 Gbps on the same H/w. System should support more then 20 MPPS. System should be factored on clean/legitimate license throughput.	Change request : System should have 5 Gbps of clean/legitimate throughput which can scale upto 10 Gbps on the same H/w. System should support more then 45 MPPS. System should be factored on clean/legitimate license throughput. Justification : As per best practices for anti DDoS solution, we suggest to size the solution for handling 45 MPPS, to handle large attacks. It is always recommended that DDoS mitigation solution should support minimum 4 MPPS for 1 Gbps of throughput. Keeping best practices in consideration older RFP was asking for 45 M PPS support on H/w.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
357	3	Functional Specs-Anti DDOS	3	System should have 8x10 G ports with fail open support without any external fail open kit. All the interfaces including fibber should support fail open.	Change request : System should have 12x10 G ports with fail open support without any external fail open kit. All the interfaces including fibber should support fail open. Justification : DDoS mitigation platform will be deployed inline and in multi homing environment and to support multiple ISP's more number of ports are preferred, this also helps in investment protection on solution keeping scalability in consideration. In order to terminate 3 ISP's in full redundancy 12 ports are required. Keeping best practices in consideration older RFP was asking for 16 x 10 G ports.	Please be guided by the RFP
358	3	Functional Specs-Anti DDOS	12	Inbuilt mechanism to inspect traffic with external threat feed. System should support minimum 2 million IoC's for both inbound and outbound blocking.	Change Request : Inbuilt mechanism to inspect traffic with external threat feed. System should support minimum 5 million IoC's for both inbound and outbound blocking. (3 Million IoC as Inbuilt and 2 Million from integration with third party intelligence platform on STIX / TAXI without any REST API) Justification : More IoC support will help Broader threat coverage with More malicious IPs, domains, URLs, can be monitored simultaneously and will help in faster detection and blocking also due to growing number of malicious IP's and DDoS launchpad support up to 5 Million IoC's is recommended. Keeping best practices in consideration older RFP was asking for support up to 5 Million IoC's.	Please be guided by the RFP
359	3	Functional Specs-Anti DDOS	21	Mitigation mechanism to protecting against zero-day DoS and DDoS attacks without manual intervention. Automatic Real time signature generation	Change Request: "Mitigation mechanism to protecting against zero-day DoS and DDoS attacks without manual intervention. Automatic Real time signature OR countermeasure generation in real-time ." Justification: DDoS Signatures are FCAP expressions which is limited to L3 and L4 and one of the examples can be "deny protocol udp port 443", which only limited to L3 and L4, while real time countermeasure can mitigate up to L7 by identifying user behaviour pattern and can differentiate between legit user and request coming from DDoS launchpad.	Please refer Addendum 1 for the revised clause.
360	4	Functional Specs-Anti DDOS	44	Able to detect and protect from Zero-Day Network DDoS/DDoS flood attacks on the basis of behavioural DDoS attacks/challenge response mechanism or by an automatically created signature / countermeasure within a minute and must be mentioned in data sheet. The proposed device should also support inbuilt Signatures apart from custom Signatures from Day 1.	Change Request: Able to detect and protect from Zero-Day Network DDoS/DDoS flood attacks on the basis of behavioural DDoS attacks/challenge response mechanism or by an automatically created signature / countermeasure within a minute. The proposed device should also support inbuilt Signatures apart from custom Signatures OR reputation feeds from Day 1. Justification: DDoS Detection and Mitigation signatures are reputation feeds which is the datasets of malicious IP addresses and IP domains along with L3 and L4 expressions.	Please refer Addendum 1 for the revised clause.
361	5	Functional Specs-Anti DDOS	70	The proposed solution shall support on-premises appliance-based, cloud-based/ service-provider-hosted (scrubbing center), or hybrid architectures combining on-premises and cloud-based mitigation, as applicable to the Bank's deployment requirements.	Clarification required : We understand the Hybrid solution of On-Prem Appliance and Cloud Signalling to Upstream ISP fulfils the requirement (refer to Clause #46)	Please be guided by the RFP
362	5	Functional Specs-Anti DDOS	73	The proposed solution shall support PQC readiness and migration capability, including identification of quantum-vulnerable cryptographic algorithms and support for PQC-enabled or quantum-resistant cryptographic standards, wherever applicable to the solution.	Kindly Remove this point. Justification :PQC is not relevant to DDoS mitigation solution.	PQC readiness is intended to cover applicable cryptographic functions, communication interfaces, authentication mechanisms, APIs, certificates and other security components of the proposed solution and support migration to quantum-resistant standards. DDoS vendor need to submit their roadmap or approach on PQC
363	116-118	11 Payment Terms	11.1-11.6	Product, implementation, hardware, ATS/AMC and FM payment milestones	Several payment milestones are linked to UAT/Go-Live/sign-off and, for implementation cost, 10% is payable within three months after successful Go-Live. Please clarify the deemed-acceptance/approval timeline for Bank sign-offs and confirm that payment milestones will not be withheld for delays in Bank approvals or dependencies not attributable to the bidder.	Please be guided by the RFP
364	119-136	12 Service Levels & Penalties	12.2 / 12.3	Penalty cap and At-Risk Amount	Section 12.2 states that total penalties under LD and SLA are capped at 10% of overall contract value, while Section 12.3 defines a monthly At-Risk Amount of 15% of estimated monthly payout. Please confirm that the 10% aggregate cap applies to all LD/SLA/service-credit deductions and that there will be no double recovery through monthly deductions, ARA, PBG invocation or other remedies for the same underlying event.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
365	143-144	13 Terms & Conditions	13.19 / 13.21	Liquidated Damages and Limitation of Liability	Section 13.21 caps aggregate liability at the total Project Cost but excludes specified indemnity/serious misconduct/confidentiality/regulatory claims from the limitation. Please clarify whether SLA penalties, LD, indemnities, recovery amounts and PBG invocation are intended to be cumulative, and confirm the overall liability treatment for claims arising from the same event to avoid double recovery.	Please be guided by the RFP
366	97	8 Contract Period	8	Two-year extension and extension-period pricing	The extension-period pricing is stated as 'shall not exceed 110-120% of last year's AMC/ATS/Facility management rates', which creates ambiguity between 110% and 120%. Please confirm the exact maximum percentage applicable to each extension year and whether the percentage applies separately to AMC, ATS and FM rates or to their combined value.	Shall not exceed 120% of last year AMC/ATC/Facilicity management Rates
367	144-146	13 Terms & Conditions	13.22 / 13.23	Termination for convenience and transition	In case of termination for convenience, the bidder is entitled only to payment for services rendered up to termination and no compensation for the unexecuted portion. Please clarify the treatment of prepaid annual subscriptions/ATS/AMC and delivered hardware/software licenses that remain valid beyond the termination date, including whether unused prepaid amounts will be reimbursed on a pro-rata basis.	Please be guided by the RFP
368	145-146	13 Terms & Conditions	13.23	Transition support beyond contract term	The RFP requires transition assistance to a successor and states that such assistance may extend beyond the contract term. Please confirm that transition services beyond the original contract period, where termination/expiry is not attributable to bidder default, will be separately payable at the agreed contractual rates and that the transition duration will be mutually agreed.	Please be guided by the RFP
369	97	8 Contract Period	8	End-of-Support / End-of-Sales commitment	The RFP requires supplied hardware/software to remain supported throughout the contract including the two-year extension. Please clarify whether the bidder is expected to guarantee OEM support for the full potential seven-year period at bid stage, and whether replacement obligations apply only where an OEM formally announces End-of-Support during the contracted/extended period.	Please be guided by the RFP
370	100 & 158	10.2 Eligibility Evaluation Criteria / Annexure 5 – Pre-Qualification Criteria	Clause 4	Minimum Average Annual Turnover	The RFP stipulates a minimum average annual turnover of INR 1,000 crore in India during the last three financial years (FY 2022-23, FY 2023-24 and FY 2024-25), along with positive net worth. Considering the specialized nature of the proposed IT Security Solutions and Services and to encourage wider participation from established and financially sound system integrators having relevant technical capabilities and experience, we request the Bank to kindly consider reducing the minimum average annual turnover requirement from INR 1,000 crore to INR 500 crore. This relaxation would enable capable bidders with proven experience in implementing and managing large-scale IT security solutions for BFSI/Banking customers to participate, while the requirement for positive net worth and other technical/eligibility criteria would continue to ensure financial and technical capability.	Please refer Addendum 1 for the revised clause.
371	7	1. Key Information	Security Deposit / Earnest Money Deposit	EMD of INR 8.65 Crore	Considering the objective of encouraging wider participation from established and technically capable system integrators, we request the Bank to kindly rationalize the EMD from INR 8.65 Crore to INR 1 Crore. The proposed reduction would enable participation by capable bidders without compromising the Bank's financial safeguards, as the RFP already provides for bid security provisions, performance guarantee and contractual remedies."	Please be guided by the RFP
372	Page No. 104	10.2 Eligibility Evaluation Criteria	Sr.No.18	The proposed OEM solution/product should have been successfully implemented in least two Scheduled bank (including financial regulators). The reference implementation need not be of the same model, version, or product family as the proposed solution. List of Product which is required to comply with the above clause 1. Anti-Distributed Denial of Services (Anti-DDoS) 2. DNS protection (Internal DNS Security) 3. Web Application Firewall (WAF) 4. DNS Security Services (Internet-Facing DNS Security Services)	We request the Bank to kindly amend the eligibility criterion to consider deployments of the proposed or technically similar must be deployed by the OEM or the Bidder across BFSI organizations, Government/Public Sector organizations, or Scheduled Commercial Banks (SCBs). Further, the reference customer may be a BFSI/ Government/Public Sector organization, or an SCB with at least 500 branches/offices in India. This modification will broaden participation by allowing OEMs with proven large-scale enterprise deployments in highly regulated environments, while ensuring that the solution has demonstrated capability, scalability, and operational maturity. Such an amendment will encourage wider competition without compromising the Bank's technical and operational requirements.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
373	Page No. 105	10.2 Eligibility Evaluation Criteria	Sr.No.19	The proposed OEM solution/product for Privilege Identity/Access Management should have been successfully implemented in at least 2 BFSI in India, out of which at least one (1) BFSI Client should have a deployment covering more than 1,500 privileged users Note: Experience should be during the five-year period preceding the RFP publication date. Even if the installation was completed more than five years ago, it will still qualify, provided the product is currently under maintenance or has been maintained at any time during the five-year period preceding the RFP publication date	We request the Bank to kindly broaden the eligibility criteria to consider deployments of the proposed or technically similar solution by the OEM or the Bidder in BFSI organizations, Government/Public Sector organizations, or Scheduled Commercial Banks (SCBs). Large-scale deployments in these sectors demonstrate comparable capabilities in terms of security, scalability, availability, and operational requirements.	Please be guided by the RFP
374	Page No. 68	Appendix 1A Functinal Sepecification	Sr.No.7	Authoritative DNS services should be ISO 27001:2013 & ISO 27701:2019 compliant	We request the Bank to kindly consider updating the specified ISO certification requirements in line with the latest applicable standards. The requirement for ISO/IEC 27001:2013 may kindly be updated to ISO/IEC 27001:2022, as ISO/IEC 27001:2013 is an older version of the information security management standard and the latest 2022 edition provides the currently applicable framework for Information Security Management Systems (ISMS). Further, ISO/IEC 27701:2019 is specifically focused on Privacy Information Management Systems (PIMS) and is generally applicable to organisations that store, process, or manage personal and privacy-related information or provide PIMS-related solutions. Therefore, making ISO/IEC 27701:2019 mandatory in addition to ISO/IEC 27001 may restrict participation where the organisation's primary scope is information security and the required privacy and data protection controls are otherwise adequately addressed. Accordingly, we request the Department to kindly amend the clause as follows: "The OEM must be certified under ISO/IEC 27001:2022 OR ISO/IEC 27701:2019." This amendment would recognise the latest ISO/IEC 27001 standard while also providing an equivalent compliance option for OEMs holding ISO/IEC 27701:2019 certification, thereby ensuring broader and increased participation without compromising the required information security and privacy controls.	Please refer Addendum 1 for the revised clause.
375	Page No. 3	Appendix 1A doucment, Page no-3	Sr.No.1	Anti- DDoS - System should be Stateless appliances in DC and DR, It should be sized on clean traffic throughput irrespective of mitigation. System should support unlimited number of concurrent sessions.	Kindly specify the required number of concurrent sessions within the proposed licence and appliance capacity. Since every appliance has finite hardware resources and a defined session-handling capacity, the requirement for "unlimited concurrent sessions" may kindly be replaced with a measurable minimum value to enable accurate sizing and fair technical evaluation.	The requirement for supporting an unlimited number of concurrent attack sessions shall be retained, as the volume and nature of concurrent attack sessions during a DDoS event cannot be predicted or prescribed in advance; the proposed stateless solution shall accordingly be capable of sustaining effective and uninterrupted mitigation of large-scale and complex DDoS attacks without session-based limitations.
376	Page No. 39	Appendix 1A doucment, Page no-39	Sr.No.92	WAF - The solution must have bypass segments to ensure that fail open in case of hardware failure	Kindly confirm whether High Availability deployment with automatic failover and software bypass may be accepted as an alternative to dedicated hardware bypass segments, particularly for virtual or reverse-proxy WAF deployments where physical bypass interfaces are not applicable.	Please be guided by the RFP
377	Page No. 68	Appendix 1A doucment, Page no-68	Sr.No.2	DNS - DNS Platform should be purpose-built exclusively to serve DNS traffic to avoid any inter-dependency on other solutions on the provider's platform. DNS Platform to have 1000+ POPs globally with multiple POPs in India as well.	Kindly clarify the technical justification for requiring a minimum of 1,000+ global PoPs. We request that the clause be amended to accept an enterprise DNS platform with geographically distributed PoPs, including multiple PoPs in India, provided it meets the required availability, latency, scalability and security SLAs, irrespective of the absolute PoP count.	Please be guided by the RFP
378	Page No. 68	Appendix 1A doucment, Page no-69	Sr.No.9	DNS - 3) AFSDB AFS Database 7) HINFO System Information 8) LOC Location 12) NSEC3PARAM NSEC3 Parameters 14) RP Responsible Person	As AFSDB, HINFO, LOC, NSEC3PARAM and RP are specialized/legacy DNS record types and are generally not required for the Bank's routine DNS operations, kindly confirm whether these record types may be excluded. Support for all standard DNS record types required for the Bank's actual operational and security use cases shall be provided.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
379	Page No. 69	Appendix 1A doucment, Page no-69	Sr.No.38	DNS - DNS Service Provider OEM must have their own First Party NOC, SOC, and Technical Support Centre (24 x 7 x 365) in India. This is to ensure that DNS Service provider has significant commitment towards India region. Bank may request to visit these centers for verification of support & services centers.	Kindly confirm whether an OEM having its own 24×7×365 Technical Assistance/Support Centre in India, with continuous product monitoring, incident response and escalation capabilities, may be accepted. We request that the mandatory requirement for separate OEM-owned NOC and SOC facilities be relaxed, as these are operational service models and not essential to the technical functionality or support of the DNS solution.	Please be guided by the RFP
380	Page No. 69	Appendix 1A doucment, Page no-69	Sr.No.43	DNS - Pricing for DNS or GSLB Solution must not be dynamic or traffic consumption based e.g. Based on DNS queries or traffic served. There should not be any extra cost to absorb DDoS attack traffic handled by the DNS platform for Bank DNS Zones or GSLB. Pricing should be predictable & Flat based on the number of DNS zones or GSLB configurations as per Bank's requirement.	Kindly confirm whether a fixed-term subscription based on the mutually agreed DNS query capacity, protected domains/zones and GSLB configurations may be accepted, with no additional charges for temporary traffic spikes or DDoS attack traffic within the proposed capacity. Any permanent capacity enhancement beyond the initially agreed sizing may be considered separately.	Please be guided by the RFP
381	136	13 TERMS AND CONDITIONS 13.1 Assignment & Subcontracting		The selected bidder shall not subcontract /JV /Consortium or permit anyone to perform any of the work, service or other performance required under the contract (excluding Proposed OEM personnels).	Considering the extensive and specialized nature of the project scope, we request the Authority to kindly allow participation through a Consortium/JV arrangement of up to two (2) members. This would enable bidders to leverage complementary technical expertise, specialized capabilities, infrastructure, and domain experience while ensuring effective and timely delivery of the project. We further request that the eligibility and technical credentials of the consortium members may be considered collectively, subject to the lead bidder retaining overall responsibility and accountability for the successful execution of the contract. Request: Kindly consider permitting a Consortium/JV of up to two (2) members for participation in the tender.	Please be guided by the RFP
382	100	10.2 Eligibility Evaluation Criteria Sr. No. 2		The bidder should have a minimum average annual turnover of INR 1000 crore in India during the last 3 financial years (i.e. 2022-23, 2023-24 & 2024–25) along with positive net worth.	We request you to amend the clause as; The bidder should have a minimum average annual turnover of INR 250 crore in India during the last 3 financial years (i.e. 2022-23, 2023-24 & 2024–25) along with positive net worth.	Please refer Addendum 1 for the revised clause.
383	158	15.5 Annexure 5: Pre-Qualification Criteria Sr. No.4			In case Consortium/JV participation is permitted, we request the Authority to kindly amend the clause as follows: "The bidder/consortium members collectively should have a minimum average annual turnover of INR 280 crore in India during the last 3 financial years (i.e. 2022-23, 2023-24 & 2024-25), along with positive net worth." Justification: Considering the large and specialized scope of the project, allowing the consortium members to meet the turnover requirement collectively will enable participation of organizations with complementary financial and technical capabilities. This will encourage wider participation and competition while ensuring that the consortium has the required overall financial strength to execute the project successfully.	Please be guided by the RFP. Refer Clause 13.1 (Assignment and Subcontracting), point 1
384	159	15.5 Annexure 5: Pre-Qualification Criteria Sr. No. 8		Bidder must have at least enrolled manpower (on bidder's payroll) of 150 experienced employees skilled in areas of Cyber/IT security.	Kindly amend the clause as; Bidder must have at least enrolled manpower (on bidder's payroll) of 100 experienced employees skilled in areas of Cyber/IT security.	Please refer Addendum 1 for the revised clause.

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
385	158	15.5 Annexure 5: Pre-Qualification Criteria Sr. No.7		Bidder should have supplied, installed and maintained (or under maintenance) at least 10 of the below solutions in any one PSU/PSE/ BFSI/Government Organizations / Regulatory & Statutory body in India: 1. Anti-Distributed Denial of Services (Anti-DDoS) 2. SSL Interception/SSL offloader 3. DNS protection (Internal DNS Security) 4. Web Gateway 5. Zero-Day Attack Protection at Endpoint and network/Anti-APT 6. Zero Trust Network Access (ZTNA)/Remote Access VPN 7. Data Loss Prevention (DLP) 8. Information/Digital Right Management 9. Database Activity Monitoring 10. Mobile SDK 11. Host IPS including Application Change Control (HIPS) 12. Web Application Firewall (WAF) (Mandatory Requirement) 13. Centralized key management solution 14. Certificate Lifecycle management 15. Identity & Access Management Solution 16. Multi Factor Authentication/2FA 17. Privilege Identity/Access Management 18. DNS Security Services (Internet-Facing DNS Security Services)	Bidder should have supplied, installed and maintained (or under maintenance) at least 8 of the below solutions in any one PSU/PSE/ BFSI/ Government Organizations/Regulatory & Statutory body in India: 1. Anti-Distributed Denial of Services (Anti-DDoS) 2. SSL Interception/SSL offloader 3. DNS protection (Internal DNS Security) 4. Web Gateway 5. Zero-Day Attack Protection at Endpoint and network/Anti-APT 6. Zero Trust Network Access (ZTNA)/Remote Access VPN 7. Data Loss Prevention (DLP) 8. Information/Digital Right Management 9. Database Activity Monitoring 10. Mobile SDK 11. Host IPS including Application Change Control (HIPS) 12. Web Application Firewall (WAF) (Mandatory Requirement) 13. Centralized key management solution 14. Certificate Lifecycle management 15. Identity & Access Management Solution 16. Multi Factor Authentication/2FA 17. Privilege Identity/Access Management 18. DNS Security Services (Internet-Facing DNS Security Services)	Please be guided by the RFP
386	158	15.5 Annexure 5: Pre-Qualification Criteria Sr. No.7 Supporting Documents		Copy of Purchase Order/Work Order/ Contract AND In addition to the above, bidder to provide the following: d) Client credential/reference letter specifying the product deployed and the current status/ stage of the project; OR e) Email confirmation from the client specifying the product deployed and the current status/ stage of the project; OR f) Client-signed implementation signoff/ report confirming successful implementation of the solution;	Kindly amend the clause as; Copy of Purchase Order/Work Order/ Contract OR In addition to the above, bidder to provide the following: d) Client credential/reference letter specifying the product deployed and the current status/stage of the project; OR e) Email confirmation from the client specifying the product deployed and the current status/stage of the project; OR f) Client-signed implementation signoff/ report confirming successful implementation of the solution;	Please be guided by the RFP
387	TECHNICAL – 7.1 / 7.3.1	7.3.1.1 Anti-DDoS		Anti-DDoS is required at DC & DR for network and application layer attacks.	Please provide the expected protected internet bandwidth, peak traffic, committed clean bandwidth and maximum attack traffic volume to enable uniform Anti-DDoS sizing.	The bidder shall undertake & proposed sizing based on the RFP requirements,
388	TECHNICAL – 7.3.1	7.3.1.1 Anti-DDoS		Protection includes volumetric and application-layer attacks.	Please clarify whether on-premises mitigation only is required or whether an upstream/cloud scrubbing service may be proposed as part of the architecture.	Please refer Functional Requirement, Anti-Ddos, Point 70
389	TECHNICAL – 7.3.1	7.3.1.1 Anti-DDoS		Protection includes UDP, ICMP, SYN, Smurf, HTTP Flood, zero-day and TCP exhaustion attacks.	Please confirm whether both IPv4 and IPv6 traffic must be protected for all internet-facing services.	Please refer Functional Requirement, Anti-Ddos, Point 10 and 13.
390	TECHNICAL – 7.3.1	7.3.1.1 Anti-DDoS		Detailed attack detection, mitigation and geographic reporting is required.	Please clarify the minimum retention period for attack logs, mitigation events, dashboards and reports.	Please refer Annexure 21 for retention period
391	TECHNICAL – 7.3.1	7.3.1.2 SSL Orchestrator		SSL Orchestrator and PCAP are required for deep inspection.	Please provide SSL/TLS throughput, concurrent connections, new connections per second and expected encrypted-traffic percentage for sizing.	Bidder and OEM shall undertake sizing based on the requirements specified in the RFP and shall factor adequate capacity, performance headroom and scalability.
392	TECHNICAL – 7.3.1	7.3.1.2 SSL Orchestrator		Packet capture is to be supported through port mirroring.	Please provide the existing SPAN/TAP/packet broker capabilities and expected interface speeds to determine placement.	Bidder and OEM shall undertake sizing based on the requirements specified in the RFP and shall factor adequate capacity, performance headroom and scalability.
393	TECHNICAL – 7.3.1	7.3.1.2 SSL Orchestrator		Service chaining with IPS, WAF, NGFW and other tools is required.	Please provide the complete inline-tool chain and traffic steering flows expected at DC and DR.	The bidder shall design and propose the end-to-end service chaining architecture in accordance with the RFP requirements and Bank's security architecture. Detailed internal network topology and traffic-flow information, wherever security-sensitive, shall be shared only with the selected bidder on a need-to-know basis during implementation.
394	TECHNICAL – 7.3.1	7.3.1.4 Web Gateway		Hybrid cloud/on-premises SWG deployment is required.	Please provide the number of users/endpoints, internet bandwidth and expected concurrent web sessions for sizing.	Please be guided by the RFP, Refer Annexure 21 for details
395	TECHNICAL – 7.3.1	7.3.1.4 Web Gateway		Reverse proxy and terminal-services integration are required.	Please provide the number of applications/domains requiring reverse proxy and their protocols.	Please be guided by the RFP, Refer Annexure 21 for details
396	TECHNICAL – 7.3.1	7.3.1.5 Zero-Day Protection		Zero-Day protection must cover network and endpoint layers.	Please provide the endpoint/server count and protected network throughput for initial sizing.	Please refer Addendum 1 for the revised clause. Please be guided by the RFP, Refer Annexure 21 for details

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
397	TECHNICAL – 7.3.1	7.3.1.5 Zero-Day Protection		Integration is required with SIEM, SOAR, UEBA, XDR, SBDL, Firewall and TIP.	Please confirm the OEM/product/version of each integration and whether API/connectors are already licensed.	Bank is in process of procuring the tools and services, details of the OEMs, version, edition etc. will be shared with the successful bidder
398	TECHNICAL – 7.3.1	7.3.1.5 Zero-Day Protection		24x7 monitoring and malware scanning for critical websites is required.	Please provide the number of critical websites and their approximate transaction/traffic volumes.	Please be guided by the RFP, Refer Annexure 21 for details
399	TECHNICAL – 7.3.1	7.3.1.6 ZTNA		ZTNA must integrate with patch management, NAC, ITSM and identity systems.	Please confirm which integrations are mandatory for Go-Live and which may be phased post-Go-Live.	All required integrations with the proposed solution shall be planned and completed in a manner that ensures their readiness prior to commencement of the UAT phase.
400	TECHNICAL – 7.3.1	7.3.1.6 ZTNA		AI/ML discovery of internal applications is required.	Please provide the approximate number of internal applications and application protocols in scope.	Bidder shall consider the endpoint/server and network sizing specified in the RFP
401	TECHNICAL – 7.3.2	7.3.2.1 CASB		CASB must cover SaaS, PaaS and IaaS, sanctioned and unsanctioned applications.	Please provide the approximate number of cloud applications/services and users for initial CASB sizing.	Please refer Annexure 21
402	TECHNICAL – 7.3.2	7.3.2.1 CASB		CASB data plane is required to remain on-premises at DC & DR.	Please clarify which management, analytics or threat-intelligence functions may use OEM cloud services.	The CASB data plane shall comply with the RFP requirement for deployment at the Bank's DC/DR environment. Any OEM cloud-based management, analytics, threat intelligence or other component shall be clearly identified, and shall be subject to the Bank's cloud, data-security, privacy and regulatory requirements. No Bank data shall be transmitted outside the approved environment without Bank approval.
403	TECHNICAL – 7.3.2	7.3.2.1 CASB		Custom dashboards and compliance reports are required.	Please provide the expected mandatory reports, frequency and retention period.	The bidder shall provide all dashboards and reports specifically required under the RFP, along with reports required for management, operational, audit, security and regulatory purposes. Detailed formats shall be finalized during implementation in consultation with the Bank.
404	TECHNICAL – 7.3.2	7.3.2.2 DLP		DLP must cover endpoint, email, network, USB, web and SaaS.	Please provide endpoint count, email platform/version, browser mix and supported SaaS applications for sizing.	Bidder shall size the DLP solution based on the RFP quantities
405	TECHNICAL – 7.3.2	7.3.2.2 DLP		Data classification matrix and policy mapping are required.	Please clarify whether the Bank will provide the authoritative data-classification policy or the bidder must create the baseline.	The Bank shall provide its applicable policies/guidelines as appropriate. The bidder shall configure and map the solution to the Bank's approved policies and shall support identification of gaps and recommendations.
406	TECHNICAL – 7.3.2	7.3.2.2 DLP		Policy effectiveness, false positives and rule tuning must be reported.	Please clarify the expected number of DLP policies/use cases to be configured during implementation.	The bidder shall configure the policies/use cases required to meet the RFP's functional and security requirements. The bidder shall factor adequate implementation and tuning effort
407	TECHNICAL – 7.3.3	7.3.3.1 DAM		DAM must monitor local, application and remote database access.	Please provide the database platform/version inventory, number of instances and approximate transaction rates.	Detailed environment information required for implementation shall be provided to the selected bidder on a need-to-know basis.
408	TECHNICAL – 7.3.4	7.3.4.1 HIPS		Role-based dashboard views are required.	Please confirm whether dashboard access must integrate with the Bank's existing IAM and provide the expected number of roles/users.	Role-based access control shall be supported. Integration with the Bank's existing and newly proposed IAM/authentication infrastructure shall be provided where required by the RFP. The bidder shall factor all required components/licenses/connectors necessary to meet the requirement.
409	TECHNICAL – 7.3.4	7.3.4.2 WAF		WAF must protect applications and APIs against OWASP Top 10 and emerging attacks.	Please provide application count, domains, API count, peak requests/sec and throughput for sizing.	Detailed environment information required for implementation shall be provided to the selected bidder on a need-to-know basis.
410	TECHNICAL – 7.3.4	7.3.4.2 WAF		High availability is required for critical applications.	Please confirm the target WAF HA mode and DC/DR topology.	The proposed WAF solution shall comply with the HA and DC/DR architecture specified in the RFP. The solution shall support N+N Active-Active deployment at both the Primary Data Centre (DC) and Disaster Recovery (DR) site, with the required capacity and resilience available at each site.
411	TECHNICAL – 7.3.4	7.3.4.2 WAF		Minimal performance impact is required.	Please specify quantitative latency/throughput acceptance criteria for performance testing.	The bidder shall meet the performance requirements specified in the RFP. Performance shall be validated during UAT/performance testing, bidder is required showcase the performance in the bank's environment.
412	TECHNICAL – 7.3.4	7.3.4.3 Centralized KMS		KMS must manage generation, distribution, rotation, archival and revocation.	Please provide the approximate number of cryptographic keys, integrations and target systems.	Bidder shall size the KMS based on the RFP scope with adequate scalability. Detailed integration information shall be provided to the selected bidder during implementation as required.
413	TECHNICAL – 7.3.4	7.3.4.3 Centralized KMS		KMIP and segregation-of-duties controls are required.	Please provide the list of existing applications/appliances that require KMIP integration.	The bidder shall support standards-based KMIP integration wherever required. Detailed application/infrastructure information shall be shared with the selected bidder during implementation on a need-to-know basis.
414	TECHNICAL – 7.3.4	7.3.4.5 S-BOM/C-BOM/AI-BOM/Q-BOM		BOM solution covers applications, APIs, OS, containers, Kubernetes, cloud workloads, AI models and repositories.	Please provide approximate counts of applications, repositories, containers, Kubernetes clusters and AI models in scope.	Bidder shall size the proposed BOM solution based on the scope specified in the RFP
415	TECHNICAL – 7.3.4	7.3.4.5 S-BOM/C-BOM/AI-BOM/Q-BOM		The solution must support software supply-chain, crypto, AI and quantum-risk governance.	Please confirm the mandatory BOM formats/standards for machine-readable submission and exchange.	The solution shall support industry-standard, machine-readable BOM formats and standards applicable to the respective BOM type, including relevant SBOM/CBOM/AI-BOM/Q-BOM requirements.
416	TECHNICAL – 7.3.4	7.3.4.5 S-BOM/C-BOM/AI-BOM/Q-BOM		Vulnerability management and crypto-agility are required.	Please identify the Bank's existing vulnerability-management platform and required integration method.	The bidder shall provide standards-based integration with the Bank's vulnerability-management ecosystem as required.
417	TECHNICAL – 7.3.5	7.3.5.3 AI Security		AI security must cover GenAI, LLMs, AI agents and AI applications/APIs.	Please provide the estimated number of AI applications, LLM endpoints, agents and APIs in initial scope.	Bidder shall size the AI security solution based on the RFP scope
418	TECHNICAL – Security Incident/Data Breach	Cyber Security Incident / Data Breach		Incident notification is required within six hours of awareness.	Please clarify whether the six-hour clock begins at OEM detection, bidder detection, or incident confirmation.	The six-hour incident notification timeline shall commence from the time the bidder/OEM becomes aware of, detects, or reasonably determines that a security incident has occurred within the scope of its responsibility

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
419	TECHNICAL – Security Incident/Data Breach	Cyber Security Incident / Data Breach		Logs, forensic evidence and system images must be preserved.	Please specify the minimum forensic/evidence retention period and whether storage is bidder-provided.	Evidence shall be preserved in accordance with Bank policy, applicable regulatory requirements and the retention requirements specified in the RFP. The bidder shall factor the required storage/capacity and operational capability
420	TECHNICAL – 7.5.21	Customization		Customization, enhancements, workflows and dashboards are to be provided at no cost.	Please define what constitutes a major customization requiring separate OEM engineering services.	Any customization, enhancement, workflow, parser, connector, dashboard, playbook or integration required to meet the specified RFP functionality or Bank-approved use cases (defined by the bank in the SRS) within the contracted scope shall be included without additional cost. A separately chargeable CR shall apply only where the requirement constitutes materially new functionality, a new product/module/license or scope outside the RFP, subject to Bank approval.
421	TECHNICAL – 7.5.22	SBOM/CBOM/AI BOM		OEMs must maintain BOM dependencies up to the last level.	Please confirm update frequency and acceptable delivery formats for detailed/private BOMs.	The bidder/OEM shall maintain BOM/dependency information on a continuous or OEM-supported update basis
422	TECHNICAL – 7.5.1	Migration		Migration includes telemetry, logs, rules, parsers, integrations, dashboards and user profiles.	Please provide solution-wise current data volumes, log retention, rule/use-case counts, dashboards and integration counts.	The bidder shall undertake a detailed discovery and migration assessment during the transition phase. Migration shall cover the in-scope data/configurations made available by the Bank
423	TECHNICAL – 7.5.1	Migration Handover		Incumbent must hand over data dictionary, patches, software, manuals, certificates and reports.	Please confirm the Bank will facilitate a formal incumbent handover with required access and documentation.	The Bank shall facilitate transition and handover activities to the extent reasonably required. However, the bidder shall be responsible for planning, coordinating and completing the transition/migration activities within the approved implementation plan
424	TECHNICAL – 7.5.1	Migration		Parallel run and cutover are required.	Please clarify the expected parallel-run duration for each solution and support expectations during dual operation.	The duration of parallel run shall be finalized in the approved implementation and transition plan based on solution criticality, migration complexity and operational readiness.
425	TECHNICAL – 7.5.1	Incumbent Support		Bidder may have to operate incumbent solutions if implementation is delayed.	Please clarify the maximum period of incumbent-operation support that can be assigned to the bidder.	The bidder shall provide takeover/operation support for the incumbent solution for the period directed by the Bank until successful Go-Live of the corresponding replacement solution, subject to the terms of the RFP/contract Bank existing contract with the incumbant vendor is till June 2027
426	TECHNICAL – 7.13	Backup Infrastructure		Bidder/OEM must size backup infrastructure with ransomware protection.	Please provide current backup architecture, protected data volume, retention, daily change rate and replication requirements.	Bidder/OEM shall design and size the backup infrastructure based on the RFP's storage, retention, resilience and ransomware-protection requirements and applicable Bank policies. The bidder shall factor adequate capacity and scalability as sought in the RFP.
427	NON-TECHNICAL – Eligibility	10.2 Eligibility – Clause 21		Annexure 18 OEM declaration is required for every solution.	May a single consolidated OEM declaration cover multiple products from the same OEM where make/model/version are separately identified in Annexure 19?	For multiple solutions from the same OEM, a single declaration may be provided by the OEM with the name of each product/ solution and the client and other details for each solution as sought in the RFP should be explicitly mentioned.
428	NON-TECHNICAL – Commercial Evaluation	10.4 Commercial Evaluation		Bank may normalize bids and recalculate evaluated TCO where sizing is inadequate.	Please clarify the normalization methodology and whether the loaded augmentation cost affects technical qualification or only TCO.	Please be guided by the RFP
429	NON-TECHNICAL – Commercial	Sizing Responsibility		Bidder remains solely responsible for sizing adequacy and future augmentation.	May the Bank provide approved baseline volumetrics and treat material growth beyond the baseline as additional scope/change request?	Refer Annexure 21 of the RFP for Sizing and Volumetrics. Bidder is solely responsible for sizing all infrastructure and associated software/solution components, in consultation with respective infrastructure and solution/service OEMs, including projected growth over the contract period.
430	NON-TECHNICAL – Payment	11 Payment Terms		No advance payment; milestone-based payment follows delivery/UAT/Go-Live.	kindly ammend this clouse and consider OTC will be pay advanced along with purchase Order.	Please be guided by the RFP
431	NON-TECHNICAL – Payment	11.1 Product Cost		Product license cost is paid 50% on delivery, 20% on UAT and 30% on Go-Live.	kindly ammend this clouse and consider Product license cost is paid 50% on Advance, 20% on UAT and 30% on Go-Live.	Please be guided by the RFP
432	NON-TECHNICAL – Payment	11.1 Implementation Cost		Implementation payment includes 10% within three months of Go-Live.	Please define the acceptance conditions for releasing the final implementation payment.	The 10% payment shall be released within three months of successful Go-Live of the respective product, subject to satisfactory performance and acceptance by the Bank and submission of the applicable invoice and supporting documents as per the RFP
433	NON-TECHNICAL – Payment	11.2 OEM Services		OEM services are payable quarterly in arrears after service and sign-off.	Please clarify the expected number of annual architecture assessments and review sessions to be priced.	Please be guided by the RFP
434	NON-TECHNICAL – SLA	12.1 Critical Component		Critical components must be repaired/replaced/provided standby within four hours.	please concider one working day instead of Critical components must be repaired/replaced/provided standby within four hours.	Please be guided by the RFP
435	NON-TECHNICAL – SLA	Manpower Availability		Mandatory resources must be maintained at 100% availability.	May approved leave, training, statutory holidays and approved backup substitutions be excluded from the shortfall calculation?	Please be guided by the RFP
436	NON-TECHNICAL – Resources	7.11 Resource Requirement		Minimum onsite resources must be maintained and additional resources may be required.	Please confirm whether resources deployed temporarily for Bank-requested additional scope will be billable at BoM rates.	Manpower augmentation required to meet the bidder's contractual obligations/SLA shall be at no additional cost.

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
437	NON-TECHNICAL – Resources	Minimum Resource Count Deployment		L1/L2/L3/domain resources are prescribed by shift.	Please clarify whether shared/cross-skilled resources can be used across all three shifts if SLA coverage is maintained.	Please be guided by the RFP, resource requirement mentioned is mininmal requirement
438	NON-TECHNICAL – DR Drill	7.12.1 Continual Improvement		Quarterly DR drill and exact-replica DC/DR expectation are stated.	Please clarify whether exact replica includes identical capacity/licensing across DC and DR or equivalent failover capacity is acceptable.	The DR environment shall be a 100% replica of the DC environment in terms of the proposed solution components, architecture, sizing/capacity, HA configuration, functionality, and resilience. The same solution capabilities and required capacity available at the DC shall be provisioned at the DR site
439	NON-TECHNICAL – Commercial	10.4 Commercial Evaluation		Bank may add other relevant evaluation criteria at its discretion.	Please request that any additional evaluation criterion be issued to all technically qualified bidders through a formal corrigendum/addendum before final bid evaluation.	Please be guided by the RFP Refer Clause 6.18, Ammendments to the RFP Contents for the same
440	15		5 PROJECT OBJECTIVE	The quoted prices shall remain valid for all orders placed during the entire contract period and shall be binding upon the selected bidder	In the current senario no OEM providing validity beyond 30 days. Hence, please remove the clause. We reuqesst you to modify this clause - The quoted prices shall remain valid for all orders placed 30 days during the entire contract period and shall be binding upon the selected bidder	Please be guided by the RFP
441	69		7.10 Solution/Appliance Warranty, ATS and AMC	3. Warranty period for hardware/appliance and software support shall commence from the date of Go-live of the respective solution.	Please confirm the warranty start date for Software Licenses.	Refer Section 7.9 (Solution/Appliance Warranty, ATS and AMC). Warranty period for both hardware/appliance and software support/licenses commences from the date of Go-live of the respective solution.
442	97		8 CONTRACT PERIOD	End of Sales / End of support: The bidder must ensure that any equipment (hardware/software) supplied as part of this RFP should not have either reached or announced end of sales as on the date of such supply or end of support for at least duration of the contract (including the period of 2-year extension).	Since, OEM will not confirm the End of sale/support for more than 5 years. Please change the clasue as - End of Sales / End of support: The bidder must ensure that any equipment (hardware/software) supplied as part of this RFP should not have either reached or announced end of sales as on the date of such supply or end of support for at least duration of the contract.	Please be guided by the RFP
443	100		10.2 Eligibility Evaluation Criteria - Point#5	The bidder should be an authorized representative/ partner/ reseller of each of the proposed OEMs in India. MAF should be submitted from the following solution OEMs	It is observed during multiple bid submission previously with Bank. OEM does not provide the MAF as per the RFP format. Since, most of the OEM's document approved by their Legal team (outside India) and their Legal not approve the documents as per RFP format. Hence, request you to allow the MAF and other OEM Undertaking as per OEM's Legal apporved format which covers the RFP T&Cs and compliance.	The MAF and other OEM Undertakings must, at a minimum, cover the scope/content prescribed in the RFP for the said document. OEMs may submit these on their own letterhead/format, provided all mandated content and confirmations specified in the RFP are covered. Bank reserves the right to seek clarification or reject non-compliant submissions.
444	115	11 PAYMENT TERMS	11.1 Product (Software) Cost - Product License Cost	On successful delivery of the licenses which would be considered delivered once the software (with OOTB features) is made available for view and review of the bank on the proposed hardware. - 50% The Bidder is required to submit the required to submit the following: • Delivery proof • OOTB Installation Proof • Invoice of the Product	On successful delivery of the licenses which would be considered delivered once the software (with OOTB features) is made available for view and review of the bank on the proposed hardware. - 50% The Bidder is required to submit the required to submit the following: • Delivery proof • OOTB Installation Proof • Invoice of the Product	Please be guided by the RFP
445	115	11 PAYMENT TERMS	11.1 Product (Software) Cost - Product License Cost	On successful UAT Signoff of the respective product - 20% On successful Go-live of the respective product - 30%	On successful UAT Signoff of the respective product - 30% On successful Go-live of the respective product - 20%	Please be guided by the RFP
446	117	11 PAYMENT TERMS	11.3 Hardware Cost - Appliance Cost	On successful Delivery of the Appliance which would be considered delivered once the solution (with OOTB features) is made available for view and review of the bank. - 50% The Bidder is required to submit the required to submit the following: • Delivery proof • OOTB Installation Proof • Invoice of the Product	On successful Delivery of the Appliance which would be considered delivered once the solution (with OOTB features) is made available for view and review of the bank. - 50% The Bidder is required to submit the required to submit the following: • Delivery proof • OOTB Installation Proof • Invoice of the Product	Please be guided by the RFP
447	117	11 PAYMENT TERMS	11.3 Hardware Cost - Hardware Cost (Other than Appliances)	Delivery (power on) of hardware and submission of invoice with Proof of Delivery and other documents of the hardware supplied. - 70% Bank may at its discretion verify the details before releasing the payment (This verification, if required, shall be completed within 1 month of delivery of the hardware on the bank's premises).	Delivery (power on) of hardware and submission of invoice with Proof of Delivery and other documents of the hardware supplied. - 70% Bank may at its discretion verify the details before releasing the payment (This verification, if required, shall be completed within 1 month of delivery of the hardware on the bank's premises).	Please be guided by the RFP
448	150	15 ANNEXURES	15.1 Annexure 1: Submission Checklist (on bidder's letterhead)	Format for Performance guarantee Technical Presentation Submission	~~Format for Performance guarantee~~ ~~Technical Presentation Submission (Technical presentation will be prepared after bid submission)~~	Please be guided by the RFP. Technical presentation shall be part of the submitted bid
449		15 ANNEXURES	15.12 Annexure 12: Undertaking of Authenticity (on bidder's letterhead)	15.12 Annexure 12: Undertaking of Authenticity (on bidder's letterhead)	15.12 Annexure 12: Undertaking of Authenticity (on bidder's & OEM) letterhead. Since the undertaking has the details of product hence the same undertaking required by OEM also basis on the same Bidder can confirm.	Please be guided by the RFP. Bidder to submit the undertaking on their letterhead as per the RFP format
450	120		12.1 Service Level Agreement	19. Total penalties due Service level and liquidated damages shall not exceed 10% of the Total contract value.	19. Total penalties due Service level and liquidated damages shall not exceed 10% 5% of the Total contract quarterly value.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
451	136		13.1 Assignment & Subcontracting	The selected bidder shall not subcontract/JV/Consortium or permit anyone to perform any of the work, service or other performance required under the contract (excluding Proposed OEM personnels).	The selected bidder shall not subcontract/JV/Consortium or permit anyone to perform any of the work, service or other performance required under the contract (excluding Proposed OEM personnels) without the prior written consent of Bank, which shall not be unreasonably withheld or delayed..	Please be guided by the RFP
452	140		13.13 Indemnity	The bidder agrees to indemnify and keep indemnified the Bank against all losses, damages, costs, charges and expenses incurred or suffered by the Bank due to or on account of any breach of the terms and conditions contained in this RFP or Service Level Agreement to be executed. The Bidder shall indemnify, defend and hold harmless the Bank, its directors, officers, employees and representatives against all losses, damages, liabilities, claims, demands, actions, proceedings, penalties, costs and expenses (including reasonable legal expenses, forensic investigation costs, remediation costs and costs incurred in responding to regulatory/customer claims) arising out of or relating to: (a) breach of the Contract/RFP/SLA; (b) negligence, gross negligence, fraud, willful misconduct or omission of the Bidder/OEM/subcontractor; (c) breach of confidentiality or data protection obligations; (d) cyber security incident, data breach, unauthorised access, loss or disclosure of Bank/customer data attributable to the Bidder/OEM/subcontractor; (g) third-party/customer claims arising from the acts or omissions of the Bidder/OEM/subcontractor; and (h) any loss suffered by the Bank in consequence of failure of the Bidder to perform the services in accordance with the Contract.	The bidder agrees to indemnify and keep indemnified the Bank against all losses, damages, costs, charges and expenses incurred or suffered by the Bank due to or on account of any breach of the terms and conditions contained in this RFP or Service Level Agreement to be executed. The Bidder shall indemnify, defend and hold harmless the Bank, its directors, officers, employees and representatives against all losses, damages, liabilities, claims, demands, actions, proceedings, penalties, costs and expenses (including reasonable legal expenses, forensic investigation costs, remediation costs and costs incurred in responding to regulatory/customer claims) arising out of or relating to third party: (a) breach of the Contract/RFP/SLA; (b) negligence, gross negligence, fraud, willful misconduct or omission of the Bidder/OEM/subcontractor; (c) breach of confidentiality or data protection obligations; (d) cyber security incident, data breach, unauthorised access, loss or disclosure of Bank/customer data attributable to the Bidder/OEM/subcontractor; (g) third-party/customer claims arising from the acts or omissions of the Bidder/OEM/subcontractor; and (h) any loss suffered by the Bank in consequence of failure of the Bidder to perform the services in accordance with the Contract.	Please be guided by the RFP
453	142		13.19 Liquidated Damages	If the bidder fails to deliver any or all of the products and/or systems and/or services solutions within the time period(s) specified in the Delivery Schedule or installation, the Bank shall, without prejudice to its other remedies under the Contract, deduct from the Contract Price, as liquidated damages, a sum equivalent to 0.5 percent per week or part thereof of Contract Price subject to maximum deduction of 10% of the total contract value, until actual delivery, installation or performance as per related clauses mentioned in RFP.	If the bidder fails to deliver any or all of the products and/or systems and/or services solutions within the time period(s) specified in the Delivery Schedule or installation, the Bank shall, without prejudice to its other remedies under the Contract, deduct from the Contract Price, as liquidated damages, a sum equivalent to 0.5 percent per week or part thereof of Contract Price subject to maximum deduction of 10% 5% of the total contract milestone value , until actual delivery, installation or performance as per related clauses mentioned in RFP.	Please be guided by the RFP
454	143		13.21 Limitation of Liability	The aggregate liability of bidder in connection with this Agreement, in respect of any claims, losses, costs or damages arising out of or in connection with this RFP/Agreement shall not exceed the total Project Cost. Under no circumstances shall either Party be liable for any indirect, consequential or incidental losses, damages or claims including loss of profit, loss of business or revenue. The limitations set forth herein shall not apply with respect to: 1. claims that are the subject of indemnification pursuant to infringement of third-party Intellectual Property Right, 2. damage(s) occasioned by the Gross Negligence or Willful Misconduct of Service Provider, 3. damage(s) occasioned by Service Provider for breach of Confidentiality Obligations, 4. Regulatory or statutory fines imposed by a government or Regulatory agency for non compliance of statutory or regulatory guidelines applicable to the Bank, provided such guidelines were brought to the notice of Service Provider.	The aggregate liability of bidder in connection with this Agreement, in respect of any claims, losses, costs or damages arising out of or in connection with this RFP/Agreement shall not exceed the total annual Project Cost. Under no circumstances shall either Party be liable for any indirect, consequential or incidental losses, damages or claims including loss of profit, loss of business or revenue. The limitations set forth herein shall not apply with respect to: 1. claims that are the subject of indemnification pursuant to infringement of third-party Intellectual Property Right, 2. damage(s) occasioned by the Gross Negligence or Willful Misconduct of Service Provider, 3. damage(s) occasioned by Service Provider for breach of Confidentiality Obligations, 4. Regulatory or statutory fines imposed by a government or Regulatory agency for non compliance of statutory or regulatory guidelines applicable to the Bank, provided such guidelines were brought to the notice of Service Provider. Notwithstanding the foregoing, under no circumstances shall either Party be liable for any indirect, consequential, or incidental loss, damage, or claim, including any loss of profit, business, or revenue	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
455	144		13.22 Order Cancellation	The Bank reserves its right to cancel the entire unexecuted part of the Purchase Order at any time on its convenience without assigning any reason/s whatsoever by giving 'one 'month notice to the other party. Notwithstanding the foregoing, the Bank shall be entitled to terminate the Contract, in whole or in part, with immediate effect and without any cure period where:	The Bank reserves its right to cancel the entire unexecuted part of the Purchase Order at any time on its convenience without assigning any reason/s whatsoever by giving 'one Three' month notice to the other party. Notwithstanding the foregoing, the Bank shall be entitled to terminate the Contract, in whole or in part, with 1 month prior written notice to Bank immediate effect and without any cure period where:	Please be guided by the RFP
456	3	Functional Specs-Anti DDOS	2	System should have 5 Gbps of clean/legitimate throughput which can scale upto 10 Gbps on the same H/w. System should support more then 20 MPPS. System should be factored on clean/legitimate license throughput.	Change request : System should have 5 Gbps of clean/legitimate throughput which can scale upto 10 Gbps on the same H/w. System should support more then 45 MPPS. System should be factored on clean/legitimate license throughput. Justification : As per best practices for anti DDoS solution, we suggest to size the solution for handling 45 MPPS, to handle large atttacks	Please be guided by the RFP
457	3	Functional Specs-Anti DDOS	3	System should have 8x10 G ports with fail open support without any external fail open kit. All the interfaces including fiber should support fail open.	Change request : System should have 12x10 G ports with fail open support without any external fail open kit. All the interfaces including fiber should support fail open. Justification : Due to multi homing enviorment and to support multiple ISP's, (4 links for 3 ISP's = 12 Ports).	Please be guided by the RFP
458	3	Functional Specs-Anti DDOS	12	Inbuilt mechanism to inspect traffic with external threat feed. System should support minimum 2 million IoC's for both inbound and outbound blocking.	Change Request : Inbuilt mechanism to inspect traffic with external threat feed. System should support minimum 5 million IoC's for both inbound and outbound blocking. (3 Million IoC as Inbuilt and 2 Million from integartion with third party intelligence platform on STIX / TAXI without any REST API) Justification : Since due to growing number of malicious IP's and DDoS launchpad we request to increase support up to 5 Million IoC's.	Please be guided by the RFP
459	3	Functional Specs-Anti DDOS	21	Mitigation mechanism to protecting against zero-day DoS and DDoS attacks without manual intervention. Automatic Real time signature generation	Change Request: "Mitigation mechanism to protecting against zero-day DoS and DDoS attacks without manual intervention. Automatic Real time signature OR countermeasure generation in real-time ." Justification: Signatures is FCAP expression which is limited to FCAP example deny protocol udp port 443, which only limited to L3 and L4, while real time countermeasure can mitigate up to L7	Please refer Addendum 1 for the revised clause.
460	4	Functional Specs-Anti DDOS	44	Able to detect and protect from Zero-Day Network DDoS/DDoS flood attacks on the basis of behavioral DDoS attacks/challenge response mechanism or by an automatically created signature / countermeasure within a minute and must be mentioned in data sheet. The proposed device should also support inbuilt Signatures apart from custom Signatures from Day 1.	Change Request: Able to detect and protect from Zero-Day Network DDoS/DDoS flood attacks on the basis of behavioral DDoS attacks/challenge response mechanism or by an automatically created signature / countermeasure within a minute. The proposed device should also support inbuilt Signatures apart from custom Signatures OR reputation feeds from Day 1.	Please refer Addendum 1 for the revised clause.
461	5	Functional Specs-Anti DDOS	70	The proposed solution shall support on-premises appliance-based, cloud-based/ service-provider-hosted (scrubbing center), or hybrid architectures combining on-premises and cloud-based mitigation, as applicable to the Bank's deployment requirements.	Clarification required : We understand the Hybird solution of On-Prim Appliance and Cloud Signaling to Upstream ISP fulfills the requirement (refer to Clause #46)	Please be guided by the RFP
462	32, 57	7.1 Note 6 and 7.5.4.12	Sizing shortfall	Bidder must absorb all sizing shortfalls without additional cost.	Please confirm that augmentation at bidder cost applies only when measured workload remains within the Bank-published Day-1 quantities, scalability quantities, retention and SLA parameters. Any increase beyond those published parameters shall be ordered at the quoted unit rates.	The bidder is responsible for sizing the proposed solution to meet the complete RFP requirements, including applicable performance, availability, growth, retention and SLA requirements. The bidder shall not claim additional cost merely due to inadequate sizing of its proposed solution.
463	207-208	Annexure 21	DNS/DHCP/IPAM	DHCP/IPAM placement refers to “MZ”, while recursive DNS is stated to be in DMZ.	Please clarify whether “MZ” means the internal zone, management zone or DMZ, and provide the required node count and exact placement for DHCP, IPAM, authoritative and recursive DNS at DC and DR.	MZ refers to the Militarized Zone, which is an internal network zone with no direct Internet access. DMZ refers to the De-Militarized Zone, which is the designated network segment for systems requiring controlled external connectivity. The placement of DHCP, IPAM, authoritative DNS and recursive DNS shall be as per the Bank's defined & existing network architecture and security zoning requirements. The bidder shall consider the applicable DC and DR deployment requirements, including the required node count and HA configuration, as specified in the RFP
464	40, 209	7.3.2.1 and Annexure 21	CASB	RFP requires visibility across SaaS/PaaS/IaaS with on-premises data plane, but only 50 users scalable to 100 are stated.	Please confirm that CASB licensing is required for 50 users on Day 1, scalable to 100 users, and identify the specific SaaS tenants, IaaS/PaaS accounts and inline/API modes to be covered within this quantity.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
465	41, 209	7.3.2 DRM and Annexure 21	DRM licensing	Annexure 21 states 200 admin/policy creator licences and any number of users may apply policies.	Please confirm whether the 200 DRM licences are only for policy creators/administrators and whether document recipients, including external users, are licence-free. If not, provide the Day-1 recipient licence quantity.	The Bank has specifically mentioned a requirement for 200 Administrator Licenses. Accordingly, the proposed solution should provide 200 Licenses for users responsible for administration, policy creation, and rule management.
466	42, 206, 209-210	7.3.3.1 and Annexure 21	DAM	Current inventory lists 300 databases and Annexure 21 states 150 application databases at DC and 150 at DR.	Please confirm whether the stated 150 databases at DC and 150 at DR represent 150 production databases with DR replicas or 300 separately licensed database instances.	Please be guided by the RFP
467	48-49, 211	PIM and Annexure 21	PIM/PAM	750 users and 3,000 services are stated, while eligibility requires a 1,500 privileged-user reference.	Please confirm whether PIM licences required on Day 1 are 750 privileged users and 3,000 service accounts, with only technical scalability to 1,500 users and 4,500 service accounts, or whether the scalable quantities must also be licensed from Day 1.	Please be guided by the RFP
468	49-50, 211	DNS Security Services	Internet-facing DNS security	Scope permits cloud and on-premises DNS Security for 20 domains.	Please confirm whether bidders must quote both cloud-based and on-premises DNS Security Services concurrently, or may propose either one deployment model meeting the RFP. This directly changes BoM and recurring subscription cost.	Please be guided by the RFP
469	50, 212	AI Security and Annexure 21	Unlimited AI usage	The RFP requires unlimited models, users, prompts, API calls, sessions and policies for 12,000 business users.	Annexure 21 specifies unlimited AI models, users, prompts, API calls, sessions and policies. Please provide a billable Day-1 sizing baseline for peak API requests per second, concurrent sessions and monthly prompt/API volume, or confirm that the quoted enterprise licence must contractually include unlimited consumption without overage charges.	Please be guided by the RFP. Bidder to right size as per the requirements and terms specified in the RFP
470	51-57	7.5 and 7.5.4	Unlimited integrations/customization	All future connectors, parsers, APIs, workflows, playbooks, dashboards and enhancements are included without additional cost.	Please provide the fixed Day-1 integration list for each proposed solution. Any integration with a product introduced by the Bank after the approved FRSM/SRS should be procured through change control unless it uses an already included standard connector and requires no additional licence.	The bidder shall provide the integrations, parsers, connectors, workflows and enhancements required within the contracted scope, Exact details of integration shall be discussed during the SRS stage, and for the systems covered by the RFP at no additional cost.
471	52-55, 205	7.5.1 and Annexure 21.2	Migration	All historical logs, telemetry, rules, policies and customizations must be migrated from the existing solutions.	Please provide, for each incumbent solution, the data/configuration quantity to be migrated and the supported export method. Migration responsibility should be limited to data and configuration made available by the Bank/incumbent in a technically readable and OEM-supported format.	The bidder shall undertake migration of the in-scope data/configurations made available by the Bank/incumbent. The bidder shall conduct the necessary assessment and provide a migration plan. Limitations attributable solely to unavailable, corrupted or unsupported source data shall be documented and mutually disccused & agreed
472	54-55, 94	7.5.1 and 7.14.2	Existing-solution takeover	The bidder must take over existing solutions from 01.05.2027; manpower is paid at Year-1 rates, but ATS/AMC of existing products is bidder-funded.	Please provide solution-wise expiry dates of existing licences, ATS/AMC and subscriptions required from 01.05.2027 until new Go-Live. Any mandatory third-party renewal cost during this takeover period must be included as a separate reimbursable/BoM line item or provided by the Bank.	Relevant information concerning incumbent contracts/licenses shall be provided to the selected bidder as required for transition planning. The bidder shall nevertheless factor takeover and transition obligations specified in the RFP
473	59	7.5.7	Non-production environments	Dedicated Development, Testing, UAT and Pre-Production environments must be maintained throughout the contract.	Please confirm the exact non-production requirement per solution: one shared logically segregated non-production environment or separate Development, Test, UAT and Pre-Production environments. Also confirm whether HA/DR is required for non-production.	The bidder shall provide the non-production environments required to meet the RFP's functional, testing, security and operational requirements
474	69, 97, 116-118	7.10, 8 and 11	Warranty/support period	Section 7.10 states three-year comprehensive warranty and Year 4/5 ATS/AMC, while contract support is 60 months post Go-Live.	Please confirm the exact start/end dates for warranty, software subscription, ATS, AMC and FM for each solution, including staggered Go-Live, and how support charges will be prorated.	The applicable support/warranty/subscription period shall be governed by the RFP and contract, with the respective period commencing from the applicable Go-Live date unless specifically stated otherwise. For staggered Go-Live, support shall be aligned to the Go-Live of the respective solution.
475	70-75	7.11	Onsite resources	Minimum deployment tables contain inconsistent totals and resource-layer mapping, and OEM L3 is required for each solution from installation.	Please issue one definitive shift-wise minimum resource table because the resource-count and security-layer tables state different distributions. The response should specify bidder L1/L2/L3, infrastructure L1/L2, Project Manager and OEM L3 count by shift and location.	Please refer Addendum 1 for the revised clause.
476	70-75	7.11	Additional resources	The bidder must augment resources at no additional cost, while the Bank may also procure additional manpower at quoted rates.	Please confirm that bidder-funded manpower augmentation applies only to failure to meet SLA with the stipulated scope and minimum baseline. Additional resources requested for increased scope, new locations, new solutions or workload growth shall be paid at quoted BoM rates.	Bidder's augmentation shall apply where required to meet terms of the RFP, contractual obligations, SLA or minimum service requirements at no additional cost to the bank.
477	79	7.12.44 and 46	Performance and licence activation	Bidder must upgrade systems to Bank expectations and activate any available licensed feature at no cost.	Please confirm that modules/features carrying a separate OEM SKU, subscription, capacity entitlement or consumption charge are not required free of cost under Clause 7.12.46 merely because they can be enabled through a licence key.	Features/modules that are already part of the licensed and contracted solution and required to meet the RFP shall be enabled/provided without additional cost.
478	92-93, 203-213	7.13 and Annexure 21	Sizing baseline	Bidder bears all sizing risk, while several solution-specific transaction, throughput, log-rate and growth inputs remain absent or stated as tentative/unlimited.	Please confirm that the Bank-published quantities and the assumptions approved in the OEM sizing sheets will form the contractual sizing baseline. Growth beyond the published scalable quantities shall be procured using quoted unit rates.	The bidder shall comply with the quantities, capacity, performance, retention, availability, scalability and SLA requirements specified in the RFP.

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
479	92, Appendix 3	7.13.9-12 / V2P	Infrastructure sizing	Bidder must size DC, DR and non-production and obtain each solution OEM confirmation.	Please clarify Appendix 3 terminology by confirming: (a) DR capacity percentage against DC, (b) whether DC-HA and DR-HA rows are additional nodes, and (c) whether N+N means two total active nodes or two complete sets of N nodes at each site.	a) DR should 100% replica of DC b) For the Application where bank has sought N+N Active-Active HA at the DC site, comprising DC Primary and DC HA, with both operating in Active-Active mode. Similarly, N+N Active-Active HA shall be provided at the DR site, comprising DR Primary and DR HA. c) N+N for application architecture shall mean two complete sets of N nodes operating in Active-Active mode. Accordingly, at the DC site, N nodes shall be deployed as DC Primary and an additional N nodes as DC HA, with all nodes operating in Active-Active mode. Similarly, at the DR site, N nodes shall be deployed as DR Primary and an additional N nodes as DR HA, with all nodes operating in Active-Active mode.
480	97-98	8 and 9	Contract period and T0	The contract starts from effective agreement date, while T0 is acceptance of PO and support is 60 months post Go-Live.	Please confirm the precedence and exact trigger dates for T0, implementation, solution-wise Go-Live, warranty, support, FM, LD and contract expiry.	Please be guided by the RFP Please refer Section 9, Project Timelines.
481	97-98	9 Project Timelines	Five-month implementation	All S and C requirements across 21 solutions must be delivered before UAT, with customization by week 17.	Please confirm whether phased, solution-wise UAT and Go-Live are permitted within the five-month implementation period and whether LD applies only to a delayed solution rather than already completed solutions.	Phased, solution-wise UAT and Go-Live within the overall 5-month Implementation Period is permitted, subject to the Bank-approved Project Plan (Section 9). LD for delay in installation/implementation/Go-Live is calculated on the respective Product Cost of the delayed solution only, per Section 13.19. LD does not apply to solutions for which Go-Live has already been completed within timelines.
482	116-118	11.1-11.4	Payment milestones	Software/appliance payment requires OOTB installation on proposed hardware, but subscriptions/SaaS may not be installed on Bank hardware.	For SaaS/cloud subscriptions, please define the documentary evidence equivalent to OOTB installation on Bank hardware and confirm that payment milestones are released solution-wise after respective delivery, UAT and Go-Live.	For SaaS/Cloud-based subscriptions, the bidder shall submit documentary evidence of successful provisioning/activation and availability of the subscribed service for Bank's review. The payment milestones shall be applicable solution-wise and shall be released upon successful delivery/provisioning, UAT sign-off, and Go-Live of the respective solution, as specified in the RFP
483	120-122	12.1	Incident resolution	Critical, medium and low incidents require resolution within 45, 90 and 150 minutes for all hardware/software issues.	Please define "Resolution Time" as restoration of service through permanent fix or Bank-approved workaround. Time awaiting Bank access/approval or third-party action should be excluded where the bidder has provided required evidence and escalation.	Please be guided by the RFP
484	124-126	12.1 Availability	99.99% per individual component	Availability is measured for each solution and any individual component, potentially penalizing redundant component failure without service impact.	Please confirm that 99.99% availability is measured at end-to-end solution service level. Failure of a redundant node/component shall not count as downtime when service remains available without functional or performance degradation.	Please be guided by the RFP. Clarification: Availability continues to be measured for each solution and any individual component, per Annexure 21/Section 12.1. Failure of a redundant node/component, even where the surviving node/component maintains service without functional or performance degradation, shall be tracked and penalized under Incident Response & Resolution Compliance (per the applicable Criticality Table timelines), rather than being excluded from measurement. Any failure of redundant node/ component shall be considered as a critical incident
485	124-126	12.1 Availability	Availability penalty	1% of MMC for each 0.01% shortfall	Please confirm that availability penalty for an affected solution is calculated only on that solution's monthly ATS/AMC/subscription and associated FM amount, not on the aggregate maintenance cost of all solutions.	Please be guided by the RFP, Refer Section 12.1, clause 11 formula for the calculation of MMC
486	127	12.1 Performance	75% utilization for over five minutes	Every subsequent five-minute block is a separate incident and may trigger penalties.	Please replace the five-minute 75% utilization penalty trigger with a sustained threshold measured using an agreed rolling average or percentile, because short peaks without service degradation do not demonstrate capacity shortfall.	Please be guided by the RFP
487	128	12.1 DR	RPO 15 minutes and RTO 60 minutes	RPO/RTO apply instance-wise to all solutions.	Please confirm that RPO 15 minutes and RTO 60 minutes apply to restoration of the solution service at DR, not separately to every redundant supporting VM, container or component.	Please be guided by the RFP Please refer Section 12.1, Performance Measurements wherein it is stated under Minimum Service Level against DR Instance Availability, 100% compliance (Instance - wise)
488	135, 142-143	12.2 and 13.19	LD inconsistency	Section 12.2 specifies 1% per week of respective Product Cost for implementation delay; Section 13.19 specifies 0.5% per week of Contract Price.	Section 12.2 applies 1% per week on respective Product Cost for implementation delay, whereas Section 13.19 applies 0.5% per week on Contract Price. Please confirm the single applicable LD rate and base and that LD will be levied only once for the same delay.	Clause 12.2 shall apply to any delay in implementation, configuration, integration, testing, commissioning, migration, Go-Live, or other implementation-related milestone after delivery and installation of the Product/Solution/Service, whereas Clause 13.19 shall apply to delay in delivery and/or installation within the stipulated schedule.
489	120, 135	12.1.19, 12.2 and 12.3	Penalty cap and at-risk amount	Total SLA and LD are capped at 10% of contract value, while monthly ARA is 15% of estimated payout.	Please confirm that the 15% monthly At-Risk Amount is the maximum amount withheld for SLA measurement and is not an additional penalty over and above the aggregate 10% SLA/LD cap.	Please be guided by the RFP Refer Section 12, Clause 12.2: For the purpose of this RFP, the total penalties as per LD & SLA will be subject to a maximum of 10% of the overall contract value.
490	205	Annexure 21.2	Existing stack	The existing solution list omits item number 2 and does not show SSL Orchestrator/packet broker details.	Annexure 21.2 omits item 2 and does not provide the incumbent SSL Orchestrator/packet-broker inventory. Please provide the missing solution name, make, model, quantity, version and support-expiry details required for migration/takeover costing.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
491	212-213	Annexure 21.4	Backup responsibility	Row 22 states backup and retention are provided and maintained by Bank, but bidder must right-size and other sections require bidder-provided backup infrastructure/software.	Annexure 21 states backup is provided and maintained by the Bank, while Sections 7.13 and 7.12 assign backup solution sizing/operations to the bidder. Please confirm which party supplies and pays for backup software, backup storage/appliance and LTS, and which party performs backup, restore, replication and WORM operations.	Please refer Addendum 1 for the revised clause. Clarification : The bidder shall be responsible for the complete end-to-end supply, installation, configuration, integration, testing, commissioning, documentation, warranty and comprehensive maintenance of the proposed IT infrastructure throughout the contract period, as specified in the RFP. Accordingly, the complete Backup & Restoration solution, including Ransomware Protection, Backup Software, Backup Server, Backup Storage/Backup Appliance, Long-Term Storage and all associated hardware, software, licenses, accessories and components, shall be supplied, designed, sized, configured, implemented and maintained by the bidder Implementation of the IT Infrastructure at the Bank's DC, DR, NDR and/or other designated locations is the responsibility of the bidder/OEM. The bidder shall consider the complete requirement while carrying out the sizing and shall include all necessary components, licenses and associated infrastructur
492	88	7.13	IT Infrastructure	IT Infrastructure provisioning	Will bank provide Oracle DB licenses if our solution requried Oracle DB ?	The bidder shall factor all software, database, operating system, middleware, virtualization and other licenses required for the proposed solution unless specifically stated otherwise in the RFP. No assumption of Bank-provided Oracle licenses shall be made.
493	88	7.13	IT Infrastructure	The bidder/OEM is responsible for supplying, designing, sizing and configuring the Backup Software and Hardware (with Ransomware Protection). The backup solution configuration should comply with bank's policy for secure data backup, with flexibility for updates as policies evolve. Sizing should align with the overall storage requirements.	Kinldy provide the retension policy for backup appliance and Long term storage	The bidder shall comply with the backup and long-term retention requirements specified in the RFP
494	76	7.12 Facilities Management	point 6	a. "To the best of our knowledge and on the basis of logs, data, information collated by the NextGEN SOC in various systems and analysis thereof by us using NextGEN SOC tools, we confirm that no major information / cyber security incident has happened during the last month. The logs, data, information etc. correlated by us confirms no data or information having been compromised, exfiltrated or any of the systems having been compromised / hacked.	Kinldy modify the same " "Based on logs, alerts and events observed in the solutions managed under this contract, no major security incident was detected during the reporting period."	Please be guided by the RFP. The bidder undertaking is specific to the solution provided by bidder and protection that bidder proposed solution are providding
495	121	CRITICALITY TABLE	Level Classifications	Critical / High Response: 15 Minutes Resolution: 45 Minutes	Please confiim - 45-minute SLA refers to service restoration/workaround	Please be guided by the RFP Clarification: the 45-minute timeline is the Resolution Time for Critical/High severity incidents, i.e., restoration of service (including via an acceptable workaround where applicable)
496	93	7.14.1	Other Scope Activity	The Respective solution OEM along with the bidder is expected to ensure that for the purpose of this RFP, statutory and regulatory changes shall mean any change prescribed by the statutory and regulatory bodies governing/ affecting the banking industry in India viz. Reserve Bank of India, Ministry of Finance, CCIL, NPCI, IBA, SEBI, or any such bodies constituted by the RBI mandating change/s to an existing functionality of the Solution shall be provided to the Bank at no additional cost for the entire contract period. However, any Statutory and Regulatory changes post complete Go-Live of the respective applications (which are not a part of the existing functionalities) will be on CR basis based on the rates provided in the Bill of Material.	Please confirm - that only regulatory changes supported by existing licensed product functionality shall be included under ATS/AMC. New modules/licenses/products shall be treated as change requests.	New Regulatory changes, Any new or revised regulatory requirement introduced after the Bid Submission Date, required to maintain compliance with applicable requirements and supported by the existing contracted/licensed solution functionality shall be provided without additional cost. Where compliance with a new or subsequently introduced regulatory requirement requires a new product, module, additional license, or functionality that was not specified or envisaged in the RFP/Guidelines and was not available or communicated to bidders as of the bid submission date, such requirement may be processed through the applicable Change Request (CR) mechanism, subject to the Bank's approval. The bidder shall not treat configuration changes, upgrades, patches, or enhancements that are within the existing contracted/licensed functionality as a new module or additional license merely on account of a subsequent regulatory change.
497	82	7.12.3	IT Security operations	There should be considerable reduction in MTTD (Mean Time to Detect) and (Mean Time to Remediate) MTTR for security incidents by leveraging technology's own capabilities. All daily routine and standard activities of L1 and L2 to be fully automated.	Please define measurable automation expectations and identify specific activity categories expected to be automated.	The bidder shall automate routine, repetitive and standard L1/L2 activities to the maximum extent technically feasible using the proposed technologies and automation capabilities.
498	83	7.12.3	IT Security operations	Develop custom plug-ins, parsers, connectors, agents, adopters for all the systems in the Bank or related to the Bank periodically or as and when needed without any extra cost to bank.	Kindly define limits for minor enhancements versus major customizations requiring to be accomplished via CR.	Enhancements required to configure, integrate, tune, operate and optimize the proposed solutions within the RFP scope shall be included. A CR may be considered only for materially new functionality, new products/modules/licenses or requirements outside the contracted scope, subject to Bank approval.

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
499	78	7.12 Facilities Management	Facilities Management	Feature requests, all critical, showstopper declared by the Bank needs to be implemented within 1 week including thorough functional, performance and security review. There should be no negative functional impact, data loss or performance degradation whatsoever with the introduction of new feature, enhancement, upgrade, bug fixes, customization.	Please confirm implementation timelines shall be subject to OEM product roadmap, OEM release availability, and technical feasibility.	The bidder/OEM shall comply with the timelines specified by the Bank
500	74	Resource Deployment, Replacement and Governance	2	The bidder shall ensure availability of OEM L3 specialists, architects, and SMEs for all proposed solutions throughout the contract period as and when required as per the requirements, scope of the RFP, and in line with the SLAs.	Please confirm that OEM L3 support may be provided remotely through OEM TAC and resident OEM resources are required only during implementation	OEM Implementation Resources shall be deployed onsite on a full-time basis during the Implementation Phase as specified in the Section 7.11 Resource Requirement. No remote access shall be provided to any resource
501	83	7.12.3 IT Security operations	10	Perform fortnightly & monthly gap analysis of issues/threat/vulnerabilities in OS, databases, web servers, applications and devices and entire IT infrastructure & recommend and implement remedial actions.	Please clarify the inventory of systems included under log-gap analysis and whether third-party/non-integrated systems are excluded.	Gap analysis shall cover the in-scope IT/security environment and systems relevant to the proposed solutions
502	76	7.12 Facilities Management	6	Starting from Go-Live date of the respective security solutions, 7th day of every month: Monthly Security Certificate to be submitted by the Project Manager of the bidder and onsite resources of the OEMs stating:	Kindly confirm that bidder-issued consolidated monthly reports shall be accepted in lieu of OEM signed declarations.	Please be guided by the requirements specified in the RFP. OEM review/certification shall be required wherever specifically sought or mandated in the RFP. A bidder-issued consolidated monthly report may be submitted for other reporting requirements; however, it shall not be considered a substitute for OEM-signed certification/declaration where such certification is explicitly required under the RFP.
503	54	7.5.1	Migration - Activities are to be performed by Respective solution OEM (supported by bidder)	The bidder and respective OEM shall adhere to the implementation timelines approved by the Bank. In the event of any delay in implementation of the proposed solution, the bidder shall, upon the Bank's direction, undertake the takeover, transition, maintenance, and management of the corresponding existing solutions and services from the incumbent vendor until successful Go-Live of the proposed solution.	Request Bank to provide complete inventory of incumbent security solutions, OEMs, versions, licenses, support status (start and end date) and volumetrics to enable accurate effort estimation.	The Bank shall provide relevant information required for transition and implementation to the selected bidder on a need-to-know basis.
504	127	Performance Measurements	Hardware Utilization	Daily peak utilization of CPU, memory (RAM), network interfaces (NIC), storage I/O, or other critical infrastructure resources exceeds 75% for more than 5 consecutive minutes. Each subsequent block of 5 minutes shall be treated as a separate incident. Where virtual machines (VMs), containers, or similar workloads are deployed, utilization shall also be measured at the individual VM/container level. Utilization of any VM or container shall not exceed 75% for more than 5 consecutive minutes.	Request Bank to measure utilization based on average monthly utilization rather than isolated peaks of 5 minutes.	Please be guided by the RFP
505	43	IDAM	Life Cycle Management	The solution must support full lifecycle management of user's machine identities and access governance using cryptographic keys. This includes automated provisioning and deprovisioning to minimize the risk of credential sprawl and unauthorized access	1) Please clarify the usecases for access governance using cryptographic keys. 2) Would it mean that Bank wants to do the Governance on the Identities of All Target System(All OS, Network Device, Security Devices, Database), Same as IGA ?	1) Please be guided by the RFP 2)Bank wants to do the Governance on the Identities of All Target System(All OS, Network Device, Security Devices, Database) using cryptographic keys
506		IDAM	Architecture	Generic	Please confirm below details: Total Number of Application Type of Application-Web/thick , Cots/SAAS etc.	Application-related information will be provided during implementation and SRS stage
507	47	MFA	MFA	Generic	Please confirm if MFA is required for endpoints/Applications as well?	Yes, the MFA is required for the Endpoints/Applications
508	51	PIM/PAM	Public Cloud	The solution shall support privileged identity governance for major public cloud providers.	Is Bank looking for IGA Functionality for All Cloud Platforms (AWS,Azure, GCP, OCI) ?	Please be guided by the RFP
509	43	IDAM	Life Cycle Management	For access via CLI (console, Telnet, SSH), WBM and Web Services (HTTPS) users can be authenticated via RADIUS/ TACACS+ or via local table of authorized users.	Does it mean that the Bank would like to have AAA Capabiltiy within the IDAM/PAM to do fill integration with network devices ?	The proposed solution should support RADIUS and other relevant protocols for integration.
510	47	MFA	Technical Specification MFA	For access via CLI (console, Telnet, SSH), WBM and Web Services (HTTPS) users can be authenticated via RADIUS/ TACACS+ or via local table of authorized users.	Does it mean that the Bank would like to have AAA Capabiltiy within the MFA to do fill integration with network devices ?	The proposed solution should support RADIUS and other relevant protocols for integration.
511		PIM/PAM	Generic		Is Bank Looking for Just Enough privilege for Just In Time (Provisioing/ Deprovisioning) for all Infrastructures Assets(OS, Network Device, Security Device, Database) ?	Yes, bank is Looking for Just Enough privilege for Just In Time (Provisioing/ Deprovisioning) for all Infrastructures Assets(OS, Network Device, Security Device, Database)
512			Generic		Is Bank looking to Secure Outside PIM/PAM Accesse ?	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
513	105	Point Number 19	The proposed OEM solution/product for Privilege Identity/Access Management should have been successfully implemented in at least 2 BFSI in India, out of which at least one (1) BFSI Client should have a deployment covering more than 1,500 privileged users	We recommend the Bank to consider the below points that will help the bank for the OEM Eligibility Criteria: A) We recommend the clause to be added as- The Proposed OEM Solution/ Product for Privilege Identity/Access Management should have been successfully implemented and Running for More than 2 Years. (This Clause will help the Bank to understand that the Client is using the Solution till Date) B) We recommend the Clause to be added as- The Proposed OEM solution/product for Privilege Identity/Access Management should have been successfully implemented in at least 3 BFSI in India, out of which minimum (2) BFSI Client should have a deployment covering more than 1,500 privileged users	We recommend the Bank to consider the below points that will help the bank for the OEM Eligibility Criteria: A) We recommend the clause to be added as- The Proposed OEM Solution/ Product for Privilege Identity/Access Management should have been successfully implemented and Running for More than 2 Years. (This Clause will help the Bank to understand that the Client is using the Solution till Date) B) We recommend the Clause to be added as- The Proposed OEM solution/product for Privilege Identity/Access Management should have been successfully implemented in at least 3 BFSI in India, out of which minimum (2) BFSI Client should have a deployment covering more than 1,500 privileged users	Please be guided by the RFP
514		PIM/PAM	Eligibility Criteria	Generic	We recommend if the Bank can add the Below Points for the PIM/PAM Eligibility Criteria: A) Proposed PIM/PAM Solution should have the Presence in India for more than 10 Years B) Proposed PIM/PAM OEM by the Bidder should have the Annual Average Turover for last three Years should be more than INR 60Cr. C) The offered PAM OEM Solution must be certified for Common Criteria Certificate EAL 2+ and supporting certificate document should be submitted during the bid submission.	Plese be guided by the RFP
515	34	Anti-DDoS	7.3.1.1	Anti-DDoS Deployment	Kindly clarify whether the Anti-DDoS solution is expected to operate in always-on inline mode or diversion-based architecture shall also be accepted.	The Anti-DDoS solution shall support both always-on inline and diversion-based/out-of-path deployment architectures, as applicable to the Bank's network architecture and operational requirements. The deployment architecture shall be finalized during the detailed design phase in consultation with the Bank, while ensuring compliance with the RFP's requirements for availability, fail-open operation, traffic visibility, detection, and mitigation.
516	35	SSL Orchestrator	7.3.1.2	SSL Orchestrator & PCAP	Kindly provide expected average and peak SSL/TLS traffic volume for sizing SSL decryption infrastructure.	Bidder/OEM shall size the solution based on the RFP requirements and shall factor adequate capacity,
517	45	WAF	7.3.4.2	Web Application Firewall	Kindly provide the approximate number of web applications and APIs to be protected under the WAF scope.	Bidder shall size the WAF based on the RFP scope
518	70-75	Resource Requirement	7.11	Minimum Resource Count Deployment	Kindly confirm whether OEM L3 resources can be provided remotely except where onsite presence is specifically required by the Bank.	Please be guided by the RFP
519	100	Eligibility Evaluation Criteria	10.2	The bidder should be an authorized representative/ partner/ reseller of each of the proposed OEMs in India. MAF should be submitted from the following solution OEMs: 1. Anti-Distributed Denial of Services (Anti-DDoS) 2. SSL Orchestrator along with packet broker 3. DNS protection (Internal DNS Security) 4. Web Gateway 5. Zero-Day Attack Protection at Endpoint and network 6. Zero Trust Network Access (ZTNA) 7. Data Loss Prevention (DLP) Information/Digital Right Management 9. Database Activity Monitoring 10. Mobile SDK 11. Host IPS including Application Change Control (HIPS) 12. Web Application Firewall (WAF) 13. Centralized key management solution 14. Certificate Lifecycle management 15. Identity & Access Management Solution 16. Multi Factor Authentication 17. Privilege Identity/Access Management 18. DNS Security Services (Internet-Facing DNS Security Services) 19. Cloud Access Security broker (CASB) 20. AI Security 21. SBOM/CBOM/AIBOM/QBOM	The Bank is requested to remove this clause as no bidder can be an authorized representative / partner / reseller of each of the OEMs proposed.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
520	46	S-BOM, C-BOM, AI-BOM & QBOM	7.3.4.5	The Bank requires a comprehensive Software Bill of Materials (S-BOM), Cryptographic Bill of Materials (C-BOM), AI Bill of Materials (AI-BOM), and Quantum Bill of Materials (Q-BOM) solution to provide centralized discovery, inventory, governance, and continuous monitoring of software components, cryptographic assets, AI assets, and quantum-vulnerable dependencies across the Bank's IT environment.	Please clarify if a separate single solution is to be factored for this requirement or the respective solutions proposed will share the compliance to S-BOM, C-BOM, AI-BOM & QBOM as applicable to them	Please be guided by the RFP
521	100-109	Eligibility Evaluation Criteria	10.2	Eligibility Criteria/Clause and Supporting Documents	Kindly confirm whether a wholly owned subsidiary of the Bidder/Parent Company shall be permitted to participate in the RFP and submit the bid in its own name, with the contractual obligations, execution, contracting, and invoicing being managed by the subsidiary. Further, please confirm whether such wholly owned subsidiary shall be permitted to leverage the credentials, qualifications, relevant experience, past performance, technical capabilities, references, and financial credentials of its Parent Company for the purpose of meeting the Pre-Qualification and Technical Qualification criteria specified in the RFP. Additionally, in the event of any corporate restructuring, merger, demerger, acquisition, spin-off, or transfer of business between the Parent Company and its subsidiary/entity, kindly confirm whether the financial credentials, experience, past performance, certifications, technical capabilities, and other relevant qualification documents of the Parent/Predecessor Entity shall be considered for determining the eligibility and qualification of the participating entity, subject to submission of appropriate documentary evidence establishing the continuity and transfer of such business, assets, capabilities, and obligations.	Please be guided by the RFP
522	152	Annexure 2: Bidder's Information	Point 12	We agree to the splitting of order in the proportion as stated in the RFP at the discretion of Bank.	Please confirm how order will be split	Annexure 2: Point 4 states - Bank may accept or entrust the entire work to one Bidder or divide the work to more than one bidder without assigning any reason or giving any explanation whatsoever and the Bank's decision in this regard shall be final and binding on us. The above splitting of the order shall be based on the division of scope of work as specified by the Bank.
523	76	7.12 Facilities Management	Point 7.12	There should be considerable reduction in MTTD and MTTR for security incidents by leveraging technology's own capabilities and SOAR. All daily routine and standard activities of L1 and L2 to be automated in phased manner from the date of Go-live.	MTTD & MTTR not applicable for Solution management and Administration. There is no SOAR solution asked hence Bank's SOAR solution would be used?	MTTD/MTTR requirements shall apply to security incidents and operational events within the bidder's managed scope, as applicable. The absence of a separate SOAR procurement does not remove the requirement for automation and integration where such capabilities are available through existing Bank platforms or proposed solutions.
524	76	7.12 Facilities Management	Point 7.12.6	Starting from Go-Live date of the respective security solutions, 7th day of every month: Monthly Security Certificate to be submitted by the Project Manager of the bidder and onsite resources of the OEMs stating:	The SOC SIEM tool is not in scope hence this point should not be applicable	The Requirement is applicable and enforceable for the solution in-scope of the bidder. The certificate/report shall cover the bidder's managed solutions and associated security operations as specified in the RFP.
525	Additional	Additional	Additional	Working Days Shift Timings Holidays in Year	Please provide working days details Please provide shift timings Please provide holiday calendar or holiday days in year	Please be guided by the RFP, Holidays - Holidays shall be governed by the Haryana State Government holiday notifications and applicable provisions under the NI act
526	Additional	Additional	Additional	Last 6 month Ticket volume	Please provide last 6 month ticket volume data for existing technologies including incidents, service requests, change requests, Problem tickets	The details shall be shared with the successful bidder
527	32	7.1 IT Security Solution & Services	Note: Point 8	The proposed solutions shall provide dynamic, customizable dashboards and reports with analytical and actionable insights for effective monitoring, governance, and decision-making	for Dynamic, customizable dashboard, does it refer to individual technology console dashboard or expected to deploy tool to capture each technology dashboards?	Each proposed solution shall provide its required native dashboards. Where centralized reporting/visibility is required, integration with the Bank's designated SOC/security monitoring platform shall be performed.
528	207-213	Annexure 21	15.21.4	Backup Retention Requirements	Kindly confirm that storage sizing should consider the complete contract period retention requirement for Long Term Storage.	The sizing is to be proposed for the duration of the Contract
529	88-93	IT Infrastructure	7.13	Hardware Sizing	Kindly confirm whether Bank-provided TOR switches and racks are available at DC, DR and Non-Production environments.	Bank will provide racks and TOR switches ports at DC, DR and Non-production

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
530	60	7.15. Force Majeure	7.15	Any failure or delay by selected bidder or Bank in the performance of its obligations, to the extent due to any failure or delay caused by events beyond the control of either Party (Bank or Selected Bidder) and which such Party could not have avoided by use of reasonable case, including but not limited to acts of god or public enemy, actions of Governmental Authorities, acts of war, rebellion, sabotage or fires, floods, explosions, epidemic, quarantine restrictions, riots, or strikes or analogous events ("Force Majeure Events"). If the successful Bidder is prevented or delayed from the performing any of its obligations under the Contract by Force Majeure Events, then the successful Bidder shall notify Bank the circumstances constituting the Force Majeure Event and the obligations, performance of which is thereby delayed or prevented, the beginning and end of the cause of delay immediately, but in no case later than 3 days from the beginning and end of such Force Majeure Event respectively.	Informing in 3 days would be difficult. We request a window of at least 30 days. We suggest the below language - "Force Majeure Event" is any cause beyond a Party's reasonable control, including, without limitation, any act of war, act of God or nature, earthquake, hurricanes, tornados, flood, fire or other similar casualty, embargo, riot, terrorism, sabotage, strike or labour difficulty, governmental act, law or regulation, insurrections, terrorism, epidemic, quarantine, inability to procure materials or transportation facilities, failure of power, court order, condemnation, failure of the Internet, failure of a supplier or other cause, whether similar or dissimilar to the foregoing, not resulting from the actions or inactions of such Party. Except for Customer's payment obligations accruing under this Agreement for Services properly performed up to the date of a bona fide Force Majeure Event, neither Party shall be liable, nor shall any credit allowance or other remedy be extended, for any performance that is prevented or hindered due to a Force Majeure Event provided, however, that Customer shall not be required to pay for Services not provided during the period of the Force Majeure Event, and any prepaid fees for such affected Services shall be equitably prorated or refunded, as applicable. If during the Service Term Supplier is unable to provide Services for a period in excess of sixty (60) consecutive days due to a Force Majeure Event, then either Party may terminate the affected Service(s) upon written notice to the other Party, and both Parties shall be released from any further future liability in relation to such Service(s) without prejudice to any rights or obligations accrued prior to the effective date of termination or any provisions that expressly survive termination..	Please be guided by the RFP
531		7.22. Cancellation of Contract	7.22	The Bank reserves the right to cancel the contract of the selected Bidder and recover expenditure incurred by the Bank in any of the following circumstances. The Bank would provide 30 days cure period to rectify any breach/ unsatisfactory progress if: □ The selected Bidder commits a breach of any of the terms and conditions of the bid/contract.□ □ The selected Bidder becomes insolvent or goes into liquidation voluntarily or otherwise.□ □ The progress regarding execution of the contract, made by the selected Bidder is found to be unsatisfactory.□ □ If deductions on account of penalty and liquidated damages exceeds more than 10% of the total contract price.□ After the award of the contract, if the selected bidder does not perform satisfactorily or delays Execution of the contract, the bank may give a 30 days cure period. Thereafter, if the selected bidder does not perform satisfactorily or delays execution of the contract, the Bank reserves the right to get the balance contract executed by another party of its choice. In this event, the selected bidder is bound to make good the additional expenditure, which the Bank may have to incur to carry out the bidding process for the execution of the balance of the contract capped up to a maximum of 50% of the Price quoted by the bidder of the undelivered portion of services. This clause is applicable if for any reason the contract is cancelled	We suggest to add - Exception to this clause, If the Order Cancellation occurs due to Bank's direct act or omission. In such case, the Bidder shall not be liable to pay for sucg charges.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
532	212 / 88	Annexure 21.4 / Section 7.13	Annexure 21.4 Sl. 22 read with Clause 7.13 (5)(ii)	Annexure 21.4, Sl. No. 22 is titled "Backup & Retention (Provided and maintained by bank)" while the same row states "Bidder to right size". Clause 7.13(5)(ii) states the Bidder/OEM is responsible for supplying, designing, sizing and configuring the Backup Software and Hardware (with Ransomware Protection). Appendix 1B contains full technical specifications for Backup Solution and Long-Term Storage, and Appendix 2 contains priced line items for Backup Server, Backup Storage/Backup Appliance, Long Term Storage and Backup Software.	The Bank is requested to confirm whether the Backup Software, Backup Server, Backup Storage/Appliance and Long-Term Storage are to be supplied, sized and priced by the bidder, or whether these will be provided and maintained by the Bank from its existing infrastructure. If Bank-provided, please confirm whether the corresponding line items in and specification The Bank is requested to confirm that backup infrastructure supply, sizing and operation rest with the bidder, Bank is requested to provide the total data volume to be backed up (front-end TB) and the expected daily change rate, .daily data changes. does Backup storage need to replicated both side? Exact retention policy needed	Please refer Addendum 1 for the revised clause. The bidder shall be responsible for the complete end-to-end supply, installation, configuration, integration, testing, commissioning, documentation, warranty and comprehensive maintenance of the proposed IT infrastructure throughout the contract period, as specified in the RFP. Accordingly, the complete Backup & Restoration solution, including Ransomware Protection, Backup Software, Backup Server, Backup Storage/Backup Appliance, Long-Term Storage and all associated hardware, software, licenses, accessories and components, shall be supplied, designed, sized, configured, implemented and maintained by the bidder Implementation of the IT Infrastructure at the Bank's DC, DR, NDR and/or other designated locations is the responsibility of the bidder/OEM. The bidder shall consider the complete requirement while carrying out the sizing and shall include all necessary components, licenses and associated infrastructure
533	207-212 / 92	Annexure 21.4 / Section 7.13	Annexure 21.4 (Deployment & Data Retention) read with Clause 7.13 (a) and (h)	All 21 solutions require 1 month retention of logs and data on Appliance / Primary Storage. Monthly Full backups are required to be retained in Long-Term Storage in immutable WORM format for the entire contract duration. The bidder is held solely responsible for the accuracy and adequacy of sizing. However, no log generation rate, event rate (EPS), or daily data volume has been provided for any of the proposed solutions.	The Bank is requested to provide indicative daily log/data generation volume (in GB/day or EPS) per solution, or in aggregate, to enable accurate sizing of Primary Storage, Backup Storage and Long-Term Storage. In the absence of such data, the Bank is requested to confirm that bidder sizing so the storage can be factored . what are all devices need to be backup .	Bidder to right size
534	92 / 94	Section 7.13 / Section 7.14.1	Clause 7.13 (10) read with Clause 7.14.1 (13)	Clause 7.13(10) states that the Bank would provide TOR Switch and Racks, the sizing of which shall be provided by the bidder in the technical proposal. Clause 7.14.1(13) states that hosting space and power shall be provided by the Bank, however the bidder is required to factor in the requisite racks in order to operationalize the proposed hardware.	The two clauses are contradictory in respect of racks. The Bank is requested to confirm whether racks are to be supplied and priced by the bidder, or provided by the Bank with the bidder furnishing only the sizing requirement. Who will provide the cable , ports / sfp , incase of we factor new server for backup or any new solution will back provide the management leaf spine switch or bidder need to factor	Bank will provide racks and TOR switches ports at DC, DR and Non-production
535	92	Section 7.13	Clause 7.13 (10)	Clause 7.13(10) requires the bidder to provide sizing for TOR Switches and Racks. However, Appendix 1B does not contain a technical specification sheet for TOR Switch or Racks, and Appendix 2 does not contain a corresponding priced line item under the IT Infrastructure Cost sheet.	The Bank is requested to confirm that TOR Switches and Racks are excluded from the bidder's commercial scope and that only the sizing/quantity requirement is to be submitted in the technical proposal. If they are to be priced, the Bank is requested to publish the applicable technical specifications and add the corresponding line items	Bank will provide racks and TOR switches ports at DC, DR and Non-production
536	88	Section 7.13 / Appendix 2	Clause 7.13 (2)(vi) read with Appendix 2 - IT Infrastructure Cost sheet	Clause 7.13(2)(vi) includes "DC, DR & NDR Implementation" within scope, and the Scope of Work covers Data Centre (Mumbai), NDC, Disaster Recovery Centre (Noida), NDR and Cloud environments. However, the IT Infrastructure Cost, Appliance Cost, License Cost and ATS sheets in Appendix 2 provide sections only for DC-Primary + HA, DR-Primary + HA and Non-Production.	The Bank is requested to clarify whether IT Infrastructure is required at NDC and NDR, and if so, to publish the corresponding sections in Appendix 2 for pricing. Alternatively, please confirm that NDC and NDR are excluded from the IT Infrastructure supply scope under this RFP.	The proposed Long-Term Storage (LTS) solution shall be deployed at both NDC and NDR and shall support long-term retention and storage of backups, logs, files and other Bank-approved data, as applicable. The proposed solution shall provide adequate capacity, scalability, availability, data protection and access mechanisms to meet the Bank's defined retention and storage requirements at both sites.
537	128	Section 11 - Service Level Agreement	SLA - Disaster Recovery (DR) Instance Availability	The SLA prescribes RPO of 15 minutes and RTO of 60 minutes, measured instance-wise at 100% compliance, with a penalty of Rs. 10,000 for every 10 minutes or part thereof beyond the stipulated RPO or RTO.	The Bank is requested to confirm (a) whether the 15-minute RPO / 60-minute RTO applies uniformly to all 21 proposed solutions including appliance-based solutions deployed in N+N Active-Active configuration at DC and DR, and (b) whether the Bank will provide the DC-DR replication bandwidth, or whether the same is to be sized and provisioned by the bidder.	(a) RPO/ RTO applies uniformly to all 21 proposed solutions (b) Replication bandwidth to be provided by Bank
538	149	Appendix 1B	Appendix 1B - Long Term Storage, Sl. 4	Appendix 1B requires the bidder to propose Long-Term Backup Storage at both the Data Centre (DC) and Disaster Recovery (DR) sites, adequately sized to retain backup data for the entire duration of the contract.	The Bank is requested to confirm whether a complete, independent copy of all Monthly Full backups is required to be retained for the full contract duration at BOTH DC and DR (i.e. two full retention copies), or whether the DR Long-Term Storage is intended to hold a replicated subset. This materially affects Long-Term Storage capacity and cost.	Please be guided by the RFP, backup is to be taken at both DC and DR

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
539	149	Appendix 1B / Appendix 2	Appendix 1B - Load Balancer sheet	Appendix 1B contains a detailed technical specification sheet for a Load Balancer / Application Delivery Controller, including a requirement that it be a dedicated appliance and not an add-on licence feature on NGFW or WAF. However, the IT Infrastructure Cost sheet in Appendix 2 does not contain a line item for Load Balancer, and the Appliance Cost sheet lists only the 21 security solutions.	The Bank is requested to confirm under which sheet and line item of Appendix 2 the Load Balancer is to be priced, and the required quantity and deployment sites (DC / DR / Load Balancer Clarification Required The Bank is requested to clarify under which sheet and line item of Appendix 2 the Load Balancer solution should be priced. Additionally, please provide the required quantity and deployment locations across DC, DR, and Non-Production environments. To enable accurate sizing and commercial estimation, kindly share the following details: Number of Load Balancers required at DC and DR locations. Whether the Load Balancers are to be deployed in HA (High Availability) mode. Load Balancer type and functionality requirements: L4 Load Balancer L7 Load Balancer GSLB (Global Server Load Balancing) Internet/ILL-facing Load Balancer Make and preferred model (if any). Number of ports required. Port speed requirements (1G/10G/25G/40G/100G). Licensed ports and throughput requirements. Redundancy and HA features required. SSL offloading, WAF integration, DNS, and health monitoring requirements. Technical specifications, performance, and sizing parameters. Quantity of appliances/licenses required for each environment (DC, DR, and Non-Production). Required Details: Make, Model, Number of Ports, Port Speed, Licensed Ports, Throughput Capacity, Redundancy Features, Deployment Architecture (HA/Cluster), and Quantity for DC and DR locations. Additionally, please specify requirements for L4/L7 Load Balancing, GSLB, and Internet-facing Load Balancer functionalities.	Bidder to design based on the deployment requirement of the solution and sizing. Bidder to mention the item required under the row any "Any other please specifiy cell"

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
540	-	Appendix 1B / Appendix 2	Appendix 1B - x86 Servers and GPU Server sheets read with Appendix 2 IT Infrastructure Cost sheet	The IT Infrastructure Cost sheet in Appendix 2 provides line items for "Server-Compute - Configuration 1" and "Server-Compute - Configuration 2". Appendix 1B contains one x86 Server specification sheet and one GPU Server specification sheet.	The Bank is requested to clarify the following in respect of compute sizing and pricing: (a) Whether "Server-Compute – Configuration 1" corresponds to the x86 Server specification in Appendix 1B and "Server-Compute – Configuration 2" corresponds to the GPU Server specification in Appendix 1B; or alternatively, whether Configurations 1 and 2 represent two bidder-defined x86 configurations based on workload profile, in which case the Bank is requested to confirm the line item under which the GPU Server is to be quoted; (b) The proposed solution(s) that require GPU-accelerated compute, and the corresponding workload basis (for example, AI Security inferencing, sandboxing, or analytics); (c) The minimum required quantity of GPU Servers at each of DC, DR and Non-Production, and the number of GPU cards required per server; (d) Whether the GPU memory requirement of 94 GB is to be met by a single GPU card or may be aggregated across multiple cards within the same server. The Bank is requested to note that GPU-accelerated servers represent a significant cost component, and that the above clarifications are essential to ensure uniform and comparable commercial bids across all bidders.	a) Configuration 1 - Non-GPU Servers Configuration 2 - GPU Servers b) Bidder to propose the GPU conplying with the requirement and terms of the RFP after right sizing the solution c) Bidder to right size the solution and It Infrastructure d) GPU Servers with single GPU of 94GB memory or higher
541	-	Appendix 1B	Appendix 1B - GPU Server, Sl. 8 and Sl. 7	The GPU Server specification requires GPU memory of 94 GB or higher and mandates that the server be supplied with a Windows Datacentre licence.	The Bank is requested to specify (a) which proposed solution(s) require GPU-accelerated compute, (b) the required quantity of GPU servers at DC, DR and Non-Production, and (c) the number of GPU cards required per server, as these parameters are not stated in Annexure 21 or elsewhere in the RFP.	Bidder to design based on the deployment requirement of the solution and sizing
542	77		The bidder shall ensure DC and DR are exact replicas of each other in every manner.	The bidder shall ensure DC and DR are exact replicas of each other in every manner.	The Bank is requested to confirm that this requires the DR environment to be sized at 100% parity with DC across compute, storage, appliances and licences, and that DR is to be quoted on an identical bill of material to DC.	Yes. The DR environment shall be sized at 100% parity with the DC environment across compute, storage, appliances, and applicable licences.
543	87	7.12.5	SLA · Clause	requires the bidder to provide estimates of recovery time, and 7.12.5(5) requires the bidder to state the likely extent of data loss in the event of recovery. The SLA separately mandates a fixed RPO of 15 minutes and RTO of 60 minutes with penalties of ₹10,000 per 10 minutes of breach.	The Bank is requested to clarify whether the RPO and RTO are fixed contractual commitments of 15 minutes and 60 minutes respectively (as per the SLA), or whether they are to be estimated and proposed by the bidder (as per Clause 7.12.5). The Bank is further requested to confirm whether the DC–DR link is Bank-provided, and to specify the available bandwidth and latency, as replication design and storage sizing depend on this.	(a) RPO and RTO are fixed contractual commitmments. (b) Details shall be shared with the successful bidder
544	52 / 94	7.5.1 / 7.14.1	7.5.1 / 7.14.1	hosted premises at DC and DR. Clause 7.14.1(13) states hosting space and power shall be provided by the Bank while the bidder factors in requisite racks.	the DC and DR are co-hosted facilities, the Bank is requested to provide (a) the number of rack positions available to the bidder at each site, (b) power availability per rack in kW and supply configuration (single/dual feed), (c) cooling capacity and permissible heat load per rack, and (d) whether any co-location charges are payable by the bidder. These parameters constrain server and GPU density and rack quantity. The Bank is requested to confirm (a) that the Bank-provided TOR switches support 25G SFP28 ports at the required port density, (b) whether SFP28 optics and patch cords on the TOR side are to be supplied by the bidder, and (c) the make and model of the existing TOR switches for interoperability validation.	Details shall be shared with the Successful bidder.
545	76	7.12 Facilities Management	7.12.4	All onsite personnel resources of the bidder & OEMs should ensure to deliver the services leveraging security technologies as mentioned in the technology details	There is no specific OEM resource requirement mentioned. Please suggest how many OEM resource required? in which shift?	Bank sought resources are minimal requirement, bidder shall ensure OEM resources are and shall be deployed wherever necessary to meet implementation, SLA and operational requirements.
546	NA	GEM Bid Document	Additional	MII Compliance: Yes	Request relaxation on MII compliance	Please be guided by the RFP
547	NA	GEM Bid Document	Additional	Purchase Preference to MSE OEMs/ Service Provider available up to price within L1+15%	Request relaxation, all bidders should be evaluated equally without price preference for MSE.	Please be guided by the RFP
548	NA	Additional	Additional	Subsidiary/Affiliate	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. Please confirm	The bidder may participate either directly or through its wholly owned subsidiary, subject to the bidding entity meeting all eligibility, qualification, contractual, and other requirements specified in the RFP. The contracting and invoicing entity shall be the same legal entity that submits the bid and is awarded the contract

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
549	97	8 CONTRACT PERIOD	8 CONTRACT PERIOD	The bank may, at its sole discretion, extend the contract for an additional period of two years, in one year increments tranches. The Bank may extend the support services for an additional period of up to two (2) years beyond the original contract period. The pricing applicable during the extension period shall be mutually agreed and shall not exceed 110-120% of last year's AMC/ATS/Facility management rates quoted by the Selected Bidder.	Extension of contract post 5 year term and the prices should be mutually agreed during renewal. Bidder wont be able commit on prices post 5 year contract term. OEM cost can change, hence prices for contract extension period should be as per mutual agreement reflecting market rates. Request relaxation on this clause.	Please be guided by the RFP
550	136	13.2 Right to Alter quantities	13.2 Right to Alter quantities	The bank reserves the right, at the time of award of contract and/or during the currency of the contract, to increase or decrease the quantity of goods, licenses, subscriptions, appliances, equipment, services, implementation effort, support services, or any line item covered under the contract by up to twenty-five percent (25%) of the quantities specified in the RFP/Contract, without any change in the unit prices, terms and conditions, technical specifications, delivery schedule, warranty obligations, support commitments, or any other contractual conditions.	Request to ensure order is placed as per quantity in solution BoQ, as price can change in case reduction in quantity	Please be guided by the RFP
551	142	13.19 Liquidated Damages	13.19 Liquidated Damages	The Bank will consider the inability of the bidder to deliver or install the equipment & provide the services required within the specified time limit as a breach of contract and would entail the payment of Liquidated Damages on the part of the bidder. The liquidated damages represent an estimate of the loss or damage that the Bank may have suffered due to delay in performance of the obligations (relating to delivery, installation, operationalization, implementation, training, acceptance, warranty, maintenance etc. of the proposed solution/services) by the bidder. Installation will be treated as incomplete in one / all the following situations: 1. Non-delivery of any component or other services mentioned in the order 2. Non-delivery of supporting documentation 3. Delivery / availability, but no installation of the components and/or software 4. No integration/ Incomplete Integration 5. Non-Completion of Transition within suggested timeline 6. System operational, but not as per SLA, Timelines and scope of the RFP If the bidder fails to deliver any or all of the products and/or systems and/or services solutions within the time period(s) specified in the Delivery Schedule or installation, the Bank shall, without prejudice to its other remedies under the Contract, deduct from the Contract Price, as liquidated damages, a sum equivalent to 0.5 percent per week or part thereof of Contract Price subject to maximum deduction of 10% of the total contract value, until actual delivery, installation or performance as per related clauses mentioned in RFP. Once the maximum deduction is reached, the Bank may consider termination of the Contract at its discretion. In the event of Bank agreeing to extend the date of delivery at the request of successful bidder(s), it is a condition precedent that the validity of Bank guarantee shall be extended by further period as required by Bank immediately. Failure to do so will be treated as breach of contract.	LD Penalty of 0.5% per week is on the undelivered portion of product/ service, please confirm? Will penalty be on undelivered portion of ACV or TCV?	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
552	144	13.22 Order Cancellation	Termination for convenience	13.22 Order Cancellation Bank's Right to terminate the entire/ unexecuted part of the Purchase Order on Convenience 1) The Bank reserves its right to cancel the entire unexecuted part of the Purchase Order at any time on its convenience without assigning any reason/s whatsoever by giving 'one 'month notice to the other party. 2) In the event of termination of the Agreement for the Bank's convenience, bidder shall be entitled to receive payment for the Services rendered (delivered) up to the effective date of termination.	Request relaxation to exclude termination for convenience. Bidder will have to pay suppliers for Hardware/ Software/ AMC/ ATS for entire contract term. This clause will have significant commercial risk to bidder. In case customer terminates for convenience, Early termination charges for the remainer period should be paid to bidder.	Please be guided by the RFP
553	69	7.10 Solution/Appliance Warranty, ATS and AMC	7.10 Solution/Appliance Warranty, ATS and AMC	The rates quoted by the bidder for hardware, software, subscriptions, licenses, ATS, AMC, and related services shall be applicable on a pro-rata basis for any additional quantities or services procured by the Bank during the contract period.	Prices can change based on market prices within 5.5 years contract term. Bidder cant agree for price protection for incremental orders as OEMs wont provide any cost protection.	Please be guided by the RFP
554	7	1 KEY INFORMATION	1 Key Information	180 days from the date of opening of the bid.	Request bid validity to be reduced to 30 days due to fluctuating CPE prices based on present Geopolitical situations.	Please be guided by the RFP
555	116	11 PAYMENT TERMS	11 Payment Terms	Product License Cost Payment Schedule	Request to relax, payment to be offered one time in advance, net 30 days	Please be guided by the RFP
556	116	11 PAYMENT TERMS	11 Payment Terms	Subscription Cost (One time license Cost)	Request to relax, payment to be offered 100% on license activation.	Please be guided by the RFP
557	117	11 PAYMENT TERMS	11 Payment Terms	OEM Services Cost	Request to relax, payment to be offered one time in advance, net 30 days	Please be guided by the RFP
558	117	11 PAYMENT TERMS	11 Payment Terms	Hardware Cost including appliance	Request to relax, payment to be offered 100% on Hardware delivery.	Please be guided by the RFP
559	118	11 PAYMENT TERMS	11 Payment Terms	ATS/ Annual Subscription & Appliance AMC Cost	Request to relax, payment to be offered, one time in advance for 5-year support.	Please be guided by the RFP
560	32	7.1	IT Security & Solution	4. Security tools, agents, collectors, and connectors shall also be deployed in the Bank's cloud/VPC environment, wherever applicable, to ensure consistent visibility, monitoring, logging, and protection across cloud and on-premises infrastructure	Request Bank to confirm, who will deploy these in Bank's Cloud/VPC environment as SOC/SIEM is managed by BANK with their IT/Partner team.	Deployment of components forming part of the proposed solution shall be the responsibility of the bidder/OEM in line with the terms of the RFP and defined RACI. The Bank shall provide required access, connectivity and coordination subject to its security controls.
561	32	7.1	IT Security & Solution	7. All proposed solutions shall support real-time integration, event correlation, orchestration, and automated response capabilities to enable unified security operations and effective threat management.	Request Bank to confirm on the existing SOC/SIEM solution	The Bank may have existing centralized security monitoring capabilitie and additionally is in process of procuring the new NEXTGEN SOC. Relevant integration related details shall be shared with the successful bidder during detailed design. The bidder shall ensure interoperability with the Bank-designated security operations architecture.
562	32	7.1	IT Security & Solution	8. The proposed solutions shall provide dynamic, customizable dashboards and reports with analytical and actionable insights for effective monitoring, governance, and decision-making	Request Bank to confirm, if there is any existing solution present at the BANK for dashboarding or any specific solution is desired from the bidder to be considered as part of dynamic dashboard.	Native dashboards required for each proposed solution shall be provided by the respective solution.
563	51	7.4	Bidder Responsibilities	11. Support periodic review, perform fine-tuning, patch management, firmware upgrades, and signature/database updates during support period.	To manage the patches, is there any existing Patch Management software or need to consider in the solution.	The bidder shall perform patch management for the solutions within its scope using the applicable Bank-provided or solution-native mechanisms.
564	52	7.5	OEM Responsibility	17. Remediation of identified VAPT & Audit gaps related to the Configured solution.	Request Bank to confirm who will perform the VAPT and provide the report.	VAPT shall be conducted by bank security team in accordance with the Bank's security assessment process. The Bank may nominate/appoint the VAPT agency. The bidder/OEM shall provide all required support and remediate findings attributable to the proposed/configured solution.
565	52	7.5	OEM Responsibility	18. Ensure compliance with Bank security policies, regulatory requirements, and applicable industry standards	As per Regulatory if any new Security solution required the if will be cost to Bank as new solution otherwise need to clear that we are talking only for the mention product as per the same RFP.	New Regulatory changes, Any new or revised regulatory requirement introduced after the Bid Submission Date, required to maintain compliance with applicable requirements and supported by the existing contracted/licensed solution functionality shall be provided without additional cost. Where compliance with a new or subsequently introduced regulatory requirement requires a new product, module, additional license, or functionality that was not specified or envisaged in the RFP/Guidelines and was not available or communicated to bidders as of the bid submission date, such requirement may be processed through the applicable Change Request (CR) mechanism, subject to the Bank's approval. The bidder shall not treat configuration changes, upgrades, patches, or enhancements that are within the existing contracted/licensed functionality as a new module or additional license merely on account of a subsequent regulatory change.

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
566	NA	NA	Additional	Terms & Conditions	Please confirm if which T&Cs will prevail. RFP or GEM T&Cs	The terms and conditions of the RFP, including subsequent pre-bid clarifications/modifications issued by the Bank, shall prevail. The GeM General Terms and Conditions shall apply to the extent they are not inconsistent with the provisions of the RFP. However, the applicable GeM General Terms and Conditions, policies and mandatory guidelines shall prevail to the extent mandatorily applicable under the GeM framework.
567	52	7.5	OEM Responsibility	20. Bidder is also required to factor the highest-level support from the solution OEM during the O&M, warranty, ATS & AMC phase, respective solution OEM is to be involved every year during the O&M phase for performing the configuration, rules and parametrization review along with the solution architecture review at all the environment of PSB.	Request bank to confirm, if they are expecting, OEM Professional services for Annual Review for the duration of the overall contract period from the respective OEM's	Yes. Annual OEM involvement for configuration, rules, parametrization and architecture review shall be provided for the applicable solutions as specified in the RFP. The bidder shall factor the associated cost.
568	52	7.5	OEM Responsibility	21. Any requirements from the Bank for customization, enhancement and other device/solution administration-related activity required in the supplied solutions to deliver seamless, fully functional integration, custom and native parsers, connectors, incidents management and related workflows, native and custom playbooks, alerts fine-tuning, notifications, dashboards, reporting, customization of default templates, additional remediation efforts etc. shall be undertaken by the Bidder at no cost to the Bank during the Contract period, even in case of extension of timelines for the commission of IT Security due to any reason and such extension would be at the sole discretion of the Bank	Request Bank to confirm, what customization & enhancement is expected from the Bidder or an example can be provided for the same, as the SOC/SIEM is managed by the BANK IT/Partner Team	The requirement primarily covers solution-specific configuration, integration, connectors, parsers, workflows, dashboards, notifications, tuning and administration required to make the proposed solution fully operational and integrated. Central SOC/SIEM use-case ownership shall be discussed with the respective solution OEM and selected bidder during the SRS stage
569	57	7.5.4	Development and Installation - Activities are to be performed by Respective Solution OEM (supported by bidder)	2. The bidder and respective OEM shall integrate the proposed solution with the Bank's ITSM, SLA Monitoring, monitoring, logging, authentication, and other enterprise platforms, as required.	Please confirm the ITSM tool name and details.	ITSM - Manage Engine
570	58	7.5.5	Documentation - Activities are to be performed by Respective solution OEM (supported by bidder)	14. The Secure Configuration Documents (SCDs) and Baseline Hardening Standards for all in scope solutions shall be reviewed at least quarterly, updated as required, maintained under version control, and submitted to the Bank for review and approval.	Request Bank to confirm, if they are desiring, OEM PS services quarterly for the hardening activity throughout the contract period.	Quarterly review and update of SCDs and hardening standards is part of the recurring service requirement. The bidder/OEM shall provide the necessary technical expertise as part of the contracted scope.
571	61	7.5.8	Training- Activities are to be performed by Respective solution OEM (supported by bidder)	The bidder and respective OEMs shall provide comprehensive product training, knowledge transfer, and certification programs for the Bank's IT and Information Security personnel at no additional cost	Request Bank to confirm, if the training for beginner, advance, backend will be needed to be done VITRUALLY or Physically. If Physical at which location ?	Training may be conducted through physical, and/or hybrid mode as decided by the Bank. Physical sessions, where required, shall be conducted at the Bank-designated location(s) in Delhi NCR (Bank shall share the address with the successful bidder).
572	69	7.10	Solution/Appliance Warranty, ATS and AMC	3. Warranty period for hardware/appliance and software support shall commence from the date of Go-live of the respective solution.	OEM Start billing from Day-1, Bank needs to modify the comment because OEM will not support.	Support/warranty commencement shall remain governed by the RFP. The bidder shall ensure OEM support during implementation, testing and Go-Live activities necessary for successful deployment.
573	76	7.12	Facilities Management	Bidder should manage, monitor, maintain and upgrade all proposed solutions & services on ongoing basis encompassing all deployed hardware/ firmware/ middleware / software components by performing timely backups, continuous health monitoring, on-site and offsite support, troubleshooting, critical functional and performance bug fixes, all major product/feature enhancements within the warranty and AMC charges and as per the SLA defined by the Bank.	We understand from the software related upgrades, however request Bank to confirm on upgrade of the Hardware component, will be a mutual discussion during the contract period for purchase, procurement and migration of the configuration etc	Please be guided by the RFP
574	77	7.12	7.12 Facilities Management	11. Conduct DR drill of the Security on quarterly interval or as and when required by the Bank. Ensure DC & DR are exact replica of each other in every manner.	Request Bank to confirm the time duration for which the DR will be operational, to understand the DC vis-à-vis DR Solutioning to be done for all the components	DR shall be capable of supporting the Bank's approved BCP/DR requirements and applicable RTO/RPO. Detailed DR activation duration and drill procedures shall be finalized during DR design and shall not reduce the resilience requirements specified in the RFP.
575	78	7.12	7.12 Facilities Management	29. Review onsite & offsite users as per Segregation of Duties (SoD) like their roles & responsibilities, access level / rights in the proposed technologies and other related onsite / offsite systems etc. on periodic basis and deactivate / modify user access etc. as per requirement with prior approval from the Bank.	Request Bank to confirm, who are these Offsite user's, when there is no remote access permitted to the environment as part of the other RFP clause	“Offsite users” refers to authorized personnel who may be required to support or administer the environment from locations other than the primary Bank premises through Bank-approved controlled access mechanisms. Such access shall remain subject to the Bank's security policy; the clause does not mandate unrestricted remote access.

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
576	78	7.12	7.12 Facilities Management	38. An automated workflow should be created and maintained for proposed solutions change management initiation, verification, approval, implementation and post-implementation verification.	Request Bank to confirm, if they have any automated workflow tool or an additional tool needs to be considered by the bidder as part of the solution	The Bank's designated ITSM/change-management platform shall be used wherever available. The bidder shall configure the required workflows within the designated platform where such capability exists.
577	79	7.12	7.12 Facilities Management	41. Bidder & OEMs should engage data scientists for analytics, statistical models, configuring the systems for supervised & unsupervised learning leveraging AI / ML minimizing the false positives and in developing advanced analytics use cases without any additional cost to the bank.	Request Bank to confirm, is Data Scientist needed as part of the on-prem resource. If yes, what will be the time duration and contract duration for the Data Scientist	A separate full-time onsite resource is not mandated in the minimum resource table; however, adequate SME support shall be available throughout the applicable service period.
578	80	7.12.1	Continual Improvement	13 ©. Providing tools for creating knowledge repository for the bugs identified, resolution mechanism, version upgrade, future upgrade etc. of Application software, tools, OS, RDBMS, application server software, web server software, interfaces, integrations, customization, reports etc.	Request Bank to confirm, if they have any Knowledge Management Tool or the bidder needs to consider any tool as part of the solution	The Bank's designated knowledge-management/ITSM platform shall be used where available. The bidder shall provide and maintain the required knowledge content, documentation and solution-specific repository within the agreed platform.
579	80	7.12.1	Continual Improvement	d. Provision should be available for version control and restoring the old versions if required by BANK	Request Bank to confirm, if they have any Backup tool or do bidder need to consider a tool to achieve this scope.	Bidder to propose the backup tool meeting therequirement specified in the RFP
580	80	7.12.1	Continual Improvement	16. Immediate bug fixing should be undertaken in the event of software failure causing an interruption of operation as per the response / resolution times defined by BANK. In case of any software /hardware /network failure, the solution should continue to function seamlessly.	Bank agrees that Big Fixes are dependent on the OEM release for the BUG Fixes and timeline for the same will be OEM dependent. Please confirm.	The Bank agrees that the availability of a permanent software bug fix/patch may be dependent on the respective OEM's release cycle. However, such dependency shall not relieve the Bidder/OEM from its obligations towards incident response, service restoration and resolution within the SLA timelines specified by the Bank. Where a permanent bug fix is not immediately available from the OEM, the Bidder/OEM shall, wherever technically feasible, provide an appropriate temporary workaround or compensating control, including virtual patching, to mitigate the identified vulnerability/defect and maintain secure and continuous operation of the solution.
581	80	7.12.1	Continual Improvement	26. Update, or provide the information required for BANK to update the asset management with BANK	Request bank to confirm, which is the assets management tool currently present with the BANK	ITSM - Manage Engine
582	82	7.12.3	IT Security Operations	Complete Section	Section appears to be overall similar to facilities management, what is the expectation by the bank in general	IT Security Operations covers operational management of the proposed security solutions, including monitoring, alert/event handling, configuration, tuning, incident support, health monitoring, reporting, integration and security administration, while FM covers technology maintenance and lifecycle activities.
583	27	Scope of work	RFP document	SSL Orchestrator along with packet broker	I will request please ask three seprate solution SSL orchestrator, HSM and Packet broker sepeartly. Not combined solution.	Please be guided by the RFP
584	205	15.21.2	RFP document	Existing IT Security Solution Details	Kindly suggest support availble of existing solution.	Details shall be shared with the Successful bidder.
585	203	15.21	RFP document	Non-Production Environment	Do we need to consider non-prodction for entire solution. Kindly suggest minimum licences required to consider against each solution or bidder is free to design non-prod environment. Please confirm.	Please refer Annexure 21: Non Production Environment For appliance-based solutions, the bidder shall design and propose an appropriate non-production environment to support testing, validation, upgrades, patching, configuration changes, policy tuning, rule testing, and other activities during the contract period without impacting production services. For VM-based solutions, the non-production environment shall be sized at a minimum of 10% of the Production (DC) environment unless otherwise specified in the RFP.

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
586	Page no 104	10.2 Eligibility Evaluation criteria	OEM Evaluation criteria	The proposed OEM solution/product should have been successfully implemented in least two Scheduled bank (including financial regulators). The reference implementation need not be of the same model, version, or product family as the proposed solution. Copy of Purchase Order/Work Order/ Contract List of Product which is required to comply with the above clause 1. Anti-Distributed Denial of Services (Anti-DDoS) 2. SSL Orchestrator along with packet broker 3. DNS protection (Internal DNS Security) 4. Web Gateway 5. Zero-Day Attack Protection at Endpoint and network 6. Zero Trust Network Access (ZTNA) 7. Data Loss Prevention (DLP) 8. Information/Digital Right Management 9. Mobile SDK 10. Host IPS including Application Change Control (HIPS) 11. Web Application Firewall (WAF) 12. Centralized key management solution 13. Certificate Lifecycle management 14. Database Access Management (DAM) 15. Identity & Access Management Solution 16. Multi Factor Authentication 17. DNS Security Services (Internet-Facing DNS Security Services)	Please amend the clause as: The proposed OEM solution/product should have been successfully implemented in least two Scheduled bank (including financial regulators)/ PSU/ Government.	Please be guided by the RFP
587	Page no 21	Appendix 1-A Zero Day attack	1	Solution must be able to handle minimum of 10 Gbps of traffic capacity.	Please amend the clause as: he solution must be capable of handling a minimum traffic capacity of 35 Gbps or supporting analysis of a minimum of 35,000 unique/zero-day files per day, whichever is applicable to the proposed deployment architecture. Justification: The existing perimeter firewall supports approximately 35 Gbps bandwidth; therefore, the inline security solution should support equivalent capacity to avoid becoming a network bottleneck. Alternatively, 35,000 unique/zero-day files per day may be considered for OEMs that size their solution based on file-analysis capacity, ensuring adequate threat-analysis capability.	Please be guided by the RFP, bank has provided the minimal requirement
588	Page no 21	Appendix 1-A Zero Day attack	12	Solution must generates analysis reports, suspicious object lists, PCAP files, and OpenIOC and STIX files that can be used in investigations	Please amend the clause as: Solution must generates analysis reports, suspicious object lists/ Risky object, Embedded Objects, PCAP files, and OpenIOC or STIX IOC files that can be used in investigations. give changes request justification in small Justification: To provide more comprehensive investigation and threat-hunting capabilities, the requirement is expanded to include Risky Objects and Embedded Objects, which provide additional visibility into suspicious components identified during analysis. “OpenIOC and STIX” is changed to “OpenIOC or STIX” to accommodate different OEM-supported threat-intelligence formats while maintaining investigation requirements.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
589	Page no 21	Appendix 1-A Zero Day attack	19	Should have combination of signature file-based scanning and heuristic rule-based scanning to detect and document exploits & threats used in targeted attacks including Detection of zero-day threats, Detection of embedded exploit code, Detection rules for known vulnerabilities and Enhanced parsers for handling file deformities	Please amend the clause as: Should have combination of signature file-based scanning and heuristic rule-based scanning to detect and document exploits & threats used in targeted attacks including Detection of zero-day threats, Detection of embedded exploit code/ URLs, QR codes, and images, Detection rules for known vulnerabilities and Enhanced parsers/ analysis for handling file deformities. Justification: The requirement is enhanced to include detection of embedded URLs, QR codes, and images to address modern attack techniques such as malicious links, QR-code-based phishing, and image-based threats, providing more comprehensive protection against evolving targeted attacks.	Please be guided by the RFP
590	Page no 21	Appendix 1-A Zero Day attack	22	The proposed solution should be able to detect lateral movement (East-West) of the attack without installing agents on endpoint/server machines with least 100+ protocols for inspection.	Please amend the clause as: The proposed solution should be able to detect lateral movement (East-West) of the attack passing through the firewall without installing agents on endpoint/server machines with least 90+ protocols/ files types and ability to create custom file type for inspection. Justification: The requirement is revised from 100+ protocols to 90+ protocols/file types to align with the solution's actual inspection capabilities while maintaining broad threat visibility. Custom file-type creation is additionally included to support inspection of emerging or organization-specific file formats, ensuring future scalability without unnecessarily restricting the solution based on a fixed protocol count.	Please refer Addendum 1 for the revised clause.
591	Page no 21	Appendix 1-A Zero Day attack	23	The Proposed solution should monitor Inter-VLAN traffic on a Port Mirror Session/TAP mode.	Please amend the clause as: The system should be able to support file sizes upto 1 Gb or more. Justification: Inter-VLAN traffic monitoring through Port Mirror/TAP has already been covered under the overall network security architecture; reiterating it in the Sandbox requirement is therefore redundant. The requirement is revised to ensure the Sandbox can analyze files up to 1 GB or more when uploaded by users or received through network traffic, which is directly relevant to detecting malware and advanced threats within large files.	Please be guided by the RFP
592	Page no 21	Appendix 1-A Zero Day attack	26	Proposed Sandboxing should use static, heuristic and behavior analysis, web, and file reputation, to detect ransomware and advanced threats	Please amend the clause as: Proposed Sandboxing should use static, heuristic and behavior analysis, web, and file reputation /IOC Enrichment, to detect ransomware and advanced threats Justfication: IOC Enrichment is added to strengthen threat detection by correlating sandbox findings with known indicators of compromise (IOCs), threat intelligence, and contextual information. This provides better identification and validation of ransomware and advanced threats beyond file reputation alone.	Please be guided by the RFP
593	Page no 21	Appendix 1-A Zero Day attack	29	The proposed solution should be able to run at least 50 parallel sandboxes for analysis of payload and on premise customized sandbox solution should have the capability to allow manual submission of suspicious files for analysis	Please amend the clause as: The proposed solution should be able to run at least 25 parallel sandboxes for analysis of payload and on premise customized sandbox solution should have the capability to allow manual submission of suspicious files for analysis Justification: The requirement is proposed to be reduced from 50 to 25 parallel sandboxes, as the solution is expected to process approximately 35,000 files per day. With appropriate queue management and workload distribution, 25 concurrent analysis instances provide sufficient processing capacity without unnecessarily over-sizing the infrastructure. This also ensures a cost-effective and practical deployment while maintaining adequate analysis performance.	Please refer Addendum 1 for the revised clause.

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
594	Page no 21	Appendix 1-A Zero Day attack	37	The proposed solution should support on premise centralized management for viewing information about detections	Please amend the clause as: The proposed solution should support on premise centralized management or Dasboard for viewing information about detections. Justification: The requirement is revised to allow centralized management or dashboard-based visibility, providing flexibility for solutions where detection information is natively presented through a dedicated security dashboard rather than a separate centralized management platform. This avoids unnecessarily restricting the requirement to a specific deployment architecture while retaining centralized visibility	Please refer Addendum 1 for the revised clause.
595	Page no 21	Appendix 1-A Zero Day attack	40	Solution should be able to centrally manage and deploy product updates including patches, hotfixes, and firmware upgrade	Please amend the clause as: Solution should be able to centrally manage and deploy product updates including Licenses, security update, Query DB, patches. Justification: The requirement is expanded to include licenses, security updates, and Query DB updates, as these are essential for maintaining the solution's detection accuracy, functionality, and security posture.	Please be guided by the RFP
596	Page no 21	Appendix 1-A Zero Day attack	41	Solution should be able to centrally manage and deploy sandbox image update to managed products.	Please amend the clause as: The proposed solution should have the ability to be deployed in out-of-band mode (also SPAN/TAP) & inline mode with perimeter Firewall Justification: The requirement is revised to specify deployment modes (Inline and Out-of-Band/SPAN/TAP), which are critical to the Sandbox architecture and operational flexibility. Sandbox image updates are a routine product-management function and need not be separately mandated in this requirement.	Please be guided by the RFP
597	Page no 22	Appendix 1-A Zero Day attack	44	The solution central management should include various methods of sharing threat intelligence data with other products or services including TAXII / Web services.	Please amend the clause as: The solution should include various methods of sharing threat intelligence data with other products or services including TAXII / Web services. Justification: Central management" is removed because threat intelligence sharing is an integration capability and does not necessarily require a centralized management platform. The requirement focuses on the actual interoperability capability through TAXII/Web Services, allowing threat intelligence to be exchanged with other security products and services irrespective of the deployment architecture.	Please refer Addendum 1 for the revised clause.
598	Page no 38	7.3.1.5 Zero-Day Attack Protection at Endpoint and network	7.3.1.5 key Deliverables	Fully deployed Zero-Day Attack Protection at Endpoint and network solution covering both network and endpoint layers	Please clarify for endpoint protection seprate EDR licenses are required	Please refer Addendum 1 for the revised clause.
599	Page no 38	7.3.1.5 Zero-Day Attack Protection at Endpoint and network	7.3.1.5 key Deliverables	Incident response plan including rapid action and forensics procedures	This should be part of SOC infra, as will come under IR services, please remove the same.	Please refer Addendum 1 for the revised clause.
600		Appendix 1-A Zero Day attack		Missing some important functionality	The proposed solution shall incorporate an advanced ML/AI-based execution-less threat detection engine capable of analyzing suspicious files prior to execution. The solution shall use machine learning models trained on extensive malware and cleanware datasets to analyze file structure, embedded content and threat indicators, identify known and unknown malware beyond traditional signature-based detection, and provide rapid verdicts with high detection accuracy. Justification: To ensure the solution can detect known and unknown/zero-day malware before execution using ML/AI-based static analysis, reducing reliance on traditional signatures and preventing malicious files from reaching endpoints or critical systems	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
601		Appendix 1-A Zero Day attack		Missing some important functionality	The proposed solution shall provide a dedicated real-time phishing detection and prevention capability to identify zero-day phishing, credential-harvesting websites and malicious URLs. The solution shall automatically extract and analyze URLs embedded within emails, PDF files and Microsoft Office documents; perform real-time web-page analysis to detect phishing pages, visual impersonation/cloning of legitimate login portals and obfuscated or redirected malicious URLs; and provide proactive blocking of identified phishing sites through integration with the security ecosystem, enabling real-time propagation of phishing indicators and protection across connected security controls. Justification: To provide real-time detection and prevention of zero-day phishing and credential-harvesting attacks, including malicious URLs hidden in emails/documents, and enable rapid blocking and propagation of phishing indicators across the security ecosystem to prevent credential theft and user compromise.	Please be guided by the RFP
602		Appendix 1-A Zero Day attack		Missing some important functionality	The proposed solution shall support automated scanning and analysis of files stored in shared folders, file-sharing repositories and upload portals, including SMB, NFS, public/network shares and supported cloud-storage repositories such as Microsoft OneDrive. The solution shall detect malicious, suspicious and hidden malware within these locations through static, AI/ML and dynamic analysis, and shall support appropriate quarantine or containment actions to prevent malware propagation, lateral movement and insider-threat-related spread across the environment. Justification: To detect and contain malware residing in shared folders, file repositories and cloud storage before it spreads across the environment, thereby reducing the risk of lateral movement, malware propagation and insider-driven threats.	Please be guided by the RFP
603		Appendix 1-A Zero Day attack		Missing some important functionality	The proposed solution shall provide an advanced AI/ML-based adaptive malware analysis engine with heuristic and signature-based detection, intelligent sandbox resource optimization, parallel execution across multiple virtual environments, extraction and analysis of embedded files, URLs, QR codes and images using OCR, support for third-party YARA rules, cloud-based malware reputation queries, configurable file checksum allowlisting/blocklisting, email and file-based URL scanning, and intelligent VM utilization for efficient and accurate threat analysis. Justification: To enhance malware detection accuracy and analysis efficiency by combining AI/ML, heuristic, signature and sandbox techniques, while enabling analysis of embedded content, URLs, QR codes and images and supporting YARA/reputation-based detection for improved identification of sophisticated and zero-day threats.	Please be guided by the RFP
604	Page no 24	Appendix 1-A ZTNA	26	Solution should support extensive coverage with in-built Data types like Aadhar card, PII, etc with different File Types etc. Solution should support extensive coverage with 100+ in-built Data types with minimum 200 File Types.	Please amend the clause as: Solution should support extensive coverage with in-built Data types like Aadhar card, PII, etc with different File Types etc. Solution should support extensive coverage with 100+ in-built Data types with minimum 70 File Types. Justification: This maintains the required broad DLP coverage for PII/sensitive data while keeping the requirement practical, OEM-neutral, and functionally relevant rather than relying on an arbitrary file-type count.	Please refer Addendum 1 for the revised clause.

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
605	Page no 24	Appendix 1-A ZTNA	26	The ZTNA solution should have device posture validation across multiple parameters like Device Encryption, Registry Check, Process Check, AD Domain Check, OPSWAT and Certificates etc. to provide specific URL or Internet Access based on granular policy controls. The device posture check should be recurring and check the compliance of the posture periodically to maintain the Device Trust.	Please amend the clause as: The ZTNA solution should have device posture validation across multiple parameters like Device Encryption, Registry Check, Process Check, AD Domain Check and Certificates etc. to provide specific URL or Internet Access based on granular policy controls. The device posture check should be recurring and check the compliance of the posture periodically to maintain the Device Trust. Justification: OPSWAT is an OEM and not an antivirus vendor, please remove the same.	Please refer Addendum 1 for the revised clause.
606	Page no 23	Appendix 1-A ZTNA	11	The solution should provide the capability to add any number of App Connectors in DC without any additional price or license.	Please amend the clause as: The solution should provide the capability to add any number of App Connectors in DC without any additional price or license or The solution should not have seprate user based licenses for the private access it should should be part of the internet access user based licenses. Justification: The requirement is revised to remove the restriction based on the number of applications, ensuring that the SASE solution can scale as new private applications are onboarded without additional licensing limitations. This provides greater deployment flexibility and future scalability, while avoiding a licensing model tied to application count	Please refer Addendum 1 for the revised clause.
607	Page no 39	7.3.1.6 Zero Trust Network Access	Point no 6 Key Deliverables:	Discovery report of internal applications identified by AI/ML engine for policy mapping	Please amend the clause as: Discovery report of internet/Internal AI applications identified by AI/ML engine for policy mapping. Justification: Since shadow AI application detection is important and which will help in the efficient policy mapping for the users.	Please be guided by the RFP
608				Missing some important functionality	ZTNA Platform must be able to provide Browser Security for all the browsers such as Edge, Chrome or Firefox Justification: To ensure secure browser-based access to applications across commonly used browsers such as Microsoft Edge, Google Chrome and Mozilla Firefox, providing consistent protection against web-based threats, unauthorized access and data leakage without impacting user productivity.	Please be guided by the RFP
609				Missing some important functionality	Browser Security must be capable of allowing or denying traffic based on URL/URL Category. Justification: To enable granular web access control by allowing or blocking traffic based on specific URLs and URL categories, thereby preventing access to malicious, risky or unauthorized websites and reducing web-based security threats.	Please be guided by the RFP
610				Missing some important functionality	Browser Security must be capable of detecting malicious files when users are downloading files from the Internet/Intranet justification: To provide real-time protection against malicious downloads by inspecting files accessed from both Internet and Intranet sources, helping prevent malware, ransomware and other file-based threats from reaching user endpoints.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
611				Missing some important functionality	Browser security must provide visibility and control of risky extensions installed in browsers. Justification: To identify and control risky or unauthorized browser extensions that may introduce security vulnerabilities, enable data leakage, or compromise user credentials and sensitive information.	Please be guided by the RFP
612				Missing some important functionality	Browser Security must provide ability to restrict clipboard action and upload/download for specific destinations Justification: To prevent data leakage and unauthorized data transfer by controlling clipboard operations and restricting file uploads/downloads to specific destinations, based on security policies and business requirements.	Please Refer addendum 1 for the revised Clause
613				Missing some important functionality	Should have the ability to extract diagnostic endpoint logs on-demand from the admin console Justification: To enable centralized, on-demand troubleshooting and incident investigation by allowing administrators to quickly collect endpoint diagnostic logs from the management console without requiring manual intervention on user devices.	Please be guided by the RFP
614						Please be guided by the RFP
615						Please be guided by the RFP
616				Missing some important functionality	Should have the ability to apply DLP policies to the SPA traffic with the following features: (i) Predefined DLP dictionaries (ii) Support for DLP Exact Data Matching (EDM) and Indexed Document Matching (IDM) with DLP fingerprinting (iii) Blocking files with Microsoft Purview Information Protection (MPIP) sensitivity labels Any additional license for this feature should be included on Day 1. Justification: To provide inline DLP protection for SPA traffic and prevent unauthorized exposure or exfiltration of sensitive data using predefined dictionaries, EDM/IDM fingerprinting and Microsoft Purview sensitivity-label-based controls, ensuring data protection from Day 1 without additional licensing gaps.	Please Refer addendum 1 for the revised Clause
617				Missing some important functionality	The solution shall provide inline Cloud Access Security Broker (CASB) capabilities with visibility and granular control over SaaS application access, usage, and data Justification: To provide visibility and granular control over SaaS applications, enabling the organization to identify risky cloud usage, enforce access policies, and prevent unauthorized application access and sensitive data leakage.	Please be guided by the RFP
618				Missing some important functionality	The solution shall provide security controls for Generative AI applications, including visibility into GenAI usage, identification of sanctioned and unsanctioned AI applications, and enforcement of organizational security policies. Justification: To provide visibility and control over Generative AI usage, enabling identification of sanctioned/unsanctioned AI applications and enforcement of security policies to reduce data leakage, unauthorized AI usage, and emerging GenAI-related risks.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
619				Missing some important functionality	The solution shall inspect GenAI application traffic in real time and enforce Data Loss Prevention (DLP) policies to prevent sensitive, confidential, or regulated information from being submitted to unauthorized Generative AI applications. Justification: To prevent sensitive or regulated data leakage through Generative AI applications by inspecting GenAI traffic in real time and enforcing DLP policies, thereby controlling unauthorized submission of confidential information to AI services.	Please be guided by the RFP
620				Missing some important functionality	The solution shall provide granular policy controls for Generative AI applications such as ChatGPT, Copilot, Claude, Grok, and more, enabling organizations to allow, restrict, or block access based on users, groups, applications, destinations, and organizational security policies. Justification: To provide granular control over Generative AI applications, allowing organizations to permit, restrict, or block AI services based on users, groups, applications, and destinations, thereby reducing unauthorized AI usage, data leakage, and compliance risks.	Please be guided by the RFP
621	36	Appendix 1-A WAF	14	The proposed solution must support dedicated 5 Gbps of WAF throughput (HTTP/HTTPS). The bidder must provide evidence of throughput through publicly available documents /evidence based document supporting the same which needs to be submitted along with the proposal and same needs to showcased if asked by bank during Presentation & UAT (Undertaking from the OEM is not accepted in this case).	Please amend the clause as: The proposed solution must support dedicated 2.5 Gbps of WAF throughput (HTTP/HTTPS). The bidder must provide evidence of throughput through publicly available documents /evidence based document supporting the same which needs to be submitted along with the proposal and same needs to showcased if asked by bank during Presentation & UAT (Undertaking from the OEM is not accepted in this case). Justification 2.5 Gbps provides adequate headroom for the expected web application traffic while maintaining performance and security controls	Please be guided by the RFP
622	36	Appendix 1-A WAF	25	The solution must provide the following features and protection. - Web service layer correlated attack validation - HTTP protocol attack signatures - Web service layer customized protection - Cookie signing validation - Anti site scrapping - Web profile protection - Web worm protection - Web application attack signatures - Web application layer customized protection - OCSP protocol validation	Please amend the clause as: The solution must provide the following features and protection. - Web service layer correlated attack validation - HTTP protocol attack signatures - Web service layer customized protection - Cookie signing validation - Anti site scrapping - Web profile protection - Web worm protection - Web application attack signatures - Web application layer customized protection - OCSP protocol validation - CAPTCHA challenge/Device Fingerprinting Justification: The requirement is enhanced to include CAPTCHA challenge and Device Fingerprinting, which provide additional protection against automated bots, credential attacks, scraping, and abusive application traffic. These controls complement the existing WAF protections by enabling identification and validation of legitimate users/devices beyond signature-based attack detection	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
623	38	Appendix 1-A WAF	70	System should protects against the following threats: • SQL injection • Cross-site scripting (XSS) • Cross-Site-Request-Forgery (CSRF) • Parameter tampering • Hidden-field manipulation • Session manipulation • Cookie poisoning • Cookie protection • Remote file inclusion • Buffer overflow • Stealth commanding • Backdoor and debug options • Application-buffer-overflow attacks • Brute-force attacks • Data encoding • Unauthorized navigation • SOAP- and Web-services manipulation • Web Scraping	Please amend the clause as: System should protects against the following threats: • SQL injection • Cross-site scripting (XSS) • Cross-Site-Request-Forgery (CSRF) • Parameter tampering • Hidden-field manipulation • Session manipulation • Cookie poisoning • Cookie protection • Remote file inclusion • Buffer overflow • Backdoor and debug options • Application-buffer-overflow attacks • Brute-force attacks • Data encoding • Unauthorized navigation • SOAP- and Web-services manipulation • Web Scraping Justification: "Stealth commanding" is proposed for removal as it is not a commonly defined, independently measurable WAF threat category and may overlap with existing protections such as command injection, application-layer attack signatures, and behavioral controls. Removing it avoids ambiguity while retaining effective protection against the underlying attack techniques.	Please be guided by thr RFP
624	38	Appendix 1-A WAF	77	The solution should be able to block even the most advanced bots that try to emulate standard client behavior and pretend to be web browsers.	Please amend the clause as: The Solution should have following Anti-Bot Mechanisms. - Bot Deception: Provides a deception technique to identify bots. It inserts a hidden link into response pages. Clients that fetch the URL can accurately be classified as bots - Biometrics Based Detection: Verify whether a client is a bot by monitoring events such as a mouse movement, keyboard, screen touch, and scroll, etc - Threshold Based Detection: Default rules to identify various scan types using thresholds such occurrence, time period, etc Mobile Application Identification: The solution must support rnechanisms to identify and validate legitimate mobile application traffic that cannot execute JavaScript or CAPTCHA. Justification: The clause is amended to define specific Anti-Bot detection mechanisms rather than requiring only a generic capability to block advanced bots. The proposed mechanisms—Bot Deception, Biometrics-Based Detection, Threshold-Based Detection, and Mobile Application Identification—provide measurable and comprehensive controls for detecting sophisticated automated traffic while ensuring legitimate mobile applications are not incorrectly blocked.	Please be guided by the RFP
625	38	Appendix 1-A WAF	81	The client component (JavaScript) should be downloaded from the same domain as the application (first party). It is not allowed to use external locations to upload the script.	Kindly delete the same: This requirement can be deleted because it is implementation-specific and unnecessarily restricts the WAF architecture. Modern WAFs may use JavaScript security/client-side protection mechanisms where scripts are hosted, injected, or delivered through vendor-controlled infrastructure, CDN, or other secured locations.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
626	39	Appendix 1-A WAF	82	Identification should be implemented with the accuracy of the web browser. The result of the identification should be the establishment of a session with the browser, which will authorize further communication.	Please amend the clause as: Identification / Bot verification should be implemented with the accuracy of the web browser. The result of the identification should be the establishment of a session with the browser, which will authorize further communication. justification: The requirement is clarified by adding “Bot verification” to explicitly cover the validation of whether the identified browser/client is legitimate or automated. This provides clearer and more measurable anti-bot protection while retaining the existing browser session authorization requirement.	Please be guided by the RFP
627	39	Appendix 1-A WAF	83	The solution should allow the definition of specific endpoints which are crucial for the application, which will be accessible only after previous identification and application of policies. Sending a request to such an endpoint without prior identification should result in immediate block of the request and redirecting the client to the website which will initiate the identification.	Please amend the clause as: The solution should allow the definition of specific endpoints which are crucial for the application, which will be accessible only after previous identification / Bot verification and application of policies. Sending a request to such an endpoint without prior identification / Bot verification should result in immediate block of the request and redirecting the client to the website which will initiate the identification / Bot verification. Justification: The requirement is amended to include Bot Verification alongside identification, as different OEMs may use different terminology for equivalent client-validation mechanisms. This makes the requirement OEM-neutral while ensuring the underlying capability of verifying legitimate users/browsers and preventing unauthorized or automated access to critical application endpoints is retained.	Please be guided by the RFP
628	39	Appendix 1-A WAF	86	The system should provide the ability to apply the following actions against traffic classified as BOT: · blocking · monitoring · displaying a captcha	Please amend the clause as: The system should provide the ability to apply the following actions against traffic classified as BOT : · blocking · monitoring · displaying a captcha · Bot verification · Period Block Justification: The terminology is amended to accommodate anti-bot controls.	Please be guided by the RFP
629	39	Appendix 1-A WAF	87	The manufacturer should manage some of the conditions (lists) that can be easily placed in the policy, including: · Social Media Bots · Search Engines bots · Aggregator User Agents · CSPs (expected lack of client traffic)	Please amend the clause as: The manufacturer should manage some of the conditions (lists) that can be easily placed in the policy, including: · Social Media Bots · Search Engines bots · Aggregator User Agents/ Crawlers/ Feeders · CSPs (expected lack of client traffic) Justification: The terminology is expanded to include “Crawlers/Feeders” alongside Aggregator User Agents to accommodate different OEM classifications and naming conventions for automated traffic. This makes the requirement OEM-neutral while retaining the intended capability to identify and control automated traffic sources.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
630	39	Appendix 1-A WAF	96	The WAF solution should be capable to store all logs for at least one month on appliance itself. Bidder to enusre that bidder right size the same. Bidder to submit the detailed calculation of Hard Disk and RAM requirement to meet the bank RFP ask of storage on-appliance and Response along with any bottleneck mitigation and SLA compliance. If any stage the same is observed bidder is required to provide the additional hardware/component to mitigate the same at no additional cost to the bank	Please amend the clause as: The solution should be capable to store all logs for at least one month on logging applaince. Bidder to enusre that bidder right size the same. Bidder to submit the detailed calculation of Hard Disk and RAM requirement to meet the bank RFP ask of storage on-appliance or logging solution and Response along with any bottleneck mitigation and SLA compliance. If any stage the same is observed bidder is required to provide the additional hardware/component to mitigate the same at no additional cost to the bank	Please be guided by the RFP
631				Missing some important functionality	The solution should be able to secure gRPC API traffic with a variety of security controls such as signature scan, rate limiting, payload limiting, obscuring sensitive data. It should also be able to secure gRPC for mutual TLS authentication verifying Server & Client certificates Justification: As the application is expected to migrate to HTTP/2.0, support for gRPC and HTTP/2.0 security is required to ensure continued protection of application traffic, including mutual TLS authentication, signature inspection, rate limiting, payload control, and sensitive-data protection.	Please be guided by the RFP
632				Missing some important functionality	The solution should be able to secure gRPC API traffic with a variety of security controls such as signature scan, rate limiting, payload limiting, obscuring sensitive data. It should also be able to secure gRPC for mutual TLS authentication verifying Server & Client certificates Justification: As the application is expected to migrate to HTTP/2.0 and adopt gRPC-based communication, this capability is required to secure gRPC/API traffic through signature scanning, rate and payload limiting, sensitive-data protection, and mutual TLS authentication with validation of both client and server certificates.	Please be guided by the RFP
633				Missing some important functionality	The solution must be able to identify WebSocket connections, including those initiated over HTTP 1.1. The WAF should validate the WebSocket handshake request and be capable of applying security inspection (protocol validation, signatures, anomaly detection) to WebSocket traffic after the upgrade.	Please be guided by the RFP
634	1	Appendix 1-A AI Security	AI Security	As per the RFP, the specifications appear to be primarily focused on a SaaS/cloud-based offering, whereas the stated intent appears to be for an on-premises deployment to secure PSB-hosted LLMs. This creates a contradiction in the RFP requirements. Kindly clarify the intended deployment model and provide revised specifications aligned with the requirement for an on-premises AI/LLM security solution	Please clarify the intent of the proposed AI Security Solution—whether the PSB is planning to **deploy/secure on-premises LLMs or is primarily looking for Shadow AI/GenAI detection and control. The current RFP includes several GenAI/Shadow AI functionalities that overlap with capabilities already covered under **CASB, ZTNA, and the previously floated Firewall requirements. If the objective is to secure PSB-hosted/on-premises LLMs, we recommend revising the specifications to focus on AI/LLM Runtime Security, including: * Protection against **prompt injection, jailbreaks and malicious prompts** * **Model poisoning** and model integrity protection * **Unauthorized access** to LLMs and AI applications * **AI API/application security** * **DLP and sensitive-data protection** for prompts and responses * Runtime monitoring, threat detection and security logging * **On-premises deployment** to protect PSB-hosted LLMs and ensure sensitive AI data remains within the PSB environment. Please provide the modified specifications based on the intended use case.	Please refer Addendum 1 for ther revised clause

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
635		Page 15 , Appendix 2 - Bill of Material	Product License Cost (Item 13)	Centralized Key Management Solution (KMS) quantity line item provided with unpopulated baseline quantity.	Bank is requested to clarify the licensing baseline metric for Centralized Key Management (KMS). Please confirm if licensing is calculated based on active Managed Assets / Workloads / Servers (e.g. 2,000 servers) or Application Clients, and confirm the target baseline quantity.	Centralised Key Management: licensing to be provided on an Enterprise-Wide basis. No specific metric (servers/workloads/application clients) or target baseline quantity is prescribed. Bidder shall size and propose licensing to cover the Bank's entire IT environment (on-premise and cloud) requiring key management services, in accordance with the sizing responsibility clause under Annexure 21, accounting for projected growth over the contract period
636		Page 15 Appendix 2 - Bill of Material	Product License Cost (Item 14)	Certificate Lifecycle Management (CLM) quantity line item provided with unpopulated baseline quantity.	Bank is requested to clarify whether CLM software licensing is evaluated based on the number of active SSL/TLS Certificates (e.g. 5,000 certificates) or number of Target Endpoints/Nodes. Please confirm the baseline quantity for commercial pricing.	Certificate Lifecycle Management: licensing to be provided on an Enterprise-wide basis for certificate issuance, provisioning, and management. No specific metric (number of certificates/target endpoints) or baseline quantity is prescribed. Bidder shall size and propose licensing to cover the Bank's entire certificate estate, in accordance with the sizing responsibility clause under Annexure 21, accounting for projected growth over the contract period.
637		Page 24 Appendix 1A - CLM Specification	CLM Clause 7	CLM provider should be a Global CA and Licensed CA authorized agency by CCA, Govt. of India.	Please confirm that an Enterprise Private Certificate Authority (such as HashiCorp Vault PKI Secrets Engine) issuing high-assurance internal SSL/TLS certificates for internal servers, databases, microservices, containers, and VPNs satisfies 100% of internal CLM requirements, while integrating via APIs with external CCA-licensed CAs for public domain certificates.	Please be guided by the RFP
638		Page 22 Appendix 1A - KMS Specification	KMS Clause 18 & Clause 31	The KMS Platform should be able to Integrate with provided HSM to master key in Hardware Root of Trust.	Bank is requested to clarify whether physical FIPS 140-3 Level 3 Hardware Security Module (HSM) hardware appliances are to be supplied by the Bidder, or if existing Bank-owned HSMs (e.g. Thales Luna / Entrust nShield) will be provided for Vault PKCS#11 Auto-Unseal and Hardware Root of Trust.	FIPS 140-3 Level 3 Hardware Security Module (HSM) hardware appliances are to be supplied by the Bidder
639		Page 22 Appendix 1A - KMS Specification	KMS Clause 21 & Clause 24	Protection of data through encryption or tokenization using FIPS 140-2 Level 3 compliant solution and bulk transformation.	Please confirm that HashiCorp Vault Transform Secrets Engine providing Format-Preserving Encryption (FPE - AES-FF1) and Tokenization for sensitive banking data (Credit/Debit Card PAN, Aadhaar, PII) satisfies all application data protection criteria.	Please be guided by the RFP
640		Page 2 Appendix 3 - IT Infrastructure	IAM / PIM / KMS Sizing	IT Infrastructure specs require VM/Server count, CPU cores, RAM, and Storage for DC, DR, and Non-Prod.	Please confirm if Non-Production environments (Dev/UAT) can be hosted as logically isolated namespaces within the DR cluster or require dedicated physical VMs.	Please be guided by the RFP
641			General	BoQ Related	Please confirm if following inputs are correct for sizing: -No of IDAM users - No of Privilege Users - KMS: 2000 Keys - CLM: 5000 certificates - Secrets: 1500 - Data Tokenisation API Calls: 28M per annum	Please be guided by the RFP
642		Appendix 1A - MFASpecificatio n	MFA Clause 7	The MFA server must support IETF RFC4758 (Cryptographic Token Key Initiation Protocol) protocol out-of-the-box with no additional customization required.	Modern IDAM and MFA solution does not implement the legacy RFC4758 (CT-KIP) provisioning protocol; It uses more advanced token/authenticator seeding uses OATH HOTP/TOTP and FIDO2 standards instead. Please validate against this requirement.	Please refer Addendum 1 for the revised clause.
643		Appendix 1A - PIM Specification	PIM Clause 259	The solution must deliver secured, verifiable email communication authenticated in alignment with the Privileged Trust Sureness Protocol or an equivalent industry-standard cryptographic mechanism that provides message authenticity, integrity, and non-repudiation	The term 'Privileged Trust Sureness Protocol' does not correspond to a recognised industry standard; Please clarify this requirement. As a compensating control, the solution can secure administrative email notifications using industry-standard S/MIME digital signing/encryption for authenticity, integrity and non-repudiation.	Please be guided by thr RFP
644		OEM Evaluation Criteria	Clause 19	Proposed PIM/PAM OEM solution implemented in at least 2 BFSI clients in India, with at least 1 deployment covering >1,500 privileged users. Experience within 5 years preceding RFP publication (or currently under maintenance).	Request you to revise the following : Proposed PIM/PAM OEM solution implemented in at least 2 BFSI clients in India . Experience within 5 years preceding RFP publication (or currently under maintenance).	Please be guided by the RFP
645		OEM Evaluation Criteria	Clause 20	Proposed OEM solution (AI Security; SBOM/CBOM/AIBOM/QBOM; CASB) implemented in at least 2 verifiable clients in India with min. 100 licenses each. Experience within 5 years preceding RFP publication (or currently under maintenance).	This is new requirment and ongoing discussion are going , so we don't have any refrence list as of now. It will be difficult for copy of PO orders for these requirement.	Please be guided by the RFP
646		Page 22 Appendix 1A - SBOM,CBOM AI BOM Specification	Clause 120	AIBOM Solution can Scan a model file, report metadata.	The AIBOM Solution is under development , Please request you to keep this solution out of scope for this RFP	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
647		Page 42 7.3.3.1 Database Activity Monitoring Appendix 1A Functional Specification.pdf Sheet Name: DAM. Point 75	1. Proposed solution should comply with the requirement mentioned in Appendix 1: Functional compliance sheet, Sheet Name: DAM.	The proposed solution shall support monitoring of all databases covered under the procured licenses and shall support future expansion	Please confirm whether the solution is expected to support future growth in the number of databases beyond the currently stated 300 databases. If so, please provide the expected database growth over the proposed solution lifecycle.	Please be guided by the RFP
648					We request bank to kindly amend the clause as under :	Please be guided by the RFP
649	116	11 PAYMENT TERMS	11.1 Product (Software) Cost	Product License Cost - On successful delivery of the licenses which would be considered delivered once the software (with OOTB features) is made available for view and review of the bank on the proposed hardware - 50%	Product License Cost - On successful delivery of the licenses which would be considered delivered on submission of proof of delivery - 70%	Please be guided by the RFP
650				On successful UAT Signoff of the respective product - 20%	On successful UAT Signoff of the respective product - 20%	Please be guided by the RFP
651				On successful Go-live of the respective product - 30%	On successful Go-live of the respective product - 10%	Please be guided by the RFP
652				**Product Implementation Cost -** **On Successful installation of OOTB product on the sourced hardware and handing over the environment with OOTB product to Bank - 20%**	Product Implementation Cost - On Successful installation of OOTB product on the sourced hardware and handing over the environment with OOTB product to Bank - 50%	Please be guided by the RFP
653				On successful UAT Signoff of the respective product - 50%	On successful UAT Signoff of the respective product - 30%	Please be guided by the RFP
654				On successful Go-live of the respective product - 20%	On successful Go-live of the respective product - 10%	Please be guided by the RFP
655				Within 3 months of successful Go-live - 10%	Within 3 months of successful Go-live - 10%	Please be guided by the RFP
656				Subscription Cost (One time license Cost) On successful delivery of the Licenses which would be considered delivered once the software (with OOTB features) is made available for view and review of the bank on the proposed hardware - 50%	Subscription Cost (One time license Cost) for Year-1 On successful delivery of the licenses which would be considered delivered on submission of proof of delivery - 70%	Please be guided by the RFP
657				On successful UAT Signoff of the respective product - 20%	On successful UAT Signoff of the respective product - 20%	Please be guided by the RFP
658				On successful Go-live of the respective product - 30%	On successful Go-live of the respective product - 10%	Please be guided by the RFP
659	117	11 PAYMENT TERMS	11.3 Hardware Cost	Appliance Cost On successful Delivery of the Appliance which would be considered delivered once the solution (with OOTB features) is made available for view and review of the bank. - 50%	Appliance Cost On successful delivery of the licenses which would be considered delivered on submission of proof of delivery - 70%	Please be guided by the RFP
660				On successful UAT Signoff of the respective product - 20%	On successful UAT Signoff of the respective product - 20%	Please be guided by the RFP
661				On successful Go-live of the respective product - 30%	On successful Go-live of the respective product - 10%	Please be guided by the RFP
662				Hardware Cost (Other than Appliances) Delivery (power on) of hardware and submission of invoice with Proof of Delivery and other documents of the hardware supplied. - 70%	Hardware Cost (Other than Appliances) Delivery (power on) of hardware and submission of invoice with Proof of Delivery and other documents of the hardware supplied. - 70%	Please be guided by the RFP
663				On successful installation of proposed solutions on the hardware - 50% of the sought product/solutions - 15%	On successful installation of proposed solutions on the hardware - 50% of the sought product/solutions - 20%	Please be guided by the RFP
664				On successful installation of remaining proposed solution on the hardware – remaining 50% of the sought product/solutions - 15%	On successful installation of remaining proposed solution on the hardware – remaining 50% of the sought product/solutions - 10%	Please be guided by the RFP
665	118	11 PAYMENT TERMS	11.4 ATS/subscription cost & AMC Cost	ATS/ Annual Subscription & Appliance AMC Cost Yearly in advance (Post submission of 110% of Annual subscription cost in the form of Bank Guarantee of the respective product) or quarterly in arrears	As per the RFP, bidder would be submitting a PBG for 5% of the overall Project value, which would include AMC/ATS amount as well, hence, we request bank to waive-off this additional Bank Guarantee	Please be guided by the RFP
666				Appliance AMC - Yearly in advance (Post submission of 110% of the yearly AMC Amount of the respective product in the form bank guarantee) or quarterly in arrears	As per the RFP, bidder would be submitting a PBG for 5% of the overall Project value, which would include AMC/ATS amount as well, hence, we request bank to waive-off this additional Bank Guarantee	Please be guided by the RFP
667	116	11 PAYMENT TERMS	Product (Software) Cost, Appliance cost, Hardware Cost, Implementation Cost and ATS/subscription cost & AMC Cost		Since, this RFP has multiple Product & Solutions, hence, we understand that the milestones, sign-off and payment terms will be individually considered for each product & Solution.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
668	116	11 PAYMENT TERMS	Product (Software) Cost, Appliance Cost and Hardware Cost		We request bank to clarify the difference between the above stated 2 milestones - installation of OOTB product on the sourced hardware and handing over the environment with OOTB product to Bank and UAT sign-off. As per our understanding OOTB will be completed once the UAT is sign-off by bank.	Please be guided by the RFP
669	97	9 PROJECT TIMELINES	Overall Implementation period shall be 5 Months (Start Date is T0) for all solution & services	The bidder shall submit a comprehensive Project Plan, within 7 days of T0 covering each proposed product/solution & Services, detailing all project phases, milestones, tasks, sub-tasks, activities, timelines, dependencies. The bidder shall submit the detailed Project Plan within seven (7) days from T0 for the Bank's review and approval. Any Liquidated Damages (LD) for delays in project execution shall be calculated based on the bank's approved Project Plan. In the event the bidder fails to submit the Project Plan within seven (7) days from T0, the Bank reserves the right to levy applicable Liquidated Damages for each day of such delay. If the delay in submission of project plan exceeds seven (7) days, the Bank may prepare and issue the Project Plan, which shall be final and binding on the bidder. The bidder shall execute the project in accordance with the Bank-issued Project Plan, maintaining the overall implementation period of five (5) months from T0. All applicable Service Level Agreements (SLAs), milestones, Liquidated Damages (LDs), and other contractual obligations shall thereafter be governed by the Bank-issued Project Plan, which shall be deemed to have been accepted by the bidder without any further objection or reservation.	Bank has not provided milestone-wise Project timelines, hence, we understand that LD / Penalties will be considered on overall implementation / sign-off of the Project. Also considering the comprehensiveness of the Project, we request bank to allow overall implementation period of 9 (Nine) months.	the Bank has not issued a milestone-wise schedule because the Project Plan — covering each solution, all phases, milestones, tasks, and timelines — is required to be submitted by the bidder within 7 days of T0 and approved by the Bank. LD and penalties shall be computed with reference to the Bank-approved Project Plan, per Section 9 and Section 13.19.
670	135	12.2 Penalties	Liquidated Damages	Installation & Implementation Delay in installation, configuration, integration, testing, commissioning, migration, implementation, Go-Live, or any project milestone approved by the Bank., the Bank shall, without prejudice to its other remedies under the Contract, deduct from the Contract Price, as liquidated damages, a sum equivalent to 1% per week or part thereof of the respective Product Cost subject to maximum deduction of 10% of the total contract value, until actual delivery and implementation as per related clauses mentioned in RFP. * Product Cost = Product License/Subscription Cost + Implementation + Configuration + Integration + Migration + Commissioning Cost.	We request to amend the clause as: Installation & Implementation Delay in installation, configuration, integration, testing, commissioning, migration, implementation, Go-Live, or any project milestone approved by the Bank., the Bank shall, without prejudice to its other remedies under the Contract, deduct from the Contract Price, as liquidated damages, a sum equivalent to 0.5% per week or part thereof of the respective Product Cost delayed for Installation & Implementation subject to maximum deduction of 5% of the total Respective product cost, until actual delivery and implementation as per related clauses mentioned in RFP. * Product Cost = Product License/Subscription Cost	Please be guided by the RFP
671	120	12.1 Service Level Agreement	Liquidated Damages	Total penalties due Service level and liquidated damages shall not exceed 10% of the Total contract value.	We request to amend the clause as: Total penalties due Service level and liquidated damages shall not exceed 5% of the Total contract value.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
672	142	13.19 Liquidated Damages	Liquidated Damages	Delivery & Supply If the bidder fails to deliver any or all of the products and/or systems and/or services solutions within the time period(s) specified in the Delivery Schedule or installation, the Bank shall, without prejudice to its other remedies under the Contract, deduct from the Contract Price, as liquidated damages, a sum equivalent to 0.5 percent per week or part thereof of Contract Price subject to maximum deduction of 10% of the total contract value, until actual delivery, installation or performance as per related clauses mentioned in RFP.	We request to amend the clause as: Delivery & Supply If the bidder fails to deliver any or all of the products and/or systems and/or services solutions within the time period(s) specified in the Delivery Schedule or installation, the Bank shall, without prejudice to its other remedies under the Contract, deduct from the Contract Price, as liquidated damages, a sum equivalent to 0.5 percent per week or part thereof of undelivered Product Cost subject to maximum deduction of 5% of the total Respective undelivered Product Cost , until actual delivery, installation or performance as per related clauses mentioned in RFP. Further, we request Bank to specify the Supply & Delivery timeline out of total project timeline. Since no Supply & Delivery timeline is specifically mention, there is no method for calculation of applicable penalty / LD.	Please be guided by the RFP
673	142	13.19 Liquidated Damages	Liquidated Damages	Additional request	Considering global disruption of supply chain for OEM, we request Bank to accept partial delivery.	Please be guided by the RFP
674	135	12.1 Service Level Agreement	12.3 At-Risk Amount	The monthly At-Risk Amount (ARA') shall be 15% of the estimated monthly payout of the respective month.	We request to amend the clause as: The monthly At-Risk Amount (ARA') shall be 10% of the estimated monthly payout of the respective month.	Please be guided by the RFP
675	NA	NA	NA	Additional Clause	We understand Bank has enterprise agreement (EULA) for Operating System / Database hence Bank should provide licenses and OS & DB should not be part of the scope of this RFP. This will give commercial advantage to the Bank. In order to calculate the overall TCO, Bank may provide a Rate Card for all such items.	The bidder shall be responsible for right-sizing and provisioning all required software licenses, including Operating System (OS), Database (DB), application server, web server and other tools/software, as required to meet the RFP requirements. The bidder shall propose and include the required Enterprise/OEM-supported OS and DB licenses as part of its solution The bidder shall ensure that all licenses required for the proposed infrastructure, including those required for HA, clustering, virtualization, backup, replication and other applicable configurations, are adequately factored into the sizing and TCO.Accordingly, OS and DB licenses shall remain within the scope of the bidder, and the bidder shall not assume that such licenses will be provided by the Bank.
676	107	10.2 Eligibility Evaluation Criteria	Functional Compliance:	The proposed product should have minimum functional compliance score of 85% for each of the following: 1. Anti-Distributed Denial of Services (Anti-DDoS) 2. SSL Orchestrator along with packet broker 3. DNS protection (Internal DNS Security) 4. Web Gateway 5. Zero-Day Attack Protection at Endpoint and network 6. Zero Trust Network Access (ZTNA) 7. Data Loss Prevention (DLP) 8. Information/Digital Right Management 9. Database Activity Monitoring 10. Mobile SDK 11. Host IPS including Application Change Control (HIPS) 12. Web Application Firewall (WAF) 13. Centralized key management solution 14. Certificate Lifecycle management 15. Identity & Access Management Solution 16. Multi Factor Authentication 17. Privilege Identity/Access Management 18. DNS Security Services (Internet-Facing DNS Security Services) 19. Cloud Access Security broker (CASB) 20. AI Security 21. SBOM, CBOM, AIBOM & QBOM	In the current era, security of the banking and financial sector is of paramount importance. Given that this RFP pertains to critical IT security solutions and services, we believe that the Bank should consider 100% functional compliance across all specified technologies to ensure a robust overall security posture. The proposed 85% functional compliance threshold may leave gaps in the security architecture and could potentially introduce risks to the Bank's overall security posture. We recommend that the Bank consider 100% compliance for all established and mature technologies. However, the Bank may consider providing reasonable relaxation for new and evolving technologies, such as AI Security, CBOM, SBOM, AIBOM and QBOM, where the technology landscape and industry standards are still evolving. This approach would help the Bank maintain stringent security standards while providing adequate flexibility for emerging technologies.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
677	212	15.21.4 Deployment & Data Retention	15.21.4, Sr.No.22 vs 7.13(5)(ii)	Annexure 21.4 Sr.No.22: "Backup & Retention (Provided and maintained by bank)". Cl.7.13(5)(ii): "The bidder/OEM is responsible for supplying, designing, sizing and configuring the Backup Software and Hardware (with Ransomware Protection)..." Appendix 1B also carries full spec sheets for Backup Solution/Storage and Long Term Storage expecting a bidder compliance response.	These three references appear contradictory on who supplies the Backup and Long-Term Storage (LTS) infrastructure. Kindly confirm: is Backup/LTS hardware and software to be supplied, sized, and costed by the bidder (as Section 7.13 and Appendix 1B suggest), or is it to be provided and maintained by the Bank (as Annexure 21.4 states)?	Please refer Addendum 1 for the revised clause. Clarification : The bidder shall be responsible for the complete end-to-end supply, installation, configuration, integration, testing, commissioning, documentation, warranty and comprehensive maintenance of the proposed IT infrastructure throughout the contract period, as specified in the RFP. Accordingly, the complete Backup & Restoration solution, including Ransomware Protection, Backup Software, Backup Server, Backup Storage/Backup Appliance, Long-Term Storage and all associated hardware, software, licenses, accessories and components, shall be supplied, designed, sized, configured, implemented and maintained by the bidder Implementation of the IT Infrastructure at the Bank's DC, DR, NDR and/or other designated locations is the responsibility of the bidder/OEM. The bidder shall consider the complete requirement while carrying out the sizing and shall include all necessary components, licenses and associated infrastructur
678	74	7.11 Resource Requirement	7.11, Minimum Resource Table Pg.74	The "Data Security" domain (covering DAM, Database Security, and Mobile Application Security) shows 0/blank headcount across all shifts and levels (L1/L2/L3) in the minimum resource deployment table, unlike every other domain (Perimeter & Network, Endpoint, Application & Management) which has at least some dedicated minimum floor allocated.	Our understanding is that this is intentional, and the Data Security domain is expected to be covered entirely through cross-skilled L1/L2 resources drawn from the other domains (as permitted under Section 7.11's cross-skilling provision), rather than being handled separately by the Bank's own in-house team. Kindly confirm if this understanding is correct, or clarify if a dedicated minimum resource count for Data Security was intended but inadvertently omitted.	Cross-skilled resources may provide Data Security coverage where they possess the required competency and can meet the minimum coverage and SLA requirements. The absence of a separate minimum headcount shall not be interpreted as exclusion of Data Security operational responsibilities.
679	97	9 Project Timelines	9	"Overall Implementation period shall be 5 Months (Start Date is T0) for all solution & services"	For example, does this mean all 21 solutions (e.g., Anti-DDoS, DLP, IDAM, AI Security, etc.) must each independently achieve Go-Live within the same 5-month window, or can the bidder propose a phased plan (e.g., Perimeter & Network Security solutions going live by Month 3, Identity & Management Layer solutions by Month 5), provided the overall 5-month outer boundary is met? Kindly confirm which reading is correct.	Please be guided by the RFP. Overall 5 - month outer boundary needs to be met.
680	108	10.2 Eligibility Cl.22 - Functional Compliance	10.2, Cl.22 (C - Customization note)	"All identified customizations shall be completed, tested, and made available by the bidder prior to commencement of User Acceptance Testing (UAT) (i.e., within 17 weeks of acceptance of PO), without impacting the Bank's project timelines."	Since the overall Implementation Period is 5 months (~21-22 weeks per Section 9), our understanding is that Week 17 is intended as a common UAT-readiness checkpoint applicable uniformly across all 21 solutions, with the remaining ~4-5 weeks reserved for UAT, Go-live, and stabilization. Kindly confirm if this understanding is correct, or clarify if the 17-week deadline is meant to apply on a per-solution basis with staggered UAT dates instead.	Please be guided by the RFP. Clarification : Per Eligibility Evaluation Criteria 10.2, Point 22, all "C"-marked customizations shall be completed, tested, and made available prior to commencement of UAT, i.e., within 17 weeks (indicative) of PO acceptance, without impacting the Bank's project timelines. If Biddere proposed UAT for respective solution is later than 17 weeks then bidder to ensure any functionality and customization is completed before the first delivery of the said solution to the bank in UAT.
681	102	10.2 Eligibility Cl.6 - Manpower	10.2, Cl.6	"Bidder must have at least enrolled manpower (on bidder's payroll) of 150 experienced employees skilled in areas of Cyber/IT security."	Kindly clarify: (a) what qualifying certification or minimum years of experience is considered sufficient to count as "skilled" for this purpose; and (b) whether this 150-headcount requirement must be demonstrated as a dedicated BFSI/Cyber Security practice headcount, or can be met using the bidder's total pan-India IT security workforce across all industry verticals.	Please refer Addendum 1 for the revised clause. Clarification : (a) "Skilled" is not tied to any specific certification or minimum years of experience; the requirement is met by the bidder's self-certified undertaking of the employees (on bidder's payroll) with experience in Cyber/IT security. (b)The headcount is not required to be a dedicated practice across any specific indistry vertical however it is to be Cyber/ IT Security practice.
682	128	12.1 DR Instance Availability	12.1, DR Instance Availability row	"A penalty of ₹10,000 for every 10 minutes or part thereof beyond the stipulated RPO or RTO shall be levied." RPO: 15 minutes, RTO: 60 minutes.	For example, if a single DR failover event affects 3 of the 21 solutions simultaneously and each breaches RTO by 30 minutes, our understanding is that the penalty is computed once per solution (i.e., ₹10,000 x 3 solutions x 3 [30/10 blocks] = ₹90,000 total for that event), not levied as one flat bank-wide amount. Kindly confirm if this understanding is correct, and clarify how this penalty interacts with the Infrastructure Availability SLA penalty in the same section, given Cl.12.1.18 states the Bank shall not levy multiple penalties for the same event.	The applicable penalty (RTO & RPO) shall be calculated solution-wise for each affected solution based on the delay beyond the stipulated RTO/RPO.
683	66	Appendix 1B - Technical Specification Sheet	Appendix 1B	Primary Storage, x86 Server, GPU Server, SAN Switch, Backup Solution & Storage, Long Term Storage, and Load Balancer sheets carry only minimum technical specifications (per-unit capability floors) with no Bank-stated quantities or total capacity baseline; per Section 7.13, sizing is entirely bidder-determined.	Given the scale of the engagement (12,000-16,000 users, 35,000 DHCP devices, 2,500 servers, 300 databases per Annexure 21), kindly confirm if the Bank can share a reference sizing worksheet/baseline (e.g., expected minimum usable storage capacity, x86/GPU server count, SAN port count, backup/LTS capacity) to align bidder proposals and ensure comparability across bids.	Bidder to design based on the deployment requirement of the solution and sizing

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
684	66	Appendix 1B - GPU Server	Appendix 1B / Appendix 3 (V2P)	Appendix 1B carries a full "GPU Server" technical specification sheet, and Appendix 3's V2P sizing template includes "GPU Required (Yes/No)", "No. of GPUs per node" and "GPU Memory (vRAM GB)" fields for each of the 21 solutions. No functional requirement referencing GPU/AI-inference/sandboxing dependency is stated anywhere in the RFP body or in Appendix 1A's functional specification sheets (including the AI Security tab, which is described as an inline AI-traffic inspection/gateway solution).	Kindly confirm the specific solution(s) for which GPU-based infrastructure is required (for example, is this for AI Security model inference, or for Zero-Day/Anti-APT sandboxing/malware detonation?), along with the expected workload/model type driving this requirement, so bidders can size and cost it accurately.	Bidder to design based on the deployment requirement of the solution and sizing
685	207-212	15.21.4 Deployment & Data Retention (Volumetrics)	15.21.4 (read with Annexure 21 intro, Pg.203 and Cl.7.13(12))	Volumetrics for multiple solutions are stated as "X Scalable to Y" (e.g., Web Gateway "Users: 12000 Scalable to 16000," DLP "12000 Users scalable to 16000," IDAM/MFA "12000 scalable to 16000," HIPS "3000 VMs/Servers scalable to 4500"), with only PIM and Mobile SDK explicitly qualifying the base figure as "(Day 1)". Separately, Annexure 21's introductory clause (Pg.203) and Section 7.13(12)(a)/(i) require the bidder to "account for the projected growth... throughout the contract period" while sizing, with any shortfall from "failure to account for projected growth" to be rectified "at no additional cost to the Bank."	For example, for DLP: does "12000 Users scalable to 16000" mean the bidder licenses/costs only 12,000 users on Day 1 and the Bank separately procures the additional 4,000 later via pro-rata purchase (per Section 7.10 Cl.7/Section 7.11), or does it mean the bidder must architect, provision, and license all 16,000 users from Day 1 at no additional cost, as "projected growth" the Bank has already disclosed? Kindly confirm which interpretation applies, clarify the expected timeline (if any) for reaching the higher figure, and confirm whether the "Day 1" qualifier used for PIM and Mobile SDK should be read as applicable to all other volumetric entries in this table as well.	On day 1 bidder to factor the licenses for the sought requirement, however, for scalable requirements, bank will procure licenses as per rate card/ pro rata basis. However, the proposed solution should be architected to support the scalability
686	70-74	7.11 Resource Requirement	7.11	Section 7.11 specifies minimum onsite L1/L2/L3/IT-Infra resource counts without explicitly stating whether these resources are dedicated solely to the 21 solutions procured under this RFP.	Our understanding is that the minimum resource counts in Section 7.11 are meant solely to support the 21 solutions and associated IT infrastructure procured under this RFP, and do not extend to any of the Bank's other/existing IT security tools outside this RFP's scope (for example, the Bank's separately-tendered NextGen SOC). Kindly confirm if this understanding is correct.	The minimum resource requirement applies to the solutions, infrastructure and services within the scope of this RFP.
687	27, 88, 90-91, 207-212	7 Scope of Work / 7.13 IT Infrastructure	7 / 7.13(2)(vi), 7.13(6)(i),(ix),(xi)	Scope of Work and Section 7.13 reference "NDR" as one of three operational locations (DC/DR/NDR) requiring implementation, warranty/support, 24x7 operations, and backup/replication coverage. However, Annexure 21.4's per-solution deployment table (Pg.207-212) specifies HA deployment only for "Bank's DC" and "Bank's DR" for all 21 solutions, with no NDR entry anywhere; Appendix 3 (V2P) has no NDR environment block; and Appendix 2's "Appliance Cost" sheet has no NDR cost section.	Our understanding is that no separate appliances/infrastructure are required at NDR, since it has no corresponding deployment row, sizing block, or BOM line item anywhere, and the DC/DR/NDR references in Section 7.13 pertain only to service/support coverage obligations rather than a distinct physical deployment. Kindly confirm if this understanding is correct, or if appliances are in fact required at NDR, in which case kindly provide the missing volumetrics, deployment topology, and BOM line items for it.	The proposed Long-Term Storage (LTS) solution shall be deployed at both NDC and NDR and shall support long-term retention and storage of backups, logs, files and other Bank-approved data, as applicable. The proposed solution shall provide adequate capacity, scalability, availability, data protection and access mechanisms to meet the Bank's defined retention and storage requirements at both sites.
688	203	15.21.1 Non-Production Environment	15.21.1	"For appliance-based solutions, the bidder shall design and propose an appropriate non-production environment to support testing, validation, upgrades, patching, configuration changes, policy tuning, rule testing... For VM-based solutions, the non-production environment shall be sized at a minimum of 10% of the Production (DC) environment unless otherwise specified in the RFP."	For example, for an appliance-based solution like Anti-DDoS or WAF, where the OEM may not offer a VM/software edition, kindly clarify what constitutes an "appropriate" non-production environment — is a reduced-capacity physical unit of the same appliance line acceptable in lieu of a virtual instance, given no minimum sizing formula (unlike the 10% rule for VM-based solutions) is specified for this case?	Bidder to design the methodology and approach non production environment for appliance based solutions
689	203, 28-31	15.21.1 Non-Production Environment / 7.1 Solution Deployment Models	15.21.1 (read with 7.1 solution table)	Several solutions permit Cloud/Hybrid deployment models (CASB: "On-Cloud/Hybrid/On-premises at DC&DR"; SBOM/CBOM/AIBOM/QBOM: "On-Premises/On-Cloud/Hybrid"; DNS Security Services: "Cloud-based DNS Security Service... with High Availability"), while the Non-Production Environment clause (15.21.1) only distinguishes "appliance-based" vs "VM-based" solutions.	Kindly clarify whether a dedicated non-production environment/tenant is mandatory for solutions proposed under a Cloud or Hybrid deployment model (e.g., CASB, DNS Security Services, SBOM/CBOM/AIBOM/QBOM), given the OEM's shared multi-tenant test capability may be the only option available for such SaaS/cloud-delivered solutions.	For SaaS based Solution, bidder to design the methodology.
690	88, Appendix 3	7.13 IT Infrastructure / Appendix 3 (V2P)	7.13(4)(i)	"The bidder shall supply all hardware, software, operating systems, hypervisors, firmware, appliances, licences..." Appendix 3's V2P sheet carries a bidder-fill field "Virtualization Platform (VMware/Hyper-V/KVM/Physical)" with no Bank-specified platform named anywhere in the RFP body.	Kindly confirm whether the Bank has any preferred/standardized virtualization platform (e.g., VMware/Hyper-V/KVM/Nutanix) that the bidder-supplied compute infrastructure must be compatible with, or whether the choice of hypervisor is entirely at the bidder's discretion. Separately, our understanding is that the bidder must supply dedicated hardware for the Production environment, and the VM sizing declared in Appendix 3 for the Non-Production/lower environment is also to be provisioned on bidder-supplied hardware (not on the Bank's existing infrastructure/virtualization estate). Kindly confirm if this understanding is correct, or clarify if the Non-Production environment may instead be hosted on the Bank's existing hardware/virtualization platform.	The bidder may propose an OEM-supported virtualization platform compatible with the proposed architecture . The Non-Production environment shall be the same as the DC-Production (Primary) environment in terms of technology stack, OEM/product, version, edition, features, functionality, architecture, configuration compatibility and other relevant technical specifications. Only the quantity/capacity and applicable licensing metrics may differ between the Non-Production and DC-Production (Primary) environments, based on the requirements specified in the final approved Infrastructure BOQ.

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
691	46	7.3.4.4	Certificate Lifecycle Management	Quantum attacks on RSA/ECC encryption – The CLM solution should protect digital certificates, VPNs, and encrypted communications against quantum computers.	Please clarify whether the CLM solution is expected to natively support Post-Quantum Cryptography (PQC) algorithms, or whether the requirement is limited to identifying certificates using quantum-vulnerable algorithms such as RSA/ECC and facilitating their migration/replacement. Please also specify the PQC standards/algorithms, if any, that are required to be supported.	The requirements specified under the Certificate Lifecycle Management (CLM) Functional Specifications are mandatory and shall be complied with as specified in the RFP. The Bidder shall ensure that all specified capabilities, including certificate discovery, inventory, issuance, enrollment, deployment, renewal, rotation, revocation, archival, expiry monitoring, secure retirement, key management, automation, workflow, reporting, alerting, integration and audit trails, are included in the proposed solution and are available as part of the quoted solution. Where integration with third-party/public/private Certificate Authorities (CAs), operating systems, databases, middleware, network devices, applications, cloud platforms or container environments, the Bidder shall ensure the necessary connectors, APIs, agents, integrations and licenses are included in the proposed solution and TCO.
692	46	7.3.4.4	Certificate Lifecycle Management	Harvest Now, Decrypt Later (HNDL) attacks – The CLM solution should enable rapid migration to quantum-safe cryptography before future decryption becomes possible.	Please clarify whether the CLM solution is expected to provide capabilities to identify and prioritize certificates/cryptographic assets susceptible to Harvest Now, Decrypt Later (HNDL) risks and support migration to quantum-safe cryptography. Please also clarify whether automated certificate replacement and deployment across dependent systems are in scope.	Please be guided by the RFP
693	46	7.3.4.4	Certificate Lifecycle Management	Quantum compromise of PKI – The CLM solution should ensure long-term trust in certificates and digital identities.	Please clarify the specific CLM capabilities expected to address quantum compromise of PKI, including cryptographic asset discovery, algorithm risk assessment, crypto-agility, support for PQC/hybrid certificates, CA integration, and certificate migration/replacement.	Please be guided by the RFP
694	46	7.3.4.4	Certificate Lifecycle Management	Quantum attacks on payment systems – The CLM solution should ensure protection and lifecycle management of certificates securing payment applications, payment transactions, RTGS, UPI, and SWIFT communications.	Please clarify whether the CLM solution is expected to discover and manage certificates used specifically by payment applications, RTGS, UPI, SWIFT and related systems, and whether direct integration with these systems is required. If integration is required, please provide the expected interfaces/protocols and existing PKI/CA infrastructure details.	The solution shall support discovery and lifecycle management of certificates used by applicable payment and critical banking systems within the approved scope. Direct integration shall be required where technically applicable; specific interfaces shall be finalized during detailed design.
695	46	7.3.4.4	Certificate Lifecycle Management	Quantum threats to stored banking data – The CLM solution shall enable protection of customer records and financial archives from future quantum decryption.	Please clarify how protection of stored customer records and financial archives against future quantum decryption is expected to be achieved through the CLM solution, as this may involve data encryption, KMS/HSM and cryptographic key management capabilities. Please confirm whether such capabilities are expected to be provided natively by CLM or through integration with the Bank's existing/proposed KMS/HSM/data encryption solutions.	Please be guided by the RFP
696	47	7.3.5.1	Identity & Access Management Solution	The Bank requires an Identity & Access Management (IDAM) solution to establish secure, centralized control over user identities, access rights, and authentication mechanisms... The solution must be scalable, interoperable with core systems like HRMS, ITSM, and SIEM, and capable of operating in a high availability and disaster recovery setup.	Please clarify the expected scope of IDAM implementation with respect to the Bank's existing identity infrastructure, including Active Directory/directory services, HRMS, ITSM, PAM, SIEM and existing authentication systems. Please provide the current architecture, number/type of directories, applications and identities in scope, and confirm whether the bidder is expected to replace or integrate with the existing components.	The successful bidder shall assess the existing identity environment during requirement analysis and propose the approved target architecture. The solution may integrate with the existing components depending on the Bank's approved transformation roadmap.
697	48	7.3.5.1	Identity & Access Management Solution	Configuration documentation including directory and domain integration details and integration setup with HRMS, ITSM, MFA, PAM, SIEM, SOAR and other tools & infrastructures.	Please clarify whether integration with all existing Bank applications and security platforms is mandatory from Day 1, and provide the complete list of applications/systems to be integrated, along with available integration mechanisms (API, SCIM, LDAP, SAML, OIDC, database, file-based or other). Please also confirm whether custom connector development and integration effort for non-standard/legacy applications is included in the bidder's scope without additional cost.	Integration shall be phased and based on the approved implementation plan within the defined timelines. The Bank will identify priority systems during SRS stage
698	Appendix 1A – IDAM	IDAM – Functional Specification	IDAM Functional Specification – S.No. 2	Proposed unified platform components (Authentication, SSO and IDAM) should be from a single OEM for seamless integration.	Please clarify whether the requirement for Authentication, SSO and IDAM components to be from a single OEM is mandatory, or whether equivalent solutions from the same bidder with standards-based interoperability may be accepted.	Please be guided by the RFP
699	Appendix 1A – IDAM	IDAM – Functional Specification	IDAM Functional Specification – S.No. 9	Solution must be able to integrate with HRMS as Source system and integration with Active Directory and variety of business & technical applications (new-age, legacy, on-prem. and cloud with and without API's) as target system for user provisioning/de-provisioning. Bidder has to integrate all banks application with IDAM solution.	Please clarify the phrase "all banks application". Kindly provide the indicative/complete application inventory, including number of applications, technology/platform, deployment model, user population and available integration interfaces. Please also clarify whether integration with applications without APIs will require development of custom connectors and whether such effort is included in the base scope.	Application-related information will be provided during implementation and SRS stage
700	Appendix 1A – IDAM	IDAM – Functional Specification	IDAM Functional Specification – S.No. 58	The proposed solution shall provide a configurable connector framework to establish integrations using APIs and SCIM... and shall also support custom connector development for non-standard integration requirements.	Please clarify the expected number of standard and custom connectors to be developed/integrated during implementation, and whether custom connector development for non-standard applications is included in the base license and implementation scope.	Application-related information will be provided during implementation. The bidder will be responsible for integrating all the identified applications.

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
701	Appendix 1A – MFA	MFA – Functional Specification	MFA Functional Specification – S.No. 2 / 12	The proposed solution should be deployed completely on-premises without any dependency on cloud. The MFA solution must support on-premises deployment.	Please confirm whether the requirement permits optional use of cloud-based services for non-critical functions such as SMS/email delivery, software update services or threat intelligence, while the MFA authentication server and sensitive authentication data remain fully on-premises. If not, please clarify the expected architecture for SMS/email-based authentication.	The proposed should be deployed on-premise only
702	Appendix 1A – MFA	MFA – Functional Specification	MFA Functional Specification – S.No. 4	The MFA server must come with a RADIUS server with no additional cost.	Please clarify the expected number of RADIUS instances, authentication transactions/users to be supported, and whether the RADIUS capability is required to be OEM-native. Please also confirm that all required RADIUS licensing, replication and HA capabilities are included in the base MFA license.	The proposed MFA solution must have native RADIUS support with unlimited licenses. Application- and device-related information will be provided by the Bank during implementation & SRS Stage.
703	Appendix 1A – MFA	MFA – Functional Specification	MFA Functional Specification – S.No. 9	The MFA server must support multiple replicas when necessary without any additional cost and licenses.	Please clarify the required number of MFA replicas/nodes for the Bank's DC and DR environments and the expected HA/DR architecture. Please also confirm whether licenses for all production, DR and non-production nodes are required to be included without additional cost.	The bidder is requested to propose an MFA solution covering all required environments, including Non-Production, Data Centre (DC), and Disaster Recovery (DR). The DC and DR architecture shall be as per the RFP requirements.
704	Appendix 1A – MFA	MFA – Functional Specification	MFA Functional Specification – S.No. 10 / 14	The MFA solution should support FIDO2-compliant MFA tokens and adaptive authentication.	Please clarify the expected FIDO2 authentication use cases and supported authenticators, and provide the adaptive authentication policies/risk signals expected to be implemented (e.g., device, location, IP/network, user risk, time or transaction context). Please also clarify whether risk-based authentication is expected to be available without dependency on an external cloud service.	Yes, the understanding is correct.
705	Appendix 1A – MFA	MFA – Functional Specification	MFA Functional Specification – S.No. 7	The MFA server must support IETF RFC4758 (Cryptographic Token Key Initiation Protocol) protocol out-of-the-box with no additional customization required.	Please confirm the intended use case and authentication/token ecosystem for RFC4758. If this requirement is linked to an existing Bank system or token infrastructure, please provide the existing product/version and integration details so that compatibility can be assessed.	Please refer Addendum 1 for the revised clause.
706	46	7.3.4.3 / 7.3.4.4	Centralized Key Management / Certificate Lifecycle Management	KMS shall manage encryption keys including generation, distribution, rotation, archival and revocation, while CLM shall manage digital certificates and associated keys throughout their lifecycle.	Please clarify the functional boundary and integration responsibilities between the proposed KMS and CLM solutions, particularly for key generation, secure key storage, key rotation, certificate-key association, revocation and archival. Please confirm whether the Bank expects a single integrated platform or separate solutions with standards-based integration.	Please be guided by the RFP
707	46-47	7.3.4.4 / 7.3.4.5	Certificate Lifecycle Management / S-BOM, C-BOM, AI-BOM & Q-BOM	CLM shall provide key and certificate discovery and vulnerability assessment, while C-BOM/Q-BOM shall provide cryptographic asset discovery and quantum-readiness visibility.	Please clarify the expected source of truth and division of responsibilities between CLM and C-BOM/Q-BOM for cryptographic discovery. Specifically, should CLM discover only certificates/keys associated with certificates, while C-BOM/Q-BOM discovers cryptographic algorithms and dependencies across applications, libraries, devices and infrastructure?	Please be guided by the RFP
708	211	15.21.4	Deployment & Data Retention – IDAM	IDAM: Bank's DC and DR in HA (N+N Active-Active) deployment; enterprise user volumetrics are stated as 12,000 scalable to 16,000.	Please confirm whether the stated IDAM volumetric of 12,000 scalable to 16,000 represents total active identities/users to be managed by the IDAM platform, or only the licensed/transactional user population. Please also provide expected numbers of service accounts, privileged accounts, application accounts and identities from external/contractor populations, if applicable, for sizing and licensing.	Bidder to design the solution based on the volumetrics provided
709	211	15.21.4	Deployment & Data Retention – MFA	MFA: Bank's DC and DR in HA (N+N Active-Active) deployment; 12,000 users scalable to 16,000.	Please clarify whether the MFA volumetric of 12,000 scalable to 16,000 represents unique enrolled users, concurrent authenticated users, or licensed users. Please also provide indicative peak authentication transaction volume/requests per second and expected authentication factor distribution to enable accurate sizing of the MFA solution.	Bidder to design the solution based on the volumetrics provided
710	210	15.21.4	Deployment & Data Retention – CLM	Certificate Lifecycle Management: Bank's DC and DR in HA (N+N Active-Active) deployment with enterprise-wide licenses for certificate issuance, provisioning and management.	Please provide the indicative Day-1 and projected certificate volumes, including number of certificates, issuing CAs, managed endpoints/devices, applications, domains and expected certificate issuance/renewal transactions. Please also clarify whether the enterprise-wide license is intended to be unlimited with respect to certificate count, managed endpoints and issuance/renewal transactions.	Please be guided by the RFP. Bidder to design the solution based on the volumetrics provided

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
711	1	Primary Storage	5	Proposed storage solution should be offerred with minimum 2 controllers with minimum 256 GB DRAM Cache memory on the entire storage Solution. The solution should scale to atleast 512GB Cache memory by adding additional controller.	Change To: Proposed storage solution should be offered with minimum 2 controllers with minimum 128 GB DRAM Cache memory on the entire storage Solution. The solution should scale to atleast 256GB Cache memory by adding additional controller. Explanation: Cache ask should be Reduced as cache of 64GB or less per controller (128GB total) is enough as the latest CPUs, high-speed memory, and Gen 5 PCIe cards deliver the required performance efficiently. Modern storage controllers optimize cache usage, and industry benchmarks confirm that asked performance can be achieved with lower memory. This reduction not only meets technical needs but also decreases hardware, power, and cooling costs, resulting in a lower TCO for the solution	Please be guided by the RFP
712	4	Backup Solution	16	The proposed disk-based storage/appliance must interoperate with industry-leading server platforms and operating systems, and must ingest backup data over a secure, API-based disk-to-disk (D2D) connection.	Change To: The proposed disk-based storage/appliance must interoperate with industry-leading server platforms and operating systems, and must ingest backup data using standard Data protocols such as FC, ISCI, NFS, S3 Explanation: This specific ask qualifies only specific backup appliance not any target storage as enterprise storage do not support data ingestion using API rather leverage protocols such as FC, ISCI, NFS , S3.	Please be guided by the RFP
713	4	Backup Solution	25	The Proposed Appliance/Backup Storage must provide verification of the Metadata and actual data of the file with strong Checksum Mechanism	Change To:The Proposed Appliance/Backup Solution must provide verification of the Metadata and actual data of the file with strong Checksum Mechanism Explanation: Proposed ask should be from Solution instead of storage as any storage does not offer file-level checksum reporting for backup files. This is typically a function of the backup software (e.g., Commvault, Veeam) that stores backups on storage.	Please be guided by the RFP
714	2	Long Term Storage	4	Addititional Point Request	Point to be written as: Long Term Storage should support WORM (Write Once, Read Many) capability to have Data Immutability. Explanation: We recommend implementing WORM (Write Once, Read Many) capability for long-term backup storage to ensure data is protected against accidental deletion and ransomware attacks. Additionally, WORM functionality is required to comply with regulatory guidelines for banking institutions. Since backup storage is expected to provide WORM capability, long-term backup storage should also comply with this requirement to maintain robust data protection .	Please be guided by the RFP
715	1,2,4	Primary Storage Backup Storage Long Term Storage		Addititional Point Request	Point to be written as: The proposed storage systems (for all 3 storage requirements), should have launch dates within past 3 years Explanations: We recommend qualifying storage systems with a launch date within the past three years. This approach ensures a better return on investment and reliable long-term support for a period of 7 to 10 years, as required by the bank. Some OEMs are currently offering systems that are over six years old and lack a clear roadmap or support commitment, which poses a risk to long-term operational stability and longevity.	Please be guided by the RFP
716	HIPS Sheet	Appendix 1A Functional Specification	Section - Required Functionalities/Features Point 2	Solution should have all protection modules like Anti-Malware, Deep Packet Inspection with HIPS, Host-based Firewall, Integrity Monitoring, Application Control, Device Control, OS Log inspection, Memory Protection capabilities in a single agent.	Please change to "Solution should have all protection modules like Anti-Malware, Deep Packet Inspection with HIPS, Host-based Firewall, Integrity Monitoring, Application Control, Memory Protection capabilities in a single agent." this will help in braoder participation	Please be guided by the RFP
717	HIPS Sheet	Appendix 1A Functional Specification	Section - Required Functionalities/Features Point 3	The proposed server security solution must support multiple platforms of server operating systems i.e. AIX, Alma Linux, Amazon Linux, CentOS, Cloud Linux, Debian Linux, Miracle Linux, Oracle Linux, RHEL, RedHat OpenShift, Rocky Linux, Solaris, Suse, Ubuntu, Windows, Docker, Docker CE, Docker EE.	Please change to "The proposed server security solution must support multiple platforms of server operating systems i.e. Windows, Linux RedHat, CentOS, Oracle, Debian, SUSE, Ubuntu, Amazon Linux etc. for the OS versions which are under active support from respective OEM's" this will help in broader participation	Please refer Addendum 1 for the revised clause.

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
718	HIPS Sheet	Appendix 1A Functional Specification	Section - Required Functionalities/Features Point 12	The solution should provide automated recommendations and enforcement of protection policies against known vulnerabilities. It must support automatic removal or adjustment of protection rules when vulnerabilities are resolved, such as disassociating outdated signatures after patches are applied. The scheduling of these actions should be configurable by administrators with flexible options like hourly, daily, weekly, or monthly intervals.	Request to please remove this clause as it as specific OEM biased and will limit broader participation	Please be guided by the RFP
719	HIPS Sheet	Appendix 1A Functional Specification	Section - Required Functionalities/Features Point 13	The solution shall detect RCE vulnerabilities and provide complete visibility of detected vulnerabilities in servers with CVE details. The proposed solution should automatically assign the interim compensatory rules/filters on the servers to shield against the detected RCE vulnerabilities.	Please change to "The solution shall detect RCE vulnerabilities and provide complete visibility of detected vulnerabilities in servers with CVE details. The proposed solution should automatically/manually assign the interim compensatory rules/filters on the servers to shield against the detected RCE vulnerabilities" the proposed change will help in broader Participation	Please be guided by the RFP
720	HIPS Sheet	Appendix 1A Functional Specification	Section - Required Functionalities/Features Point 25	The solution should include a Log Inspection module capable of capturing and analyzing system logs, providing audit evidence to meet PCI DSS or internal requirements within your organization. Additionally, the solution should have the ability to forward suspicious events to an SIEM system or centralized logging server for correlation, reporting, and archiving purposes.	Specific OEM point- TrendMicro specific	Please refer Addendum 1 for the revised clause.
721	Zero Day Attack Sheet	Appendix 1A Functional Specification	Section - Functional Specification Point 17	Proposed solution should be able to provide customizable sandbox to match endpoint environments. Access different information about Affected Hosts on the following views: Displays a summary of affected hosts by attack phase, Provides access to Host Details views and Displays host event details in chronological order	Please change to "Proposed solution Access different information about Affected Hosts on the following views: Displays a summary of affected hosts by attack phase, Provides access to Host Details views and Displays host event details in chronological order" this will help in broader participation	Please be guided by the RFP
722	Zero Day Attack Sheet	Appendix 1A Functional Specification	Section - Functional Specification Point 45	Solution should integrate with Endpoint, Email and Server Security Solution for better Security posture and sharing of IOCs automatically, both user defined as well as the ones analyzed by sandbox	Please change to "Solution should integrate with Endpoint, Email and Server Security Solution for better Security posture and sharing of IOCs automatically in case if it cannot function in an inline mode for automatic sample submission " , this change will help in broader participation	Please be guided by the RFP
723	149	14.2 APPENDIX 1B: Technical Compliance Sheet DDoS S. No. 73	The proposed solution shall support PQC readiness and migration capability, including identification of quantum-vulnerable cryptographic algorithms and support for PQC-enabled or quantum-resistant cryptographic standards, wherever applicable to the solution.	Suggested Clause: The proposed solution shall support TLS 1.3 with hardware acceleration for encrypted traffic protection.	The technical specifications requested for TLS inspection already cover full SSL/TLS inspection as an in-built capability of the DDoS mitigation hardware. Therefore, specifying the latest cipher suites and TLS 1.3 with hardware-based acceleration should be considered as a technology-neutral requirement to enable wider OEM participation, rather than mandating any specific requirement.	PQC readiness is intended to cover applicable cryptographic functions, communication interfaces, authentication mechanisms, APIs, certificates and other security components of the proposed solution and support migration to quantum-resistant standards. DDoS vendor need to submit their roadmap or approach on PQC
724	149	14.2 APPENDIX 1B: Technical Compliance Sheet WAF S. No. 12	The proposed solution must support dedicated 5 Gbps of WAF throughput (HTTP/HTTPS). The bidder must provide evidence of throughput through publicly available documents /evidence based document supporting the same which needs to be submitted along with the proposal and same needs to showcased if asked by bank during Presentation & UAT (Undertaking from the OEM is not accepted in this case).	Suggested Clause: The proposed solution must support dedicated 5 Gbps of WAF throughput (HTTP/HTTPS) or 25 Gbps of L7 throughput. The bidder must provide evidence of throughput through publicly available documents (Undertaking from the OEM is also accepted in this case).	Not every OEM publishes WAF throughput as a standard performance parameter. However, leading vendors in the WAF and API Protection space do publish Layer-7 throughput capabilities as part of their product specifications. Therefore, vendors that can demonstrate equivalent L7/WAF and API protection performance should also be considered to ensure wider OEM participation and a technology-neutral evaluation process.	Please be guided by the RFP
725	149	14.2 APPENDIX 1B: Technical Compliance Sheet WAF S. No. 81	The client component (JavaScript) should be downloaded from the same domain as the application (first party). It is not allowed to use external locations to upload the script.	Suggested Clause: The client component (JavaScript) should be downloaded from the same domain as the application (first party).	Every OEM may use its own architecture and methodology to achieve the required functionality. Therefore, the evaluation should be functionality- and outcome-based rather than implementation-method-based. The specified clause should not be restrictive, provided that the proposed solution meets the intended security and functional requirements.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
726	149	14.2 APPENDIX 1B: Technical Compliance Sheet WAF S. No. 90	The proposed WAF solution must support high availability in both Layer 2 and Layer 3 deployments. It must include either an inbuilt bypass switch or be supplied with an external bypass switch to ensure uninterrupted traffic flow during maintenance or failure.	Suggested Clause: The proposed WAF solution must support high availability in both Layer 2 and Layer 3 deployments.	Fail-open/Bypass is not relevant in the context of a stateful security solution, as maintaining session and connection state is essential to its intended operation. If fail-open functionality is considered a mandatory requirement, it should be applied consistently across the complete network security architecture and applicable network devices. Specifying fail-open only for a single stateful solution does not provide meaningful operational value and may unnecessarily restrict wider OEM participation.	Please refer Addendum 1 for the revised clause.
727	149	14.2 APPENDIX 1B: Technical Compliance Sheet WAF S. No. 92	The solution must have bypass segments to ensure that fail open in case of hardware failure	Suggested Clause: The solution must support high availability	Fail-open/Bypass is not relevant in the context of a stateful security solution, as maintaining session and connection state is essential to its intended operation. If fail-open functionality is considered a mandatory requirement, it should be applied consistently across the complete network security architecture and applicable network devices. Specifying fail-open only for a single stateful solution does not provide meaningful operational value and may unnecessarily restrict wider OEM participation.	Please be guided by the RFP
728	1	Appendix 1A Functional Specification- DAM	105	The Risk Analytics Solution must provide behavior analytics algorithm to establish behavioral baseline and find deviations.	Kindly confirm whether the solution's built-in User and Entity Behaviour Analytics is also required to automatically establish behavioural baselines for normal database activity and identify deviations such as unusual access volumes, atypical query patterns, off-hours activity, and privilege misuse, with prioritized and risk-scored anomalies rather than only raw alerts.	Please be guided by the RFP
729	43	7.3.3.2 Mobile SDK	Key Functional Requirements	The SDK will enable key features such as biometric authentication, device binding, secure PIN input, fraud detection, transaction risk scoring, and in-app messaging. It will ensure that all security events originating from the mobile application are captured and correlated with the Bank's central security infrastructure for improved monitoring and response.	Functionalities such as biometric authentication, device binding, secure PIN input, transaction risk scoring, in-app messaging are part of the mobile application development and not part of the runtime security SDK. Therefore, these features (biometric, device binding, risk scoring, etc.) should be made part of either Bank's mobile application stack development or another section / module.	Business/application functionalities such as biometrics, device binding, transaction risk scoring and in-app messaging shall remain with the Bank's application stack
730	43	7.3.3.2 Mobile SDK	Mobile SDK	Integration of Mobile SDK into the Bank's mobile application	Kindly confirm the number of mobile applications for which Mobile SDK integration is required.	Relevant details will be shared with the successful bidder
731	113	10.3 Technical Evaluation Criteria	Experience of Proposed OEMs	Support centre in India number of enterprise deployments number of BFSI deployments; number of deployments in India number of deployments of similar scale support commitment during contract period availability of local OEM office	Kindly specify the minimum/expected number of enterprise deployments, BFSI deployments, deployments in India and deployments of similar scale required for evaluation under this criterion.	The bidder to identify the OEMs with maximum number of deployments.
732	136	13.2 Right to Alter quantities	Terms & Conditions	The bank reserves the right, at the time of award of contract and/or during the currency of the contract, to increase or decrease the quantity of goods, licenses, subscriptions, appliances, equipment, services, implementation effort, support services, or any line item covered under the contract by up to twenty five percent (25%) of the quantities specified in the RFP/Contract, without any change in the unit prices, terms and conditions, technical specifications, delivery schedule, warranty obligations, support commitments, or any other contractual conditions.	Request the Bank to reduce the quantity variation under Clause 13.2 from ±25% to ±5%.	Please be guided by the RFP
733	205-207 214	15.21 Annexure 21: Sizing/Volumetrics, Data Retention and Current Infrastructure	Sizing/Volumetrics, Data Retention and Current Infrastructure	This Section has been watermarked Draft	This section is watermarked "Draft." Kindly confirm whether this section forms part of the final RFP and is applicable to bidders.	The mentioned section forms the part of the final RFP and is applicable to the bidders
734	73	AI Guardrails	Appendix 1A Functional Specification	The proposed solution should support over 30 languages (including East Asian and European) for AI inspection.	Kindly clarify the list of languages are to be supported for AI Guardrails	Please refer Addendum 1 for the revised clause.

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
735	74	AI Gateway	Appendix 1A Functional Specification	The Proposed solution's all components (on-prem HW or Software if any) should connect to management plane within India for any kind of monitoring/health checks of components. The proposed solution should have CSA STAR, SOC 2, CIS, ISO 27001, ISO 27017, ISO 27018 certification and must be a part of Microsoft Active Protections Program (MAPP)	Requesting bank to revise the certification requirements by removing CSA STAR, CIS, ISO 27017, ISO 27018, and the requirement for Microsoft Active Protections Program (MAPP) membership, and instead include ISO 42001 (Artificial Intelligence Management System). SOC 2 and ISO 27001 already provide comprehensive assurance of an organization's information security governance and operational controls, while the other certifications largely represent overlapping or domain-specific requirements. Further, MAPP is a vendor-specific program rather than an internationally recognized security certification. Considering the requirement pertains to "AI Security" solution, inclusion of ISO 42001 would better align the RFP with globally accepted best practices for responsible AI governance while encouraging wider participation from qualified solution providers without compromising security.	Please refer Addendum 1 for the revised clause.
736	General Recommendation	General Recommendation	General Recommendation	Given the evolving AI threat landscape and the criticality of AI systems in the banking environment, it is recommended that the Bank include the following capability within the AI Security specifications of the RFP.	Adversarial Testing Evaluates AI systems against adversarial techniques, including prompt injection and evasion attacks.	Please be guided by the RFP
737	General Recommendation	General Recommendation	General Recommendation	Given the evolving AI threat landscape and the criticality of AI systems in the banking environment, it is recommended that the Bank include the following capability within the AI Security specifications of the RFP.	Custom validation & multi-turn attacks Enables application-specific test design and execution of complex, multi-turn attack scenarios.	Please be guided by the RFP
738	General Recommendation	General Recommendation	General Recommendation	Given the evolving AI threat landscape and the criticality of AI systems in the banking environment, it is recommended that the Bank include the following capability within the AI Security specifications of the RFP.	Automated OWASP reports Delivers configurable assessment reports with success/failure outcomes mapped to OWASP LLM Top 10 risks.	Please be guided by the RFP
739	General Recommendation	General Recommendation	General Recommendation	Given the evolving AI threat landscape and the criticality of AI systems in the banking environment, it is recommended that the Bank include the following capability within the AI Security specifications of the RFP.	Regulatory test patterns Enables test scenarios to be tailored to regulatory requirements and advisories.	Please be guided by the RFP
740	General Recommendation	General Recommendation	General Recommendation	Given the evolving AI threat landscape and the criticality of AI systems in the banking environment, it is recommended that the Bank include the following capability within the AI Security specifications of the RFP.	Agentic AI, MCP, workflows Extends red-team coverage across AI applications / agents, MCP, and other multi-step agent workflows	Please be guided by the RFP
741	General Recommendation	General Recommendation	General Recommendation	Given the evolving AI threat landscape and the criticality of AI systems in the banking environment, it is recommended that the Bank include the following capability within the AI Security specifications of the RFP.	Multimodal robustness Assesses resilience against attacks delivered through text, image, audio, and other supported modalities.	Please be guided by the RFP
742	General Recommendation	General Recommendation	General Recommendation	Given the evolving AI threat landscape and the criticality of AI systems in the banking environment, it is recommended that the Bank include the following capability within the AI Security specifications of the RFP.	Multilingual adversarial testing Tests AI models against adversarial techniques across multiple languages and linguistic variations.	Please be guided by the RFP
743	General Recommendation	General Recommendation	General Recommendation	Given the evolving AI threat landscape and the criticality of AI systems in the banking environment, it is recommended that the Bank include the following capability within the AI Security specifications of the RFP.	Board-level dashboards Provides executive-level AI risk visibility through Board dashboards and accountability reporting aligned with RBI technology-risk oversight expectations.	Please be guided by the RFP
744	General Recommendation	General Recommendation	General Recommendation	Given the evolving AI threat landscape and the criticality of AI systems in the banking environment, it is recommended that the Bank include the following capability within the AI Security specifications of the RFP.	Adaptive stress testing Employs adaptive, intelligence-driven attack generation rather than relying solely on predefined / static test checklists.	Please be guided by the RFP
745	General Recommendation	General Recommendation	General Recommendation	Given the evolving AI threat landscape and the criticality of AI systems in the banking environment, it is recommended that the Bank include the following capability within the AI Security specifications of the RFP.	Sensitive-data detection Identifies sensitive information and harmful content using contextual and semantic analysis instead of simple keyword matching, including obfuscated or contextually hidden data.	Please be guided by the RFP
746	General Recommendation	General Recommendation	General Recommendation	Given the evolving AI threat landscape and the criticality of AI systems in the banking environment, it is recommended that the Bank include the following capability within the AI Security specifications of the RFP.	Atypical/stressed scenarios testing Enables bank to evaluate model resilience across edge cases, abnormal conditions, manipulation attempts, and adversarial situations.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
747	General Recommendation	General Recommendation	General Recommendation	Given the evolving AI threat landscape and the criticality of AI systems in the banking environment, it is recommended that the Bank include the following capability within the AI Security specifications of the RFP.	Deep model analysis Provides model-level security analysis covering model structure, weights, artifacts, and dependencies to identify risks beyond known vulnerability databases.	Please be guided by the RFP
748	General Recommendation	General Recommendation	General Recommendation	Given the evolving AI threat landscape and the criticality of AI systems in the banking environment, it is recommended that the Bank include the following capability within the AI Security specifications of the RFP.	Internally hosted model validation Allows Bank's teams to configure the solution to use and assess privately hosted models within the Bank's environment without exposing model data to external providers.	Please be guided by the RFP
749	General Recommendation	General Recommendation	General Recommendation	Given the evolving AI threat landscape and the criticality of AI systems in the banking environment, it is recommended that the Bank include the following capability within the AI Security specifications of the RFP.	Comprehensive model lineage Generates a comprehensive AI-BOM covering model artifacts, files, libraries, and dependencies, with support for CERT-In requirements and the latest SPDX format.	Please be guided by the RFP
750	5	Appendix 1B, Backup Solution & Storage	38	The proposed solution must support LAN-Free (SAN/FC/iSCSI) transport for image-level VM backups on supported block-storage hypervisor platforms, and must ensure that on all other platforms backup data traverses a dedicated backup network/fabric isolated from production LAN traffic, such that no backup payload transits the production Ethernet infrastructure.	The proposed solution must support LAN-Free (SAN/FC/iSCSI) transport for image-level VM backups on supported block-storage hypervisor platforms, and must ensure that on all other platforms backup data traverses a dedicated backup network/fabric isolated from production LAN traffic, such that no backup payload transits the production Ethernet infrastructure. Justification: SAN transport carries its own risk. Direct SAN Access requires production LUNs to be presented to the backup proxy; a misconfigured Windows proxy can initialise/sign a production LUN. Many banks deliberately restrict SAN transport for this reason, which is worth mentioning if the Bank asks why the clause should be softened.	Please be guided by the RFP
751	5	Appendix 1B, Backup Solution & Storage	40	Backup storage/Appliance capacity expansion - whether by adding disks, adding an enclosure, or adding scale-out nodes - must be non-disruptive, and no additional storage-side licence shall be required to consume the expanded capacity where the backup software''s protected-capacity licence already covers the data being protected.'	Is the backup software required to be licensed strictly on a capacity basis, or is an instance/workload-based licence (per VM, per physical server, per database instance, per NAS TB) also acceptable? Justification: Many Backup Software OEM offer Node based licensing with unlimited capacity. While capacity-based licensing is still prevalent in the industry, we have seen a gradual shift to other licensing models which are more flexible and makes procuring the software more cost effective like Instance or Node based model. By giving option for Node -based licensing your overall TCO would reduce dramatically.	Please be guided by the RFP
752	43	IDAM	Life Cycle Management	The solution must support full lifecycle management of user's machine identities and access governance using cryptographic keys. This includes automated provisioning and deprovisioning to minimize the risk of credential sprawl and unauthorized access	1) Please clarify the use cases for access governance using cryptographic keys. 2) Would it mean that Bank wants to do the Governance on the Identities of All Target System(All OS, Network Device, Security Devices, Database), Same as IGA ?	1) Please be guided by the RFP 2)Bank wants to do the Governance on the Identities of All Target System(All OS, Network Device, Security Devices, Database) using cryptographic keys
753	43	IDAM	Life Cycle Management	For access via CLI (console, Telnet, SSH), WBM and Web Services (HTTPS) users can be authenticated via RADIUS/ TACACS+ or via local table of authorized users.	Does it mean that the Bank would like to have AAA Capability within the IDAM/PAM to do fill integration with network devices ?	The proposed solution should support RADIUS and other relevant protocols for integration.
754	47	MFA	Technical Specification MFA	For access via CLI (console, Telnet, SSH), WBM and Web Services (HTTPS) users can be authenticated via RADIUS/ TACACS+ or via local table of authorized users.	Does it mean that the Bank would like to have AAA Capability within the MFA to do fill integration with network devices ?	The proposed solution should support RADIUS and other relevant protocols for integration.
755		PIM/PAM	Generic		Is Bank Looking for Just Enough privilege for Just In Time (Provisioning/ Deprovisioning) for all Infrastructures Assets(OS, Network Device, Security Device, Database) ?	Please be guided by the RFP
756			Generic		Is Bank looking to Secure Outside PIM/PAM Access ?	Please be guided by the RFP
757		PIM/PAM	Eligibility Criteria	Generic	We recommend if the Bank can add the Below Points for the PIM/PAM Eligibility Criteria: A) Proposed PIM/PAM Solution should have the Presence in India for more than 10 Years B) Proposed PIM/PAM OEM by the Bidder should have the Annual Average Turnover for last three Years should be more than INR 60Cr. C) The offered PAM OEM Solution must be certified for Common Criteria Certificate EAL 2+ and supporting certificate document should be submitted during the bid submission.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
758	72	7.11 Resource Requirement	7.11, MINIMUM RESOURCE COUNT DEPLOYMENT table, Pg.72	The Minimum Resource Count table specifies a dedicated minimum of "1" L3/Project Manager - Operations resource for Shift A only, while the corresponding cell for Shift B and Shift C reads "Bidder to right size" with no minimum floor prescribed.	Kindly confirm whether a dedicated onsite L3/Project Manager - Operations resource is mandatorily required for Shift B and Shift C as well (i.e., 24x7 coverage for this role), or whether this role is required only during Shift A (business hours), with Shift B/C coverage for escalations left entirely to the bidder's discretion.	the bidder must right-size to meet SLA/operational obligations of the RFP
759	27, 72-73	7 Scope of Work / 7.11 Resource Requirement	Section 7 (Solution list) vs 7.11, Security Layer resource-mapping table, Pg.73	Section 7 lists 21 solutions to be procured under this RFP, however the "Security Layer" table in Section 7.11 (mapping solutions to Shift-wise L1/L2/L3 resource competency) shows a domain-wise solution count that totals 20 (Perimeter & Network: 6, Endpoint: 3, Data Security: 2, Application and Management layer: 9), not 21.	Kindly clarify which of the 21 solutions is not reflected in the Security Layer resource-mapping table (or confirm the correct domain-wise solution-to-resource mapping), since this table is used to determine the minimum onsite L1/L2/L3 competency coverage the bidder must staff for.	Please refer Addendum 1 for the revised clause. All 21 solutions/ services to be factored.
760	70, 72, 74	7.11 Resource Requirement	7.11, Resource Deployment/Governance clauses, Pg.70 & 74	The RFP states resources "may be deployed at the Bank's IT Security Office, Data Centre (DC), Disaster Recovery (DR) Site, SOC, Branches, or any other location as specified by the Bank," while the Minimum Resource Count table (Pg.72) specifies a single set of shift-wise minimum headcounts (e.g., 3 L1 in Shift A) without indicating whether this is a per-location or an overall/cumulative minimum.	Kindly confirm whether the minimum shift-wise resource counts specified in Section 7.11 (L1/L2/L3/IT Infra) apply as a single overall/cumulative minimum across all Bank locations (IT Security Office/DC/DR/SOC), or whether the same minimum count must be separately deployed at each such location.	The minimum resource count under Section 7.11 is an overall/cumulative minimum, not a per-location requirement. Bidder shall deploy as directed by the Bank within this cumulative minimum.
761	73	7.11 Resource Requirement	7.11, Pg.73 ("SME resources may be shared across domains and shifts")	The RFP requires the bidder to "provide appropriately qualified SMEs for the respective technology domains" and permits SME resources to be "shared across domains and shifts," but no minimum SME headcount, shift coverage, or onsite/offsite requirement is specified anywhere in the Minimum Resource Count table or elsewhere in Section 7.11.	Kindly confirm whether a minimum number of dedicated SME resources (onsite or offsite) is expected per shift/domain, or whether SME staffing levels and coverage model are entirely at the bidder's discretion, subject only to meeting SLAs.	The bidder shall deploy appropriately qualified SMEs in adequate numbers to meet all contractual obligations, SLAs, service continuity requirements and Bank requirements. The Bank reserves the right to require additional resources where service performance or operational requirements so warrant, without compromising SLA obligations.
762	70	7.11 Operations and Maintenance (O&M) Phase:	7.11, Page 70 Operations and Maintenance (O&M) Phase	The respective OEMs shall provide L3 support resources and subject matter experts from the date of installation and throughout the contract period to support operations, troubleshooting, optimization, upgrades, audits, and major incidents.	Kindly confirm whether bidder has to provide a dedicated OEM L3 support resource for complete O&M Phase or jus for managing SLA on need basis.	The bidder shall ensure timely availability of OEM L3 SMEs for operations, troubleshooting, optimization, upgrades, audits and major incidents. Any delay attributable to OEM support shall remain the bidder's responsibility.
763	70	7.11 Resource Management and Governance	7.11, Page 70 Minimum transition and knowledge transfer periods	The following minimum transition and knowledge transfer periods shall be adhered to in case of resource replacement: • Project Manager: 60 Days • Key Personnel: 45 Days • Other Personnel: 30 Days	We request to Bank amend this clause as esource replacement: • Project Manager: 30 Days • Key Personnel: 15 Days • Other Personnel: 7 Days	Please be guided by the RFP
764	76	7.12 Facilities Management	7.12 Page 76 point 6 : Monthly Security Certificate	Starting from Go-Live date of the respective security solutions, 7th day of every month: Monthly Security Certificate to be submitted by the Project Manager of the bidder and onsite resources	We request to modify this clause as bidder PM has to submit the letter after getting confirmation from OEM/OEM PS over mail. OEM/PS can share confirmation on statement over mail as it is monthly activity.	The bidder shall submit the monthly security certificate within the prescribed timeline. OEM confirmation may be used as supporting evidence; however, responsibility for obtaining OEM confirmation and submitting the certificate to the Bank shall remain with the bidder.
765	104	Main RFP Document	10.2 Eligibility Criteria/Clause - OEM Evaluation Criteria	Pt 18. The proposed OEM solution/product should have been successfully implemented in least two Scheduled Bank (Including Financial Regulator) 14. DAM	We kindly request bank to allow Govt/PSU/BFSI/Critical Infrastructure organizations as well for wider participation.	Please be guided by the RFP
766	30, 31	7.1	D.	S-BOM, CBOM, AIBOM and QBOM To provide centralized discovery, inventory,governance, and continuous monitoring of software components, cryptographic assets, AI models, and quantum-vulnerable dependencies across the Bank's IT environment. The solution shall identify security, compliance, software supply chain, cryptographic, AI, and post-quantum risks while supporting vulnerability management, crypto-agility, AI governance, and regulatory compliance through a unified Bill of Materials (BOM) framework.	Please clarify whether the proposed solution must provide IT asset auto-discovery and inventory, continuously updated asset documentation, configuration monitoring, and configuration drift/change detection, with historical visibility and reporting, to support continuous risk exposure management, audit readiness, Governance and compliance assurance.	Please be guided by the RFP, Any activity requird to meet the scope and Functional requirement is to be performed by the proposed solution
767	105	10.2 Eligibility Evaluation Criteria Point no. 19	(OEM Evaluation Criteria)	The proposed OEM solution/product for Privilege Identity/Access Management should have been successfully implemented in at least 2 BFSI in India, out of which at least one (1) BFSI Client should have a deployment covering more than 1,500 privileged users	The proposed OEM solution/product for Privilege Identity/Access Management should have been successfully implemented in at least one (2) BFSI Client should have a deployment covering upto 500 privileged users Justification: Privileged user count reflects the client's organization size, not the OEM solution's capability or maturity. Restricting eligibility to a single 1,500-user reference limits competition to very few OEMs and may reduce the Authority's options. We request the clause be revised to "minimum 2 BFSI clients in India, each with upto 500 privileged users", a more balanced, industry-standard benchmark that still validates proven BFSI experience while enabling wider, competitive participation.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
768	211	15.21.4 Deployment & Data Retention	PIM (Volumetrics)	1. User Licenses: 750 User (Day 1) scalable to 1500	Kindly confirm whether resource sizing (hardware/VM specifications, HA/DR architecture, and performance benchmarking) should be designed for 750 users at Day 1 with a scale-up path to 1,500, or whether the infrastructure must be sized for 1,500 users from Day 1 itself. This clarification is required for bidders to propose accurate and cost-optimized sizing.	On day 1 bidder to factor the licenses for the sought requirement, however, for scalable requirements, bank will procure licenses as per rate card/ pro rata basis. However, the proposed solution should be architected to support the scalability
769	206	15.21.3 Current IT assets	Branches	4. Desktops with various agents like AV, DLP, NAC, ITAM etc. 12000 5. Routers & Switches 7200	Kindly clarify the network connectivity between branches and DC/DR (MPLS/SD-WAN/VPN, bandwidth/latency, firewall/NAT policies). This will determine whether PAM gateways at DC/DR can reach branch-level routers/switches, or if local gateways are needed at branches.	Details will be shared with the successful bidder
770	203	15.21 Annexure 21: Sizing/Volumetrics, Data Retention and Current Infrastructure	Non-Production Environment	For VM-based solutions, the non-production environment shall be sized at a minimum of 10% of the Production (DC) environment unless otherwise specified in the RFP.	Kindly confirm whether the non-production environment is required as a standalone/single-node setup, or must also include HA/DR replication similar to Production. This impacts BOQ for additional nodes/DR components for non-prod	Non production environment is to be proposed in standalone mode.
771	49	Appendix 1A Functional Specification.pdf Point no. 25	Certificate Management	The solution shall support management of privileged certificates and cryptographic identities.	This is not a core feature of PAM. It typically falls under a different use case and is usually handled by a separate product/solution	The Key Discovery capability should support the discovery of a broad range of secrets, cryptographic keys, credentials, API tokens, certificates, etc. across enterprise environments.
772	51	Appendix 1A Functional Specification.pdf Point no. 89	Certificate Lifecycle	The solution should support lifecycle management of digital certificates used for privileged access.	This is not a core feature of PAM. It typically falls under a different use case and is usually handled by a separate product/solution	Please be guided by the RFP
773	1	KMS	3	The system should support AES(128-256), ARIA,ECC(224-512), Brainpool curves, HMAC , TDES, RSA(512-4096) and the Crypto mode (CBC, CBC-CS1,ECB,GCM) etc.	Please note that RSA 512 and 1024 are not FIPS approved algorithms. Hence, we would humbly request to ammend this specification to mention RSA (2048-4096). Please remove CBC-CS1 as it's specific to a particular OEM.	Please refer Addendum 1 for the revised clause.
774	1	KMS	4	The system should support API REST (JWT),SOAP, KMIP, PKCS#11, JCE, .NET, MSCAPI, MS CNG, C,NAE,XML, Java API's and libraries for integration with custom applications.	Please note that some of the APIs such as NAE XML are specific to a particular OEM. Humbly request the bank to please remove the above ones.	Please refer Addendum 1 for the revised clause.
775	1	KMS	5	The System shall support Multi-tenancy using multiple domains, Clustering, High Availability and Backup.	Multiple domains is a concept specific to a particular OEM. Humbly request the bank to please modify it to multiple domains or multiple vaults or multiple tenants.	Please refer Addendum 1 for the revised clause.
776	1	KMS	8	Solution should support Multi Factor Authentication (MFA) for users accessing protected path on Windows Servers either throught inbuilt feature or intergrating with the bank's MFA solution.	Please note that this specification is applicable to traditional agent based file encryption tools which are endpoint based and it seems that this requirement is specific to a particular OEM. Modern file encryption solutions use agentless techniques for file/folder encryption. For an agentless file encryption solution, authentication and access control are typically enforced through the existing enterprise identity and access management framework, including Active Directory, LDAP, SSO, and MFA platforms. Requiring the encryption solution to independently provide MFA functionality may unnecessarily restrict participation by solutions that leverage the Bank's established security controls rather than duplicating them. We humbly request the bank to please modify it to this specification. Solution should support Multi Factor Authentication (MFA) for users accessing protected path on Windows Servers either throught inbuilt feature or intergrating with the bank's MFA solution OR by leveraging authentication and access control that are typically enforced through the existing enterprise identity and access management framework, including Active Directory, LDAP, SSO, and MFA platforms ELSE Please remove this clause	Please refer Addendum 1 for the revised clause.

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
777	1	KMS	14	The Key Discovery tool should be able to be managed from the KSM console and should be able to discover secrets like AES Key, AWS Key ID, Azure Storage Key, Mailchimp Access Key, Private Key, SendGrid API Key, SSH Private Key, SSH Public Key, Stripe Access Key, TDES Key, Twilio API Key, RSA Key, PGP Key, ECC Keys, Asymmetric Keys etc.	We would request to specify which type of keys are there in bank's environment. This specification should be part of a Data discovery solution and specific to a particular OEM.	Please refer Addendum 1 for the revised clause.
778	1	KMS	19	The Solution supports capability to protect data through encryption or tokenization using a FIPS 140-2 level 3 compliant solution.	Please update the specification to FIPS 140-3 Level 3, since FIPS 140-2 is moving to historical on 21st September.	Please refer Addendum 1 for the revised clause.
779	1	KMS	44	HSM should have FIPS 140-3 Level 3 security certification (with certification in the name of OEM)	Since HSMs are a critical component and act as a Root of Trust in a data security landscape, hence it's of utmost importance that OEM should not use a whitelabelled FIPS 140-3 certification of another OEM and all approved algorithms should be in the name of OEM, not 3rd party. We would request the bank to please additionally mention the below clause: Rebranded, private label, or third party sourced cryptographic modules are not permitted. The FIPS 140-3 security policy of the HSM should not have any references to a third party certified firmware.	HSM should have FIPS 140-3 Level 3 security certification (with certification in the name of OEM). Rebranded, private label, or third party sourced cryptographic modules are not permitted. The FIPS 140-3 security policy of the HSM should not have any references to a third party certified firmware.
780	1	KMS	52	The HSM OEM should provide a software-based simulator, virtual HSM, or equivalent development environment to facilitate application integration, testing, and validation. The simulator/virtual HSM/Development environment should support standard HSM interfaces/APIs and enable remote connectivity over the network wherever applicable. Availability of such simulator/ virtual HSM/Development environment shall be provided by the OEM without additional licensing cost to the bank.	In HSMs world, simulators are usually not provided considering HSMs as Root of Trust and secure devices. Hence physical test devices can be provided for application integration. We would request the bank to include test HSM devices as well.	The HSM OEM should provide a software-based simulator, virtual HSM, test HSM or equivalent development environment to facilitate application integration, testing, and validation. The simulator/virtual HSM/Development environment should support standard HSM interfaces/APIs and enable remote connectivity over the network wherever applicable. Availability of such simulator/ virtual HSM/Development environment shall be provided by the OEM without any additional licensing cost to the bank.
781	1	KMS	55	The HSMs must be in Secure Transport Mode (STM), to ensure HSM have not been altered while in transit	Please note that HSMs include tamper evident packaging for physical security perspective. This specification seems to be applicable to a particular OEM. We would request the bank to include tamper evident packaging labels as well.	Please refer Addendum 1 for the revised clause.
782	1	KMS	56	HSM should support the backup on FIPS certified hardware device, not to file in any form.	Please note that FIPS 140-3 guidelines never mention using only backup HSM devices for backups. This increases the cost of the overall solution substantially. We would request the bank to modify as "HSM should support the backup as per FIPS 140-3 guidelines".	Please refer Addendum 1 for the revised clause.
783	Technical Specification	MFA	6	Solutions should be capable for integration with TACACS solution being used by the Bank.	TACACS is single OEM specific. However we support SAML and RADIUS.	Please refer Addendum 1 for the revised clause.
784	Technical Specification	ZTNA	7,21	Solution should have Zero trust security and Digital Experience Management (DEM) from Day 1 using the same Endpoint Agent and single management console for both capabilities.	DEM is OEM single specific name, however we provide similer features which DEM is providing.	Please be guided by the RFP
785	203-204	15.21.1	Existing and Envisaged Stack	Tools Integration	Is this project is just of Migration or need to introduce new tools to fulfill the integration requirement?	The project covers supply and implementation of the proposed IT Security Solutions along with migration of the existing IT and security solutions and integration with the Bank's existing security ecosystem. The bidder shall be responsible for implementing the proposed solutions and migrating applicable data, configurations, policies, rules, telemetry, logs, parsers, metadata, integrations and customizations from the existing solutions. The proposed solutions shall also be integrated with the Bank's existing and future security platforms as specified in the RFP.

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
786	40	7.3.2.2	Data Loss Prevention	Advanced DLP	Explain OCR, EDM, Fingerprinting, IDM, Image Analysis and Source Code Detection.	OCR- OCR to extract and inspect sensitive information from images and scanned/image-based PDFs and apply DLP policies. EDM- Exact Data Matching to identify sensitive information against defined structured/reference data sets, helping improve detection accuracy and reduce false positives. Fingerprinting: DLP supports fingerprinting of structured and unstructured data and can identify complete or partial matches of protected information for DLP enforcement. IDM: indexed/content-based identification of protected documents and content for detection and policy enforcement. Image Analysis: Inspect image content using OCR and apply DLP policies to sensitive information identified within images/scanned documents. Source Code Detection: Identifying source-code content and applying appropriate DLP policies.
787	40	7.3.2.2	Data Loss Prevention	DLP Incident Management	Explain incident workflow, escalation, disposition, and closure process.	The Indicative process flow is as follows: Detect → Alert → Prioritize → Assign → Investigate → Escalate → Remediate/Disposition → Close → Audit. The Incident management workflow shall be discussed and finalised with the successful bidder
788	40	7.3.2.2	Data Loss Prevention	DRM-DLP Integration	Can DLP automatically trigger DRM based on classification?	Connector/classification-based integration. Sensitive documents identified/classified by DLP can be automatically DRM-protected before download/distribution.
789	41	7.3.2	Information/Digital Right Management	Data Discovery	Explain discovery across databases, file shares, endpoints, M365, SharePoint, Teams and cloud repositories.	Solution should provide centralized discovery, visibility and protection of enterprise data across endpoints, file shares and cloud repositories. Through its integration with DLP/content-discovery solutions, Solution should support discovery and identification of sensitive data across databases, M365, SharePoint, Teams and other enterprise repositories, followed by policy-based DRM protection.
790	41	7.3.2	Information/Digital Right Management	Data Classification	Explain classification methodology and supported classifications (PII, PAN, Aadhaar, PCI, SWIFT, Financial Data).	Solution should support classification-based protection and integration with DLP solutions for content-aware classification. PII, PAN, Aadhaar, PCI, SWIFT, Financial Data and other sensitive information can be identified using keywords, dictionaries, Regex, fingerprinting, EDM and other data classifiers. Based on the classification, Solution shall automatically apply the appropriate DRM policy.
791	41	7.3.2	Information/Digital Right Management	DRM/IRM	Explain persistent protection beyond Bank network.	Persistent protection beyond Bank network: Protection remains with the information even when files are downloaded, copied or shared outside the Bank network. Access and usage rights continue to be enforced based on authorized users, devices, locations, time and configured policies.
792	41	7.3.2	Information/Digital Right Management	DRM Features	Explain watermarking, expiry, revocation, geofencing and external sharing control.	Solution should provide comprehensive DRM controls including dynamic watermarking, expiry, remote revocation, geofencing/location-based access control and external sharing controls. Policies can control viewing, editing, printing, copy/paste, forwarding and downloading. All relevant access and usage activities can be audited
793	41	7.3.2	Information/Digital Right Management	DRM Formats	Confirm support for Office, PDF, Images, CAD, ZIP and custom file formats.	Solution should provide format-independent protection, enabling protection of Office documents, PDF, images, ZIP and other/custom file formats. Protection to be applied to the information irrespective of the original file format, enabling persistent control beyond the Bank perimeter.
794	109	10.2 Eligibility Evaluation Criteria	Note regarding NextGen SOC RFP	Reference to a separate NextGen SOC RFP	Kindly provide the RFP Number, procurement status, award status, OEM details, implementation timeline, and expected integration readiness date of the referenced NextGen SOC RFP, as successful implementation of multiple solutions under this RFP is dependent upon integration with SIEM, SOAR, UEBA, TIP, and SOC Big Data Lake platforms.	Please keep referring the bank's RFP as well as the GeM portal for updates on the NextGen SOC RFP
795	33	Cyber Security Incident	Incident Response	Bidder to notify cyber incidents within 6 hours and support investigations.	Please clarify the roles and responsibilities between the NextGen SOC vendor and IT Security solution vendor during incident detection, investigation, containment, and closure.	Please be guided by the RFP
796	40	7.3.2.1	CASB	Integration with SIEM, SOAR, DLP, XDR, TIP and SOC platforms.	Please provide details of available APIs, syslog formats, and connector standards supported by the Bank's SOC platform.	The Bank shall provide relevant integration specifications and available interface details during the design/implementation phase. The bidder shall use standard APIs, syslog and supported connector mechanisms. Absence of a specific connector does not automatically exclude integration; the bidder shall provide an appropriate supported/custom integration mechanism within the RFP scope.
797	35	7.3.1.3	DNS Protection	Connectivity with SIEM, SOAR, Zero-Day Attack Protection, TIP, Firewall and DLP.	Is the bidder expected to develop/customize SOC parsers and correlation rules, or will this responsibility remain with the NextGen SOC vendor?	The bidder shall provide the required solution-side integration, log forwarding and supported parser/connector configuration Where custom parser/use-case development is required as part of the proposed solution integration, it shall be delivered by the bidder/OEM within scope.
798	36	7.3.1.4	Web Gateway	Integration with DLP, SIEM, and IT Security solutions.	Please confirm the number of correlation rules, and SOC use cases expected from Web Gateway integration.	The bidder shall provide the required integration and relevant standard security use cases. Exact quantity shall be finalized during detailed design based on Bank requirements, available telemetry and SOC use cases

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
799	43-44	7.3.4.1	HIPS	Customized dashboards and incident visibility.	Kindly clarify whether creation and maintenance of SOC dashboards within SIEM is in scope of this RFP or the NextGen SOC project.	Proposed Product-native dashboards shall be configured by the bidder. Central SOC/SIEM dashboards shall be coordinated with the SOC implementation team. The bidder shall provide all required data feeds, fields, APIs and solution-specific dashboard inputs necessary for effective centralized visibility.
800	45	7.3.4.2	WAF	Integration with SIEM and SOAR solutions.	Clarify on the WAF-related use cases and correlation rules required.	WAF shall be integrated with SIEM/SOAR, with relevant security events and WAF attack/use cases enabled. Detailed use cases and correlation rules shall be finalised during design based on the Bank's approved SOC use-case catalogue.
801	49	7.3.5.2	DNS Security Services	Integration logs with SIEM and other security tools.	Please provide details of log retention, archival, and storage requirements at SOC/SIEM level for DNS logs.	Please be guided by the RFP
802	63-65	7.6	Cloud Service Provider Responsibilities	Centralized monitoring, logging, audit trails and reporting.	Kindly provide cloud log source inventory and their onboarding status within the current/proposed SOC platform.	Relevant information and inventory available with the Bank shall be shared during the appropriate project stage.
803	76	7.12	Facilities Management	Reduction of MTTD and MTTR using technology and SOAR.	Please provide baseline MTTD and MTTR values against which performance improvements will be measured.	Please be guided by the RFP
804	78	7.12	Facilities Management	Auto alert if logs are not received for 15 minutes.	Please clarify whether log source monitoring and health monitoring are managed by SOC vendor or solution vendor.	Solution-level health monitoring shall be provided by the bidder for the in-scope solutions. The bidder remains responsible for ensuring that the solution generates the required health/status information and that failures affecting SLA compliance are promptly identified and addressed.
805	79	7.12.1	Continual Improvement	Threat management, alert management, rules creation and fine-tuning.	Please clarify ownership of continuous SOC use-case tuning, alert tuning, false-positive reduction and threat hunting activities.	The bidder shall remain responsible for solution-specific rule configuration, tuning and technical optimisation necessary for effective operation.
806	82-85	7.12.3	IT Security Operations	Monitoring, incident management and analytics.	Kindly provide the expected number of custom SOC use cases, correlation rules, dashboards and playbooks to be delivered by the successful bidder.	Please be guided by the RFP
807	84	7.12.3	Performance Monitoring	Monitoring and management of applications and security platforms.	Kindly confirm whether the bidder is required to integrate with existing SOC monitoring tools or provide additional monitoring capabilities.	The Bidder shall integrate applicable proposed solutions with the Bank's designated SOC/security monitoring platforms. Solution-native monitoring, alerting and health monitoring shall be configured as applicable.
808	111-113	10.3	Technical Evaluation	Technical Architecture & Solution Design.	Kindly provide the target-state cybersecurity architecture showing interactions between NextGen SOC and all requested security solutions.	Bidder to design the architecture for IT Security solution and its interaction with other tools and services running/ to be procured in the bank
809	111-113	10.3	Technical Evaluation	Operations, Managed Services & SLA.	Please confirm whether SOC operations are handled by a separate vendor and provide the RACI matrix between SOC vendor and IT Security vendor.	Details will be shared with the successful bidder
810	27-32	7.1	Scope of Work	Centralized visibility, monitoring, detection, prevention and response.	Please provide the Bank's expected SOC operating model, including L1/L2/L3 responsibilities.	The details shall be shared with the successful bidder
811	32	7.1	Scope Note 8	Dynamic dashboards and reports.	Kindly share sample executive, operational, compliance, and regulatory dashboards expected from SOC integrations.	The details shall be shared with the successful bidder
812	33	7.2	RACI Matrix	Incident Management	Please clarify if incident triage and incident closure ownership will reside with the SOC vendor or the individual technology vendor.	The Bank/SOC shall retain overall security incident management and coordination. The Bidder/OEM shall be responsible for technical triage, investigation, remediation and resolution of incidents attributable to the respective in-scope solutions, in accordance with the applicable SLA and escalation matrix.
813	76-83	7.12	Facilities Management Services	Automation through SOAR.	Kindly provide details of existing SOAR platform, number of active playbooks, and expected integrations under this project.	The details shall be shared with the successful bidder
814	97	9	Project Timelines	Overall implementation period is 5 months.	Since multiple solutions require mandatory SIEM, SOAR, UEBA, TIP and SOC-Big Data Lake integration, please clarify dependency management and timeline relaxation in case the NextGen SOC platform is not available during implementation.	Please be guided by the RFP
815	68	7.9	Executive Governance and Project Oversight	Nomination of Project Sponsor / Project Director for the engagement	Is there a requirement of Bidder's PMO to be deployed for governance and oversighting the overall engagement?	Please be guided by the RFP
816	68	7.9	Executive Governance and Project Oversight	Nomination of Project Sponsor / Project Director for the engagement	Please confirm the frequency of governance meetings, strategy workshops, presentations and executive review meetings that requires participation of Project Sponsor / Director.	Please be guided by the RFP
817	79	7.12.1	Continual Improvement	Review and Updating of policies & procedures	Please confirm if Bank has design level policies & procedures established for existing tools and processes within the Bank or bidder is required to develop all the policies & procedures from baseline?	The Bidder shall review applicable Bank policies, standards and procedures and shall prepare/update solution-specific policies, SOPs, operational manuals and hardening/configuration guidelines required for the in-scope solutions.
818	79	7.12.1	Continual Improvement	Review and Updating of policies & procedures	Please confirm whether Bidder need to develop and update policies & procedures related to all tools and solutions implemented within the Bank. Also, please confirm whether hardening guidelines needs to be updated by the Bidder on behalf of Bank.	The Bidder shall develop/review/update policies, SOPs and hardening guidelines specifically applicable to the solutions implemented under this RFP
819	91	7.13	IT Infrastructure	Governance, SLA Compliance & Service Delivery Management	Please confirm whether any specific GRC tools, reporting templates, compliance frameworks, or regulatory standards are mandated by the Bank for service delivery and compliance management.	Please be guided by the RFP
820	91	7.13	IT Infrastructure	Internal, External and regulatory audits	Kindly clarify the expected scope of support for internal, external, and regulatory audits, including audit frequency, response timelines, and any requirements for dedicated audit coordination resources.	The Bidder shall provide technical and documentary support for internal, external and regulatory audits relating to the in-scope solutions during the contract period.
821	91	7.13	IT Infrastructure	Internal, External and regulatory audits	Please confirm how many internal, external and regulatory audits will be conducted in a calendar year.	Please be guided by the RFP
822	68	7.9	Executive Governance and Project Oversight	Dashboard and Reporting	Please specify the total number of Dashboards and Reports required to be submitted by the Bidder along with frequency / timelines	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
823	68	7.9	Executive Governance and Project Oversight	Dashboard	Please specify the expectation and frequency around Management Dashboarding?	Please be guided by the RFP
824	97	9	Project Timelines	Project Implementation Start Date	Please confirm tentative start date when bank has planned to commence the overall project	Please be guided by the RFP
825	N/A	N/A	RFP Query	Overall query	The RFP mandates integration with SIEM, SOAR, UEBA, TIP and SOC Big Data Lake. Kindly clarify whether the SOC Big Data Lake platform is already deployed, under implementation, or being procured under the separate NextGen SOC RFP. Please provide OEM details, architecture, log ingestion mechanisms, retention requirements, and integration specifications.	The successful bidder shall be responsible for integrating the proposed IT Security Solutions with the Bank's existing security platforms, as specified in the RFP. The Bank is also in the process of procuring a new vendor for implementation of its NextGen SOC solution under a separate RFP, which is currently under process. If the NextGen SOC is implemented first, the bidder shall integrate the proposed IT Security Solutions with the newly implemented NextGen SOC platform. If the IT Security Solutions are implemented first, the bidder shall integrate with the Bank's existing security platforms and subsequently with the newly implemented NextGen SOC solution. All such integration requirements shall be included within the bidder's scope.
826	48-49	7.3.5.1	PIM/PAM	Privileged account management.	Kindly provide current and projected numbers of privileged users, service accounts and integrations to be considered for sizing.	Please be guided by the RFP
827	27-32	7.1	IT Security Solutions & Services	Multiple solutions to be deployed across DC, DR and Cloud environments.	Kindly provide detailed sizing inputs including users, servers, databases, applications, branches, bandwidth, storage, EPS/FPS, certificates, privileged users, mobile users, and expected growth for each solution for accurate sizing and commercial estimation.	Please be guided by the RFP. Refer Section 15.21.4Deployment & Data Retention
828		Server - Internal Storage		Server should be supplied with 2x 1.92TB NVMe SSD or higher. Bank will not return the defective disk(s) in case of disk failure	Server should be supplied with 2x 1.92 3.2TB NVMe SSD or higher. Bank will not return the defective disk(s) in case of disk failure	Please be guided by the RFP
829		Server - Internal Storage		The Server hardware RAID controller should support the following configurations RAID 0, 1, 5, 6, 10, 50, and 60. The raid controller should have minimum 4GB NV cache or higher	The Server hardware RAID controller should support the following configurations RAID 0, 1, 5, 6, 10, 50, and 60. The raid controller should have minimum 4 8GB NV cache or higher	Please be guided by the RFP
830	3	SAN Switch		The switch should support auto-sensing 64,32,16, 8 Gbit/sec FC capabilities.	The switch should support auto-sensing 64,32,16, 8 Gbit/sec FC capabilities.	Please be guided by the RFP
831	5	Backup Solution		Proposed backup software must support Multi-Tenancy feature.	Proposed backup solution should support Multi-Tenancy feature	Please be guided by the RFP
832	17	Backup Solution		Proposed backup solution must support software based de-duplication and shall be capable of taking backup of data and workloads (irrespective of the underlying storage OEM) and the solution shall support deduplicated backup copies for long-term retention. Based on policy backup software should be able to move deduplicated backup copy to a Long term storage automatically. The proposed backup solution shall support deduplicated backup targets across leading OEM storage systems and shall not be restricted on any specific OEM/vendor.	Proposed backup solution must support source side as well as target de-duplication and shall be capable of taking backup of data and workloads (irrespective of the underlying storage OEM) on the proposed solution shall support deduplicated backup copies for long-term retention. Based on policy backup software should be able to move deduplicated backup copy to a Long term storage automatically. The proposed backup solution shall support deduplicated backup targets across leading OEM storage systems and shall not be restricted on any specific OEM/vendor.	Please be guided by the RFP
833	18	Backup Solution		Proposed Disk Based Appliance/backup storage should have the capability to tier backup data to an external cloud storage (on premise / public cloud) and the required licenses must be provided on day 1. Proposed backup solution with storage/appliance should have redundant components (Backup Storage - controllers, Power , fans etc. and Backup Appliance - Power , fans etc.) , HA mechanism in place to avoid Single Point of Failure and should have minimum of 4x16/32 GB FC ports & 2x32G ports on each controller for Host connectivity. Proposed Backup Solution should have minimum 4x scalability of the current quoted capacity for future growth.	Proposed Disk Based Appliance/backup storage should have the capability to tier backup data to an external cloud storage (on premise / public cloud) and the required licenses must be provided on day 1. Proposed backup solution with storage/appliance should have redundant components (Backup Storage - controllers, Power , fans etc. and Backup Appliance - Power , fans etc.) , HA mechanism in place/solution to avoid Single Point of Failure and should have minimum of 4x10/25 GbE network ports & 4 x 32G FC ports on each controller for Host connectivity. Proposed Backup Solution should have minimum 4x scalability of the current quoted capacity scalable design for future growth.	Please be guided by the RFP
834	20	Backup Solution		The proposed appliance/backup storage must ensure that all scheduled backups complete within an 8-hour backup window, with data protected via RAID 6 (or equivalent - providing 2 disk failure protection). Backup solution must support required technology and storage capacity to manage and compensate duplication across multiple pools, ensuring consistent performance and efficiency. Overheads in terms of memory, capacity, technology and IOPS to handle the bottleneck due to multiple deduplication pools should be factored and required documentation from the OEM is to be submitted along with the proposal.	The proposed appliance/backup storage must support a minimum of 25 TB/hr so as to ensure that all scheduled backups complete within an 8-hour backup window, with data protected via RAID 6 (or equivalent - providing 2 disk failure protection). Backup solution must support required technology and storage capacity to manage and compensate duplication across multiple pools, ensuring consistent performance and efficiency. Overheads in terms of memory, capacity, technology and IOPS to handle the bottleneck due to multiple deduplication pools should be factored and Bidder must provide a sizing certificate showcasing this sizing consideration on the OEM's letter head required documentation from the OEM is to be submitted along with the proposal.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
835	38	Backup Solution		The proposed backup solution must natively support a LAN-Free architecture for all image-level VM backups to prevent performance degradation on production networks. All raw backup data payloads must stream directly from production storage to the backup appliance/storage over a dedicated Storage Area Network (SAN/Fibre Channel/iSCSI) or dedicated storage fabric. Production Ethernet/LAN infrastructure must be completely bypassed, restricting its use strictly to minor control traffic and metadata orchestration.	The proposed backup solution must natively support a LAN efficient/LAN free architecture for all image-level VM backups to prevent performance degradation on production networks. All raw backup data payloads must stream directly from production storage to the backup appliance/storage over dedicated Backup LAN / Storage Area Network (SAN/Fibre Channel/iSCSI) or dedicated storage fabric. Production Ethernet/LAN infrastructure must be completely bypassed/minimal disruption, restricting it's use strictly to minor control traffic and metadata orchestration.	Please refer Addendum 1 for the revised clause
836	100	10.2	4	The bidder should have a minimum average annual turnover of INR 1000 crore in India during the last 3 financial years (i.e. 2022-23, 2023-24 & 2024–25) along with positive net worth.	The RFP stipulates a minimum average annual turnover of INR 1,000 Crores, which may significantly restrict participation to a limited number of bidders. To encourage wider participation and promote healthy competition while ensuring adequate financial strength and execution capability, we request the Bank to kindly consider reducing the minimum average annual turnover requirement from INR 1,000 Crores to INR 350 Crores, while retaining the requirement of positive net worth. This would enable participation from established and financially sound bidders with relevant technical capabilities and experience, thereby providing the Bank with a wider pool of qualified bidders and competitive offerings.	Please refer Addendum 1 for the revised clause.
837	Appendix 1A	DRM Functional Specification	F90	The system should be able to interface with MS Teams.	Kindly clarify, interface, ideally any unprotected data which is being shared via any of these tools should be automatically protected based on pre defined policies. Instead of interface, we suggest bank should ask for integration, interface has no practical relevance. Additionally, since 200 licenses are requested for the DRM solution, if required—will apply only to these 200 users.	Please be guided by the RFP All features and capabilities sought in the RFP shall be for the number of defined users sought.
838	Appendix 1A	DRM Functional Specification	F91	The system should be able to interface with SharePoint.	Kindly clarify, interface, ideally any unprotected data which is being shared via any of these tools should be automatically protected based on pre defined policies. Instead of interface, we suggest bank should ask for integration, interface has no practical relevance. Additionally, since 200 licenses are requested for the DRM solution, if required—will apply only to these 200 users.	Please be guided by the RFP All features and capabilities sought in the RFP shall be for the number of defined users sought.
839	Appendix 1A	DRM Functional Specification	F92	The system should be able to interface with OneDrive.	Kindly clarify, interface, ideally any unprotected data which is being shared via any of these tools should be automatically protected based on pre defined policies. Instead of interface, we suggest bank should ask for integration, interface has no practical relevance. Additionally, since 200 licenses are requested for the DRM solution, if required—will apply only to these 200 users.	Please be guided by the RFP All features and capabilities sought in the RFP shall be for the number of defined users sought.
840	RFP No. PSB/HOIT/RFP/53/2026-27 Bid Number:GEM/2026/B/7936763 Appendix 1A Functional Specification	DNS Protection	General. Point No:2	The DDI solution should be a hardware appliance for DNS & DHCP and virtual appliance for IPAM and reporting, all from a single vendor.	The best way is to use virtual platform to deploy these solutions in the environment. It gives more control & scalibilty to the solution so request you to update the point as: The DDI solution should be a virtual appliance for DNS & DHCP and virtual appliance for IPAM and reporting, all from a single vendor. The OS must be the hardent OS.	Please be guided by the RFP
841	RFP No. PSB/HOIT/RFP/53/2026-27 Bid Number:GEM/2026/B/7936763 Appendix 1A Functional Specification	DNS Protection	General		As Document talks about Hardware based DDI solution but there is no guideline for the security of Hardware. so to make sure the hardware is complient on a security standards please include the point mentioned below: "The DDI solution should be certified to Common Criteria 2, EAL2 or IC3S." This will help to get a proper hardware based solution.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
842	RFP No. PSB/HOIT/RFP/53/2026-27 Bid Number:GEM/2026/B/7936763 Appendix 1A Functional Specification	DNS Protection	Architectural Requirements Point No:65	The threat intelligence must be consumed from on-premises for Authoritative, Recursive and Caching DNS	As the Recursive DNS response comes from the public internet and queries has to go out to internet its better to use hybrid deployment where Authoritative Remains on-premises & Caching happens on- premises but Recursive DNS security happens on cloud (SAAS). Please update the point as: The threat intelligence must be consumed In a hybrid mode on-premises for Authoritative, on cloud for Recursive and Caching should happend on-premises.	Please be guided by the RFP
843	RFP No. PSB/HOIT/RFP/53/2026-27 Bid Number:GEM/2026/B/7936763 Appendix 1A Functional Specification	DNS Protection	Security RequirementsPoint No: 73	73The solution must be able to prevent infections, blocking the DNS requests towards malware distribution domains or drive-by domains, and contain the pre-existing infections, blocking the DNS requests towards command and control infrastructures. The solution should support following Feeds : 73.1Base Hostnames 73.2Anti-malware 73.3Ransomware 73.4Bogon 73.5Malware Ips/Domains 73.6Bot IPs/Domains 73.7Exploit Kit IPs/Domains 73.8Malware DGA hostnames 73.9TOR Exit Node IPs/Domains 74.10 Extended Base & anti-malware Hostnames 74.11 Extended malware IPs /Domains 74.12Extended TOR Exit Node IPs /Domains 74.13Extended Ransomware IPs /Domains 74.14Extended Exploit Kits IPs/Domains 74.15SpamBot IPs/Domains 74.16Spambot IPs DNSB/Domains	As we are talking about DNS protection and there are multiple feeds are mentioned but Extended feeds get covered in the base feed it self and few feeds are very old and been replaced by new feeds so i have updated the feed request you to update the same. Please update the point as: 73 The solution must be able to prevent infections, blocking the DNS requests towards malware distribution domains or drive-by domains, and contain the pre-existing infections, blocking the DNS requests towards command and control infrastructures. The solution should support following Feeds : 73.1 Base Hostnames 73.2 Anti-malware 73.3 Ransomware 73.4 Bogon 73.5 Malware Ips/Domains 73.6 sinkholes. 73.7 Exploit Kit IPs/Domains 73.8 Malware DGA hostnames 73.9 TOR Exit Node IPs/Domains 74.10 malicious Name Servers 74.11 C&C malware 74.12 Newly Observed Emergent Domains 74.13 Cryptocurrency 74.14 DOH Public Hostnames 74.15 DOH Public IPs (Public_DOH_IP) 74.16 EECN IP (EECN_IP)	Please be guided by the RFP
844	RFP No. PSB/HOIT/RFP/53/2026-27 Bid Number:GEM/2026/B/7936763 Appendix 1A Functional Specification	DNS Protection	Management Requirements Point No:93	The vendor must have support center in India	Make in India gives more control and localization capability so please request you to modify the point. Please update the point as: The vendor must have Development Center and support center in India	Please be guided by the RFP
845	RFP No. PSB/HOIT/RFP/53/2026-27 Bid Number:GEM/2026/B/7936763 Appendix 1A Functional Specification	DNS Protection	Management Requirements	The solution must support two factor authentication	As a best practies all the solution must use two factor authentication so please include this point	Please be guided by the RFP
846	27	7 SCOPE OF WORK	7 SCOPE OF WORK	“The Bank is undertaking a comprehensive enhancement of its cybersecurity and information security infrastructure… across its Data Centre (Mumbai), NDC, Disaster Recovery Centre (Noida), NDR Cloud environments, and branch/office network.”	Kindly provide a location-wise solution deployment matrix covering Mumbai DC, Noida DR, NDC, NDR Cloud, branch/office network, and any other in-scope sites for accurate scope and effort estimation.	Please be guided by the RFP
847	27	7 SCOPE OF WORK	7 SCOPE OF WORK	“The Bank intends to procure, implement, integrate, operate, and maintain advanced IT/information Security & cybersecurity technologies…”	Kindly clarify whether the bidder’s scope includes only the listed security solutions or also complete end-to-end operations of the integrated overall security ecosystem formed using these solutions.	The Bidder shall be responsible for implementation, integration, operation and maintenance of the solutions specifically identified as in scope under this RFP, including their approved integrations and dependencies.

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
848	27	7 SCOPE OF WORK	7 SCOPE OF WORK	"The proposed solution shall enable the Bank to establish comprehensive, multilayered defense architecture…"	Kindly clarify whether the bidder is expected to establish and operationalize a unified multilayer defense architecture across all 21 tools as part of this RFP, including correlation, workflows, and governance integration.	The Bidder, along with respective OEMs, shall establish an integrated security architecture for the in-scope solutions, including required interoperability, event sharing, correlation and workflows as specified in the RFP.
849	27	7 SCOPE OF WORK	7 SCOPE OF WORK	"Achieve end-to-end visibility and control over security events"	Kindly clarify whether this objective is expected to be delivered through existing Bank platforms, through solution-native consoles, or through bidder-led integration of all proposed tools into a centralized view.	The proposed solutions shall provide the visibility and control capabilities specified in the RFP through solution-native consoles and/or integration with designated Bank security monitoring platforms,
850	27	7 SCOPE OF WORK	7 SCOPE OF WORK	"Support the Bank's digital & Cyber transformation initiatives without compromising on security or performance."	Kindly provide details of the current and planned transformation initiatives that may run in parallel and impact dependencies, implementation sequencing, and effort estimation.	The Bank shall provide relevant information concerning known dependencies and initiatives to the extent available and permissible. The Bidder shall undertake necessary discovery and dependency assessment.
851	27	7 SCOPE OF WORK	7 SCOPE OF WORK	"Solutions proposed under this RFP must integrate seamlessly into the Bank's existing ecosystem…"	Kindly share the current ecosystem inventory, including existing security tools, enterprise tools, infra platforms, and ongoing projects, to support integration effort estimation.	Please refer Annexure 21: Sizing/Volumetrics, Data Retention and Current Infrastructure for the existing and envisaged tools/solutions
852	28	7.1 IT Security Solution & Services	7.1 IT Security Solution & Services	"The bidder will be responsible for delivering and implementing these solutions at the locations as defined…"	Kindly share solution-wise location mapping and volumetric applicability for each proposed technology to enable realistic delivery planning.	Please be guided by the RFP
853	32	7.1 IT Security Solution & Services	7.1 IT Security Solution & Services	"The implementation of each solution, including design, installation, configuration, integration, migration, testing, and Go-Live, shall be performed by OEM."	Kindly clarify the exact implementation responsibility demarcation between bidder and OEM for each stage, including whether bidder is expected to provide working-level technical support resources alongside OEM teams.	The respective OEM shall perform OEM-specific design, deployment, configuration, integration, migration, testing and commissioning as stipulated in the RFP. The Bidder shall remain responsible for overall project management, coordination, dependency management, integration governance, documentation consolidation, SLA management and contractual delivery.
854	32	7.1 IT Security Solution & Services	7.1 IT Security Solution & Services	"The bidder shall arrange OEM resources, coordinate implementation activities, and ensure timely project completion."	Kindly clarify whether the bidder's responsibility is limited to coordination and governance for OEM-led tasks, or whether bidder remains execution-support owner for all workstreams.	The Bidder's responsibility is not limited to administrative coordination. The Bidder shall provide necessary project and technical coordination/execution support to ensure successful delivery, while OEMs shall remain responsible for OEM-specific technical activities assigned to them.
855	32	7.1 IT Security Solution & Services	7.1 IT Security Solution & Services	"Upon successful implementation, the respective OEM shall provide a certificate confirming that the solution has been deployed by OEM…"	Kindly clarify whether such OEM certification is expected solution-wise, environment-wise, or milestone-wise, and whether it is a prerequisite for payment/sign-off.	OEM certification shall be obtained solution-wise. payment and final acceptance shall remain subject to fulfilment of all applicable contractual acceptance criteria a
856	32	7.1 IT Security Solution & Services	7.1 IT Security Solution & Services	"System Integrator (Bidder): Supply the proposed solutions, provide onsite L1/L2/L3 support resources, manage the project, and coordinate with OEMs."	Kindly clarify whether bidder L3 resources are expected to be dedicated product specialists across all solutions or service-management leads supported by OEM technical SMEs.	The Bidder shall provide appropriately qualified L1/L2/L3 resources commensurate with the in-scope solutions. OEM technical SMEs may be engaged for product-specific/escalated issues. Such OEM engagement shall not relieve the Bidder of its contractual SLA and service-delivery responsibilities.
857	32	7.1 IT Security Solution & Services	7.1 IT Security Solution & Services	"Solution OEM: Deploy, configure, integrate, test, commission, and migrate data/logs from existing solutions…"	Kindly confirm whether all configuration and integration activities are to be executed by OEM only, with bidder involvement limited to planning, monitoring, and governance.	OEM shall undertake OEM-specific configuration and integration activities as specified in the RFP. The Bidder shall provide required coordination, technical support, dependency management, and integration governance to ensure end-to-end implementation.
858	32	7.1 IT Security Solution & Services	7.1 IT Security Solution & Services	"Security tools, agents, collectors, and connectors shall also be deployed in the Bank's cloud/VPC environment, wherever applicable…"	Kindly share the count and type of cloud/VPC environments, along with in-scope workloads and applications, for effort estimation.	Please be guided by the RFP. Refer Section 15.21.4Deployment & Data Retention
859	32	7.1 IT Security Solution & Services	7.1 IT Security Solution & Services	"The bidder shall be responsible for implementation, integration, migration, upgrades, patching, troubleshooting, health checks, backups, audit support, documentation, SOP creation, and lifecycle management…"	Kindly clarify whether all these activities are to be delivered directly by bidder onsite personnel or may be fulfilled through a mix of bidder onsite team, bidder offsite SMEs, and OEM support.	Please be guided by the RFP
860	32	7.1 IT Security Solution & Services	7.1 IT Security Solution & Services	"In case of implementation delays, the bidder shall ensure seamless takeover and transition of in-scope existing security solutions…"	Kindly clarify whether this obligation applies solution-wise for delayed components only or for the complete incumbent estate.	The takeover/transition obligation shall apply to the affected in-scope solution(s) for which implementation has been delayed, to the extent necessary to maintain continuity of Bank operations.
861	32	7.1 IT Security Solution & Services	7.1 IT Security Solution & Services	"...without disruption to Bank operations at no additional cost to the bank."	Kindly clarify whether this includes only manpower-based support or also third-party/OEM renewal costs for incumbent tools during such interim takeover period.	The Bidder shall ensure continuity of services within its contractual responsibilities without additional cost to the Bank.
862	32	7.1 IT Security Solution & Services	7.1 IT Security Solution & Services	"All proposed solutions shall support real-time integration, event correlation, orchestration, and automated response capabilities…"	Kindly clarify whether bidder is expected to implement and maintain custom cross-platform orchestration among all tools wherever native integration is unavailable.	Required orchestration and integrations for approved in-scope use cases shall be implemented using standard/native capabilities. Custom integration/orchestration required for in-scope requirements shall be provided as specified in the RFP.
863	32	7.1 IT Security Solution & Services	7.1 IT Security Solution & Services	"The proposed solutions shall provide dynamic, customizable dashboards and reports…"	Kindly clarify whether dashboard/report customization is expected in each native product console, through a centralized platform, or both.	Dashboards and reports shall be configured in the respective solution consoles and/or designated centralized monitoring/reporting platforms
864	33	7.1 IT Security Solution & Services	7.1 IT Security Solution & Services	"All supporting and underlying software components… shall be enterprise licensed version & OEM-supported…"	Kindly confirm whether all supporting software required for non-production, test, UAT, pre-prod, and DR environments is also to be included in bidder scope and commercial sizing.	The Bidder shall include all licences/subscriptions and supporting software components expressly required for the environments identified as in scope in the RFP
865	33	7.1 IT Security Solution & Services	Cyber Security Incident / Data Breach (a)	"The Bidder shall immediately… not later than six (6) hours from becoming aware of any actual, suspected or reasonably suspected cyber security incident…"	Kindly clarify whether this reporting requirement applies only to incidents attributable to bidder/OEM managed in-scope solutions, or also to adjacent Bank systems where the solution only provides visibility/telemetry.	The SLA items in the RFP is applicable for Bidder proposed solutions and services
866	33	7.1 IT Security Solution & Services	Cyber Security Incident / Data Breach (b)	"The Bidder shall immediately take all necessary steps for containment, mitigation, investigation, eradication and recovery…"	Kindly clarify the extent of bidder responsibility for containment and recovery where the underlying affected system/application is owned and operated by a separate Bank/internal/third-party team.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
867	33	7.1 IT Security Solution & Services	Cyber Security Incident / Data Breach (c)	"The Bidder shall preserve all logs, records, forensic evidence, system images…"	Kindly clarify whether the bidder is expected to maintain forensic evidence handling capability for all proposed solutions as part of standard FM scope.	Please be guided by the RFP
868	33	7.1 IT Security Solution & Services	Cyber Security Incident / Data Breach (e)	"The Bidder shall provide a preliminary incident report immediately and a detailed Root Cause Analysis…"	Kindly clarify whether OEM-certified RCA is expected for all critical incidents and whether any standard RCA format will be prescribed by the Bank.	Please be guided by the RFP
869	33	7.1 IT Security Solution & Services	Cyber Security Incident / Data Breach (f)	"All reasonable costs incurred by the Bank… attributable to the Bidder/OEM/subcontractor shall be recoverable from the Bidder"	Kindly clarify the attribution and approval mechanism for determining whether an incident is attributable to bidder/OEM scope.	Please be guided by the RFP
870	33	7.2 RACI (Responsible, Accountable, Consulted, Informed)	Activity 1	"Requirement Analysis – Bidder A,R / OEM R / Bank R,A,C,I"	Kindly clarify the intended role split, as the Bank is also marked R,A,C,I. Please confirm the practical ownership model for requirement analysis.	The RACI represents participation and governance responsibilities and shall not be interpreted as transfer of delivery accountability to the Bank. The Bidder & OEM shall lead requirement analysis and documentation, while the Bank shall provide business/technical inputs, clarifications, approvals and decisions within its responsibility.
871	33	7.2 RACI (Responsible, Accountable, Consulted, Informed)	Activity 2	"Solution & System Design – Bidder A,R / OEM R / Bank C,I"	Kindly clarify whether bidder is expected to create the integrated overall design while OEMs create solution-level design artifacts.	OEMs shall prepare solution-specific technical designs. The Bidder shall consolidate and govern the overall integrated architecture
872	33	7.2 RACI (Responsible, Accountable, Consulted, Informed)	Activity 3	"Installation, Integration & Implementation – Bidder A,R / OEM R / Bank C,I"	Kindly confirm whether all implementation execution remains OEM-led and bidder accountability is governance-based, or whether bidder is expected to contribute execution resources as well.	Implementation shall be OEM-led for OEM-specific activities; however, the Bidder shall provide sufficient resources for project management, integration coordination, dependency management
873	34	7.2 RACI (Responsible, Accountable, Consulted, Informed)	Activity 8	"Facility Management & Resource Management – Bidder A,R / OEM C / Bank I"	Kindly clarify whether OEM involvement during FM is advisory/on-demand or mandatory active participation for all technologies.	OEM participation shall be on an as-required basis for product-specific technical support, complex incidents, upgrades, reviews and escalations.
874	34	7.2 RACI (Responsible, Accountable, Consulted, Informed)	Activity 9	"IT Security Operations – Bidder A,R / OEM C / Bank I"	Kindly clarify whether bidder is expected to operate only newly proposed solutions or also incumbent/integrated surrounding components forming the operational security estate.	T Security Operations under this RFP shall cover the proposed/in-scope solutions and their approved integrations. The Bidder shall coordinate with the Bank and relevant third parties for dependencies
875	34	7.2 RACI (Responsible, Accountable, Consulted, Informed)	Activity 10	"Business Continuity & DR Support – Bidder A,R / OEM C / Bank I"	Kindly clarify whether DR support is expected solution-wise for each tool or as an integrated program-level responsibility.	The Bidder shall provide DR support for each in-scope solution and shall coordinate solution dependencies as part of the integrated implementation/operations framework.
876	34	7.2 RACI (Responsible, Accountable, Consulted, Informed)	Activity 14	"Incident, Problem & Service Management – Bidder A,R / OEM R / Bank A,C,I"	Kindly clarify operational ownership for incident closure where the root cause lies in OEM product behavior or Bank-managed integrated systems.	The Bidder shall own incident coordination and ensure timely escalation/resolution of incidents relating to the in-scope solutions. Where root cause is attributable to an OEM product defect, the Bidder shall pursue OEM resolution and provide appropriate workarounds/compensating controls
877	34	7.2 RACI (Responsible, Accountable, Consulted, Informed)	Activity 16	"Product Upgrades, Patches & Hotfixes – Bidder A,R / OEM R / Bank I"	Kindly clarify whether all product upgrades and patch execution are to be performed by OEM or by bidder operations team with OEM guidance after go-live.	Routine patching and upgrades may be performed by the Bidder's qualified O&M resources in accordance with OEM recommendations and Bank-approved procedures. OEM shall be engaged where product expertise, certification, complex upgrade activity or escalation is required.
878	50	7.4 Bidder Responsibilities	7.4(1)	"Project planning, rollback planning, project governance, and submission of detailed implementation methodology and timelines."	Kindly clarify whether solution-wise project plans under a consolidated master plan will be acceptable.	The Bidder shall submit a consolidated master implementation plan supported by solution-wise detailed plans, milestones, dependencies, resource plans, risks, testing, migration, rollback and Go-Live activities
879	50	7.4 Bidder Responsibilities	7.4(2)	"The Bidder should note that the Bank is in the process of modernizing and migrating its IT Security ecosystem…"	Kindly provide details of planned/ongoing modernization programs that may affect scope, integration, and sequencing assumptions.	Relevant known dependencies shall be shared by the Bank to the extent available.
880	50	7.4 Bidder Responsibilities	7.4(3)	"The Bidder shall ensure that the proposed solution is designed and implemented in a manner that is fully compatible with the Bank's current environment as well as its target security architecture."	Kindly request the Bank to share the current and target security architecture documents for effort estimation.	Details shall be shared with the Successful bidder.
881	50	7.4 Bidder Responsibilities	7.4(4)	"The Bidder shall be responsible for factoring all required integration, interfacing, API connectivity, log forwarding, and interoperability requirements…"	Kindly confirm whether integrations with future tools procured after project initiation are also included under this obligation.	The integration obligation shall apply to systems/ tools identified as in scope and documented in the approved SRS
882	50	7.4 Bidder Responsibilities	7.4(5)	"Capacity planning, hardware/software sizing, and bill of materials validation."	Kindly clarify whether bidder is expected to perform final sizing independently or whether OEM-certified sizing reports will be acceptable as supporting basis.	OEM sizing reports will be used as supporting technical evidence

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
883	50	7.4 Bidder Responsibilities	7.4(6)	"Security baseline configuration as per industry best practices and security configuration document of the bank."	Kindly share whether the Bank's security configuration baseline document can be provided during bid/pre-bid stage for accurate estimation.	Relevant Bank security baseline requirements shall be shared to the extent feasible and permissible to the successful bidder. The Bidder shall also comply with applicable Bank security policies, standards, regulatory requirements and OEM hardening guidelines.
884	50	7.4 Bidder Responsibilities	7.4(7)	"Knowledge transfer sessions and administrator training for Bank IT/Security teams."	Kindly clarify expected number/frequency of bidder-led KT sessions in addition to OEM formal training.	The Bidder shall provide adequate KT sessions required for operational takeover and effective O&M.The detailed KT plan, audience, topics and number of sessions shall be finalized during implementation and documented in the approved training/KT plan.
885	50	7.4 Bidder Responsibilities	7.4(8)	"Coordination with OEMs, third-party vendors, ISPs, and internal stakeholders during implementation and troubleshooting"	Kindly clarify whether the Bank will nominate SPOCs from each stakeholder group and whether dependency-driven delays caused by external parties will be excluded from bidder delay attribution.	The Bank shall nominate appropriate SPOCs for coordination. Dependencies on third parties/Bank stakeholders shall be documented through the project governance mechanism. However, the Bidder shall remain responsible for proactive follow-up, escalation, dependency tracking and mitigation
886	50	7.4 Bidder Responsibilities	7.4(9)	"Provide post Go-Live support, stabilization support, and issue resolution during warranty/ATS period"	Kindly confirm the expected stabilization period per solution after go-live.	Please be guided by the RFP
887	50	7.4 Bidder Responsibilities	7.4(10)	"Configure monitoring, alerting, dashboards, reporting, and automated notification mechanisms."	Kindly clarify whether these are required in each product console only or also in a centralized framework spanning all solutions.	Both shall be implemented where required by the approved solution architecture and use cases. Native monitoring shall be configured for solution health and operation, while centralized monitoring/SOC integration shall be provided for designated security events and use cases
888	51	7.5 OEM Responsibilities	7.5(1)	"all the requirements pertaining to Requirement analysis, System design, Development & Installation, Documentation, Deployment and Go-live are to be performed by the respective solution OEM."	Kindly clarify whether bidder is expected to deploy domain consultants/business analysts/architects even for OEM-owned tasks, or whether OEM staffing alone is sufficient.	The Bidder shall deploy appropriately qualified project, architecture, integration and domain resources necessary to fulfil its contractual responsibilities
889	51	7.5 OEM Responsibilities	7.5(2)	"Respective solution OEM along with the bidder should design High-Level Enterprise Security Architecture…"	Kindly clarify whether one enterprise architecture document is expected across all OEMs, and who among bidder/OEMs is expected to own final integration architecture.	Bidder to right size the resources, bank has provided minimal requirement in the RFP
890	51	7.5 OEM Responsibilities	7.5(3)	"Assessment of existing system, deployment, configurations, policies and Preparation and submission of High-Level Design (HLD) and Low-Level Design (LLD) documents."	Kindly confirm whether these deliverables are required separately for each solution plus a consolidated integration design.	The OEMs shall provide solution-wise HLD/LLD documents and bidder shall provide consolidated integration architecture/design covering interfaces, dependencies, data/event flows and security workflows
891	51	7.5 OEM Responsibilities	7.5(4)	"Preparation of as-built documentation, configuration documents, SOPs, and operational manuals"	Kindly clarify final documentation ownership—OEM-authored and bidder-consolidated, or bidder-owned final submission.	OEM shall author product-specific technical documentation; however, the Bidder shall be responsible for consolidating, validating and submitting the final as-built documentation, configuration records, SOPs and operational manuals for Bank acceptance.
892	51	7.5 OEM Responsibilities	7.5(5)	"Integration of the proposed solution with Bank IT & Cyber Security systems like SIEM, two-factor authentication, wireless APs, reporting tools, etc."	Kindly request the complete list of systems requiring integration, with current OEM/version and scope of interface required.	The Bank shall provide available information regarding designated integration endpoints to successful bidder. Final interface inventory shall be validated during discovery/design and captured in the approved integration design.
893	51	7.5 OEM Responsibilities	7.5(6)	"Configuration/integration for log correlation with standard SIEM tools, SOC Big Data Logs, syslog servers etc."	Kindly clarify whether the Bank already has log onboarding standards, parser specifications, and field normalization standards to be followed by bidder/OEMs.	The Bidder/OEM shall comply with the Bank's approved SIEM/log onboarding standards and shall provide required parsers, mappings and normalization for approved in-scope integrations
894	51	7.5 OEM Responsibilities	7.5(7)	"Integration with enterprise authentication systems, including Microsoft Active Directory (AD), RADIUS, and TACACS+ etc."	Kindly provide the number and type of existing enterprise identity sources and environments to be integrated.	Please be guided by the RFP, further details shall be shared with successful bidder
895	51	7.5 OEM Responsibilities	7.5(9)	"Enable/Configure application-based policies, user controls, bandwidth rules, and ensure proper deployment of IPS/IDS capabilities."	Kindly clarify whether this requirement is generic for all relevant perimeter/network solutions and whether policy design is fully in bidder/OEM scope.	The Bidder/OEM shall configure and implement IPS/IDS capabilities and policies based on Bank-approved security requirements and operating procedures.
896	51	7.5 OEM Responsibilities	7.5(10)	"Ensure compatibility and integration of the proposed solution with the existing IT infrastructure including wired and wireless components."	Kindly request high-level current network and security topology diagrams for accurate effort estimation.	Relevant topology information shall be provided to the extent available and permissible to the successful bidder. The Bidder shall validate current-state topology during assessment/discovery
897	51	7.5 OEM Responsibilities	7.5(11)	"Configuration of the proposed to ensure SSL decryption rule configuration and policy enforcement for encrypted traffic inspection."	Kindly clarify whether SSL inspection policy definition, exception design, and privacy/legal use case alignment will be jointly finalized with Bank stakeholders.	SSL inspection/decryption policies, exceptions and applicable privacy/legal/business requirements shall be finalized during the SRS stage. The Bidder/OEM shall implement the approved policies and controls.
898	52	7.5 OEM Responsibilities	7.5(12)	"Perform feasibility study and conduct actual migration of the existing firewalls architecture, configuration, rules, application profile, signatures, policies etc."	Kindly clarify the scope and rationale of firewall migration under this RFP and identify the related incumbent and target workstream.	The Requirement stands deleted
899	52	7.5 OEM Responsibilities	7.5(13)	"Develop and Configure Out of the box or custom interfaces to integrate with multiple security monitoring and reporting tools…"	Kindly clarify whether custom interfaces for future systems added during contract period are also included in scope without commercial impact.	Custom interfaces required for approved in-scope systems/use cases is to be provided by the bidder. Exact list of interfaces shall be finalised during SRS stage
900	52	7.5 OEM Responsibilities	7.5(14)	"Migration planning, testing, phased rollout, and cutover execution with minimal downtime."	Kindly confirm whether phased rollout by solution/domain is acceptable within the overall implementation timeline.	Implmentation shall be phased and based on the approved implementation plan within the defined timelines. The Bank will identify priority systems during SRS stage hwoever, the implementation has to be completed within the timelines defined
901	52	7.5 OEM Responsibilities	7.5(15)	"Performance tuning, health checks, and system stabilization post deployment."	Kindly clarify expected duration and closure criteria for post-deployment stabilization.	Please be guided by the RFP
902	52	7.5 OEM Responsibilities	7.5(16)	"Performing System Integration Testing (SIT), and support during audit/compliance validation"	Kindly clarify whether SIT will be solution-wise or integrated program-wide across multiple interdependent tools.	SIT shall be conducted at solution level and, wherever dependencies/interoperability require, through integrated end-to-end testing across relevant solutions. The scope and test cases shall be documented in the approved SIT plan.
903	52	7.5 OEM Responsibilities	7.5(17)	"Remediation of identified VAPT & Audit gaps related to the Configured solution."	Kindly clarify whether remediation timelines will be based on clause 12 severity timelines and whether product limitations/OEM roadmap items are excluded.	Configuration and implementation-related gaps attributable to the Bidder/OEM shall be remediated within the timelines specified in the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
904	52	7.5 OEM Responsibilities	7.5(19)	"Submission of final acceptance & go-live report and successful handover of the solution to the Bidder's operations team"	Kindly confirm whether formal handover from OEM implementation to bidder O&M team is expected for each solution and whether a standard handover checklist/template will be shared by the Bank.	Formal handover shall be completed solution-wise using a detailed handover checklist covering configuration, credentials/access procedures where applicable, documentation, known issues, monitoring, backup/restore, support/escalation matrix and operational readiness.
905	52	7.5 OEM Responsibilities	7.5(20)	"respective solution OEM is to be involved every year during the O&M phase for performing the configuration, rules and parametrization review along with the solution architecture review…"	Kindly clarify whether such annual OEM reviews are required for all 21 solutions and whether onsite presence is mandatory.	Please refer Section 7.12.4OEM Services & Deployment (Architecture Assessment)
906	52	7.5 OEM Responsibilities	7.5(21)	"Any requirements from the Bank for customization, enhancement… parsers, connectors… dashboards, reporting… shall be undertaken by the Bidder at no cost to the Bank during the Contract period…"	Kindly clarify whether this obligation is limited to in-scope systems/use cases identified during implementation, or extends to all future onboarding and enhancements requested during the contract period.	The Bidder shall provide customization, enhancement, parsers, connectors, dashboards and reports required for the approved in-scope solutions and use cases as specified in the RFP
907	52	7.5.1 Migration - Activities are to be performed by Respective solution OEM (supported by bidder)	7.5.1	"coordinate with the Bank and incumbent vendors to ensure seamless migration from the existing solutions to the proposed platform…"	Kindly request the Bank to share incumbent vendor details, current contracts, support model, and transition dependencies solution-wise.	Details shall be shared with the Successful bidder.
908	52	7.5.1 Migration - Activities are to be performed by Respective solution OEM (supported by bidder)	7.5.1	"The bidder shall take over all relevant artifacts, documentation, configurations, customizations, software components, manuals, certificates, reports, patches, releases…"	Kindly clarify whether the Bank will ensure mandatory handover by incumbent vendors for all listed artifacts.	The Bank shall facilitate handover of available incumbent artifacts within its possession/control and shall coordinate with incumbent vendors as reasonably required.
909	52	7.5.1 Migration - Activities are to be performed by Respective solution OEM (supported by bidder)	7.5.1	"The OEM… shall be responsible for migration of all applicable data, configurations, policies, rules, telemetry, logs, parsers, metadata, integrations, and customizations…"	Kindly clarify whether "all applicable" will be jointly finalized solution-wise during discovery based on feasibility and relevance, rather than presumed as full one-to-one migration in all cases.	Migration scope shall be finalized solution-wise during discovery/migration planning
910	53	7.5.1 Migration - Activities are to be performed by Respective solution OEM (supported by bidder)	7.5.1	"The migration approach shall be applicable across all proposed IT and Cyber Security solutions wherever relevant."	Kindly request the Bank to specify which listed solutions are expected to involve incumbent-to-target migration versus greenfield deployment.	Please refer 15.21.2 - Existing IT Security Solution Details for the list of solutions available with the bank
911	53	7.5.1 Migration - Activities are to be performed by Respective solution OEM (supported by bidder)	7.5.1	"The OEM shall perform all necessary mapping, transformation, parser development/customization, rule migration, configuration alignment, validation, reconciliation, and testing…"	Kindly clarify whether rule/parser migration complexity assumptions and count baselines can be shared from the incumbent estate.	Details, as available, shall be shared with the successful bidder
912	53	7.5.1 Migration - Activities are to be performed by Respective solution OEM (supported by bidder)	7.5.1	"The Respective OEM along with the bidder has to take handover of Data Dictionary, Patches & Releases… Technical Documents, user manual, functional manual, certifications…"	Kindly confirm whether all such incumbent artifacts exist and will be made available by the Bank/incumbent vendors.	Details, as available, shall be shared with the successful bidder
913	53	7.5.1 Migration - Activities are to be performed by Respective solution OEM (supported by bidder)	7.5.1	"Bank currently has an IT Security setup in its co-hosted premises at DC & DR."	Kindly provide the incumbent setup architecture and ownership split between Bank, hosting partner, incumbent SI, and OEMs for accurate transition assessment.	Details, as available, shall be shared with the successful bidder

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
914	53	7.5.1 Migration - Activities are to be performed by Respective solution OEM (supported by bidder)	Detailed Migration Plan	“Current State Assessment”	Kindly clarify whether the Bank will provide a current state assessment baseline to all bidders, or whether this must be fully derived post-award.	Details, as available, shall be shared with the successful bidder
915	53	7.5.1 Migration - Activities are to be performed by Respective solution OEM (supported by bidder)	Detailed Migration Plan	“Dependency and Integration Mapping”	Kindly request dependency maps between incumbent tools and Bank systems, if available, for migration effort planning.	Details, as available, shall be shared with the successful bidder
916	53	7.5.1 Migration - Activities are to be performed by Respective solution OEM (supported by bidder)	Detailed Migration Plan	“Rule, Policy and Parser Migration”	Kindly provide indicative volumes of rule sets, policy objects, parser customizations, and correlation logic in the incumbent environment.	The Bidder shall be responsible for procurement, implementation, integration, operation and maintenance of the solutions specifically identified as in-scope under this RFP, including their approved integrations and dependencies
917	53	7.5.1 Migration - Activities are to be performed by Respective solution OEM (supported by bidder)	Detailed Migration Plan	“Parallel Run and Cutover Strategy”	Kindly clarify whether parallel run is mandatory for all solutions or only for critical solutions identified by the Bank.	The Bidder, along with respective OEMs, shall establish an integrated architecture for the in-scope solutions, including required interoperability, event sharing, correlation and workflows.
918	53	7.5.1 Migration - Activities are to be performed by Respective solution OEM (supported by bidder)	Detailed Migration Plan	“Rollback and Recovery Plan”	Kindly clarify whether rollback to incumbent solution is expected to be maintained for all migrations and for what minimum duration.	The Bidder shall plan and execute migration in a manner that minimizes the requirement for rollback. However, where rollback is required due to migration failure the Bidder shall maintain and execute an appropriate rollback/recovery plan on a case-by-case basis, subject to Bank approval.
919	54	7.5.1 Migration - Activities are to be performed by Respective solution OEM (supported by bidder)		“The bidder shall be responsible for migrating all applicable data…”	Kindly clarify solution-wise expected retention and migration of historical logs versus active configurations/use cases only.	Please be guided by the RFP refer Annexure 21
920	54	7.5.1 Migration - Activities are to be performed by Respective solution OEM (supported by bidder)	Item 1	“Telemetry Data”	Kindly clarify whether historical telemetry migration is mandatory for all relevant solutions or only where supported by OEM/product design.	All Historical data/log migration shall be undertaken.
921	54	7.5.1 Migration - Activities are to be performed by Respective solution OEM (supported by bidder)	Item 2	“Historical and Active Logs”	Kindly provide historical log volumes and expected migration depth/period, if migration of historical logs is mandatory.	Details shall be shared with the Successful bidder.

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
922	54	7.5.1 Migration - Activities are to be performed by Respective solution OEM (supported by bidder)	Item 3	“Rules, Policies, Configurations, and Use Cases”	Kindly provide indicative incumbent object counts solution-wise for effort estimation.	Details shall be shared with the Successful bidder.
923	54	7.5.1 Migration - Activities are to be performed by Respective solution OEM (supported by bidder)	Item 4	“Existing Customizations and Workflows”	Kindly request the Bank to share incumbent customization inventory and whether documentation/source configuration is available.	Details shall be shared with the Successful bidder.
924	54	7.5.1 Migration - Activities are to be performed by Respective solution OEM (supported by bidder)	Item 5	“Parsers, Connectors, and Integrations”	Kindly provide indicative number of custom parsers/connectors/integrations currently deployed in incumbent environment.	Details shall be shared with the Successful bidder.
925	54	7.5.1 Migration - Activities are to be performed by Respective solution OEM (supported by bidder)	Item 7	“Dashboards, Reports, and Alerts”	Kindly clarify whether dashboard/report migration is expected one-to-one or whether redesigned equivalent reporting may be accepted.	The Bidder shall configure the solution’s out-of-the-box (OOTB) dashboards, reports, workflows, policies, rules, and other applicable capabilities in accordance with the Bank’s approved configuration and requirements. Where the required functionality cannot be achieved through OOTB configuration, the Bidder shall propose an appropriate technically feasible alternative, including customization or functionally equivalent redesign, subject to the Bank’s approval.
926	54	7.5.1 Migration - Activities are to be performed by Respective solution OEM (supported by bidder)	Item 8	“Asset Inventory and Discovery Data”	Kindly clarify which solutions are expected to carry asset discovery/inventory migration responsibilities.	Please be guided by the RFP
927	54	7.5.1 Migration - Activities are to be performed by Respective solution OEM (supported by bidder)	Item 9	“User Profiles, Roles, and Access Configurations”	Kindly clarify whether identity/role migration will be handled through target system reconfiguration or direct import from incumbent systems.	Migration shall use the method supported by the target solution and approved by the Bank However, completeness of migration, data, logs etc. should maintained
928	54	7.5.1 Migration - Activities are to be performed by Respective solution OEM (supported by bidder)	Detailed Migration Plan	“Review, Validation, Testing, and Sign-off Processes”	Kindly clarify whether sign-offs will be obtained solution-wise and phase-wise.	Signoff would be provided solution & Agreed milstones wise
929	54	7.5.1 Migration - Activities are to be performed by Respective solution OEM (supported by bidder)	Service Requirement: Initiation	“Establish migration governance, conduct kick-off meetings…”	Kindly clarify whether one unified migration governance model is expected across all solution OEMs or separate governance workstreams per domain.	A unified overall migration governance framework shall be maintained by the Bidder, with solution/domain-specific workstreams wherever required.

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
930	54	7.5.1 Migration - Activities are to be performed by Respective solution OEM (supported by bidder)	Service Requirement: Execution	"Execute migration… while ensuring minimal risk, business continuity, data integrity, and no disruption to critical banking operations."	Kindly clarify the Bank's acceptable maintenance windows and downtime constraints for migration activities.	Maintenance windows and downtime shall be mutually planned based on solution criticality, business impact and Bank operational constraints.
931	55	7.5.1 Migration - Activities are to be performed by Respective solution OEM (supported by bidder)	Service Requirement: Closure & Stabilization	"Complete validation, documentation, knowledge transfer, sign-offs, stabilization activities…"	Kindly clarify expected stabilization duration and acceptance criteria after migration of each solution.	Please be guided by the RFP
932	55	7.5.2 Requirement Analysis - Activities are to be performed by Respective Solution OEM (supported by bidder)	7.5.2(1)	"conduct a detailed assessment of the Bank's business, functional, technical, operational, security, compliance, and integration requirements…"	Kindly clarify whether the Bank expects separate requirement analysis workshops for each solution or domain-wise consolidated workshops.	Workshops may be conducted solution-wise or through domain-wise consolidated sessions depending on interdependencies. The Bidder shall ensure that all solution-specific requirements are separately captured and traceable.
933	55	7.5.2 Requirement Analysis - Activities are to be performed by Respective Solution OEM (supported by bidder)	7.5.2(2)	"conduct workshops, discovery sessions, interviews, and discussions with the Bank's stakeholders and appointed consultants"	Kindly share the expected stakeholder groups and whether a consultant is already appointed by the Bank for this program.	The Bank shall nominate relevant stakeholders and consultants, where applicable, based on the requirements of the programme. The Bidder shall coordinate with such stakeholders
934	55	7.5.2 Requirement Analysis - Activities are to be performed by Respective Solution OEM (supported by bidder)	7.5.2(3)	"review the Bank's existing IT, security, application, network, cloud, and infrastructure landscape…"	Kindly clarify whether existing architecture documents and inventories will be shared upfront to reduce discovery effort during the five-month implementation period.	Relevant available documents and inventories shall be shared to the extent permissible.
935	55	7.5.2 Requirement Analysis - Activities are to be performed by Respective Solution OEM (supported by bidder)	7.5.2(4)	"identify all required data sources, integrations, dependencies, interfaces, telemetry sources, and compliance requirements…"	Kindly request a preliminary list of known data sources and dependencies that the Bank already expects to be in scope.	Known and available information shall be shared during requirement analysis/discovery. The Bidder shall identify additional dependencies necessary to fulfil the approved scope
936	56	7.5.2 Requirement Analysis - Activities are to be performed by Respective Solution OEM (supported by bidder)	7.5.2(5)(e)	"Definition of data sources, use cases, workflows, dashboards, reports, and analytics requirements"	Kindly clarify whether the Bank has predefined use case and reporting catalogs or whether these are to be built from scratch by bidder/OEM teams.	Existing known requirements/catalogues, where available, shall be shared. The Bidder/OEM shall analyse, validate and configure the required in-scope use cases, workflows, dashboards and reports.

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
937	56	7.5.2 Requirement Analysis - Activities are to be performed by Respective Solution OEM (supported by bidder)	7.5.2(6)	"coordinate with the Bank's internal teams, existing vendors, OEMs, and service providers…"	Kindly confirm whether the Bank will drive mandatory participation from incumbent teams and third parties within defined timelines.	The Bank shall facilitate participation of relevant internal stakeholders and available incumbent/third-party stakeholders. However, the Bidder shall remain responsible for proactive coordination, follow-up
938	56	7.5.2 Requirement Analysis - Activities are to be performed by Respective Solution OEM (supported by bidder)	7.5.2(7)	"prepare and submit a Functional Requirement Specification Manual (FRSM)…"	Kindly clarify whether FRSM is expected per solution, per domain, or as an overall integrated program artifact.	FRSM is to be provided solution wise
939	56	7.5.2 Requirement Analysis - Activities are to be performed by Respective Solution OEM (supported by bidder)	7.5.2(8)	"implement and deliver all functionalities… required to meet the requirements defined in the approved FRSM, RFP, and associated project documents."	Kindly clarify whether post-FRSM additions requested by the Bank but not explicitly covered in RFP will be treated as in-scope or governed separately.	Requirements added after FRSM approval and not part of the RFP requirement & approved scope shall not automatically become part of the Bidder's scope.
940	56	7.5.3 System Design - Activities are to be performed by Respective solution OEM (supported by bidder)	7.5.3(1)	"responsible for the end-to-end design, sizing, customization, configuration, integration, implementation…"	Kindly clarify whether "end-to-end design" includes underlying infrastructure sizing and environment design for all environments per solution.	End-to-end design shall include infrastructure sizing and environment design for the environments identified as in scope, including relevant capacity, availability, security and integration requirements.
941	56	7.5.3 System Design - Activities are to be performed by Respective solution OEM (supported by bidder)	7.5.3(2)	"support seamless interoperability, real-time integration, event sharing, correlation, orchestration, and automated response capabilities…"	Kindly clarify whether there is a Bank-mandated integration standard or central security operations platform architecture that all OEMs must align to.	The Bidder shall comply with Bank-approved enterprise architecture, security standards, integration standards and designated security operations platforms.
942	56	7.5.3 System Design - Activities are to be performed by Respective solution OEM (supported by bidder)	7.5.3(3)	"configurable and customizable to meet the Bank's functional, technical, operational, reporting, security, and compliance requirements."	Kindly clarify whether all customizations are expected within product-native capabilities or whether bespoke development across solutions is anticipated.	Product-native configuration/customization shall be preferred. Bespoke development shall be undertaken only where necessary for approved in-scope requirements and technically justified
943	56	7.5.3 System Design - Activities are to be performed by Respective solution OEM (supported by bidder)	7.5.3(5)(a)	"High-Level Design (HLD), including solution architecture, deployment architecture, integration architecture, and data flow architecture."	Kindly clarify whether a separate integration HLD across all solutions is required in addition to solution-level HLDs.	Solution-wise HLDs shall be supported by a consolidated integration architecture/HLD covering relevant cross-solution interfaces, dependencies and data flows.

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
944	56	7.5.3 System Design - Activities are to be performed by Respective solution OEM (supported by bidder)	7.5.3(5)(b)	"Low-Level Design (LLD), including detailed technical specifications, interface specifications, deployment details…"	Kindly confirm whether detailed interface specification documents are required for each integration point.	Detailed interface specifications shall be provided for material/critical integration points as required by the approved design, including interface method, protocols, authentication, data flow, dependencies and security requirements.
945	56	7.5.3 System Design - Activities are to be performed by Respective solution OEM (supported by bidder)	7.5.3(6)	"responsible for implementation of all solution components, integrations, interfaces, workflows, automation, business rules…"	Kindly clarify whether workflow and automation design across tools is to be centrally owned by bidder or by respective OEMs per product.	Product-specific workflow/automation shall be designed and implemented by the respective OEM/Bidder
946	56	7.5.3 System Design - Activities are to be performed by Respective solution OEM (supported by bidder)	7.5.3(7)	"ensure seamless integration with the Bank's internal systems, external entities, regulatory interfaces, fintech partners, and third-party applications…"	Kindly provide an indicative list of such external/regulatory/fintech integrations expected within scope.	Available known integrations shall be identified during discovery and documented in the approved integration inventory.
947	57	7.5.4 Development and Installation - Activities are to be performed by Respective Solution OEM (supported by bidder)	7.5.4(1)	"All installation, configuration, customization, testing, migration, integration, UAT, Go-Live… shall be performed from the Bank's premises."	Kindly clarify whether secure controlled remote support may be allowed for OEM TAC/product engineering activities where physical onsite presence is impractical.	Please be guided by the RFP
948	57	7.5.4 Development and Installation - Activities are to be performed by Respective Solution OEM (supported by bidder)	7.5.4(2)	"integrate the proposed solution with the Bank's ITSM, SLA Monitoring, monitoring, logging, authentication, and other enterprise platforms"	Kindly provide the enterprise platform list and indicate which ones are mandatory from day one versus phased.	The Bank shall provide the available enterprise platform inventory relevant to the scope with the successful bidder
949	57	7.5.4 Development and Installation - Activities are to be performed by Respective Solution OEM (supported by bidder)	7.5.4(3)	"coordinate with all relevant third parties, OEMs, service providers, and Bank stakeholders…"	Kindly clarify whether dependency-driven delays from these external stakeholders will be excluded from LD attribution.	Please be guided by the RFP. Penalty shall be levied for the delays attributable to the bidder.
950	57	7.5.4 Development and Installation - Activities are to be performed by Respective Solution OEM (supported by bidder)	7.5.4(4)	"provide all required integrations, connectors, parsers, APIs, workflows, playbooks, dashboards, reports, alerts, fine-tuning…"	Kindly clarify whether this requirement is limited to identified integrations/use cases at implementation stage or also includes future Bank demands during five-year O&M.	The requirement shall cover approved in-scope solutions, integrations and use cases.

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
951	57	7.5.4 Development and Installation - Activities are to be performed by Respective Solution OEM (supported by bidder)	7.5.4(6)	"The proposed solution shall be complete in all respects and shall not require any additional third-party software…"	Kindly clarify whether standard enterprise dependencies such as AD, DNS, SMTP, NTP, virtualization, and load balancer services are excluded from this restriction.	Please be guided by the RFP.
952	57	7.5.4 Development and Installation - Activities are to be performed by Respective Solution OEM (supported by bidder)	7.5.4(8)	"The implementation approach shall clearly define inputs, activities, outputs, deliverables, tools, templates, timelines…"	Kindly clarify whether the Bank has a prescribed PMO/governance template pack to be adopted by the bidder.	The Bidder shall propose and provide appropriate PMO/governance templates, end to end responsibilty lies with the bidder.
953	57	7.5.4 Development and Installation - Activities are to be performed by Respective Solution OEM (supported by bidder)	7.5.4(10)	"The implementation scope shall include requirement gathering, SRS/FRS preparation…"	Kindly clarify whether a separate Business Analyst role is expected as part of bidder team, especially since technical evaluation refers to PM and Business Analyst.	Please be guided by the RFP
954	57	7.5.4 Development and Installation - Activities are to be performed by Respective Solution OEM (supported by bidder)	7.5.4(12)	"Any shortfall in sizing, capacity, performance, availability, or scalability… shall be rectified by the bidder at no additional cost"	Kindly clarify whether Bank-driven growth beyond stated annexure volumetrics will also be treated as bidder sizing obligation or handled through right-to-alter quantities/commercial augmentation.	The Bidder shall be responsible for adequacy of sizing against the volumes, requirements and assumptions stated in the RFP
955	58	7.5.5 Documentation - Activities are to be performed by Respective solution OEM (supported by bidder)	7.5.5	"prepare, maintain, obtain Bank approval/sign-off, and submit all project, technical, operational, security, and administrative documentation…"	Kindly clarify whether documentation sign-off will occur solution-wise or only at aggregate program milestones.	documentation may be reviewed and signed off solution-wise and milestone-wise,
956	58	7.5.5 Documentation - Activities are to be performed by Respective solution OEM (supported by bidder)	Deliverable 1	"Detailed Project Plan and Implementation Plan"	Kindly confirm whether these documents are expected at both master program level and individual solution level.	The Bidder shall submit a consolidated master programme plan supported by detailed solution-wise implementation plans covering activities, dependencies, milestones, resources, risks, testing, migration, cutover and Go-Live.
957	58	7.5.5 Documentation - Activities are to be performed by Respective solution OEM (supported by bidder)	Deliverable 3	"High-Level Design (HLD) and Low-Level Design (LLD) Documents"	Kindly clarify whether HLD/LLD are required per environment (DC/DR/UAT/Pre-Prod) as separate annexures.	HLD/LLD shall address each applicable environment. Separate documents/annexures shall be provided where architectural or deployment differences warrant separate treatment

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
958	58	7.5.5 Documentation - Activities are to be performed by Respective solution OEM (supported by bidder)	Deliverable 7	"Testing, Validation, Acceptance, and Go-Live Documents"	Kindly clarify whether a common Bank acceptance template will be provided for each solution.	The Bidder shall prepare solution-specific acceptance evidence, test results and supporting documents
959	58	7.5.5 Documentation - Activities are to be performed by Respective solution OEM (supported by bidder)	Deliverable 11	"Backup, Recovery, Business Continuity, and Disaster Recovery Procedures"	Kindly clarify whether these procedures are expected per solution or as a consolidated platform-level DR runbook.	The Bidder shall prepare solution-specific Backup, Recovery, BC and DR procedures Integrated DR/BC runbook shall also be maintained for inter-solution dependencies and coordinated exercises.
960	58	7.5.5 Documentation - Activities are to be performed by Respective solution OEM (supported by bidder)	Deliverable 14	"The Secure Configuration Documents (SCDs)… shall be reviewed at least quarterly…"	Kindly clarify whether this quarterly review is part of recurring FM effort for all solutions across the full contract period.	Quarterly review shall form part of recurring FM activities for all applicable in-scope solutions throughout the contract period.
961	58	7.5.6 Deployment and Go-Live - Activities are to be performed by Respective Solution OEM (supported by bidder)	7.5.6(1)	"deployment of the solution in the production environment, Go-Live planning, implementation, installation, configuration, fine-tuning, migration, stabilization, and hyper care support."	Kindly clarify whether hyper-care commences solution-wise immediately after each go-live or only after program-wide go-live.	Hyper-care shall commence solution-wise upon the respective Go-Live
962	58	7.5.6 Deployment and Go-Live - Activities are to be performed by Respective Solution OEM (supported by bidder)	7.5.6(2)	"provide onsite support during the hyper care period…"	Kindly clarify minimum expected onsite hyper-care staffing duration and whether this is over and above O&M team deployment.	Minimum staffing shall be as specified in the RFP/approved resource plan.
963	58	7.5.6 Deployment and Go-Live - Activities are to be performed by Respective Solution OEM (supported by bidder)	7.5.6(4)	"Prior to Go-Live, the solution shall undergo security validation activities, including VAPT, IS Audit, readiness assessments…"	Kindly clarify which validation activities are Bank-arranged versus bidder/OEM-arranged.	Bidder/OEM shall conduct and support solution-level security validation, testing and remediation. Bank/appointed auditors may conduct independent IS Audit/VAPT/readiness assessments
964	59	7.5.6 Deployment and Go-Live - Activities are to be performed by Respective Solution OEM (supported by bidder)	7.5.6(5)	"conduct performance testing prior to UAT and Go-Live…"	Kindly clarify whether performance testing is mandatory for all products irrespective of traffic/control plane relevance.	Performance testing shall be applicability-based, considering traffic, transaction volume, control-plane/data-plane relevance, scalability and criticality. Bank may require testing where risk warrants.

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
965	59	7.5.6 Deployment and Go-Live - Activities are to be performed by Respective Solution OEM (supported by bidder)	7.5.6(6)	"Load Testing / Stress Testing / Scalability Testing / Endurance Testing / Failover and Recovery Testing"	Kindly confirm whether the Bank will accept applicability-based testing plans per solution.	Test types shall be determined through the approved solution-specific test plan and risk assessment.
966	59	7.5.6 Deployment and Go-Live - Activities are to be performed by Respective Solution OEM (supported by bidder)	7.5.6(7)	"measure and report key performance indicators…"	Kindly clarify whether target KPI thresholds will be provided by the Bank solution-wise.	RFP/SLA thresholds shall prevail. Where a KPI is not expressly defined, bidder shall propose measurable thresholds for Bank approval during requirement finalization.
967	59	7.5.7 Testing- Activities are to be performed by Respective solution OEM (supported by bidder)	7.5.7(1)	"The Bank shall conduct User Acceptance Testing (UAT)…"	Kindly clarify whether UAT will be conducted separately for each solution/workstream.	UAT shall be conducted solution/workstream-wise, with integrated UAT where cross-solution dependencies require it.
968	59	7.5.7 Testing- Activities are to be performed by Respective solution OEM (supported by bidder)	7.5.7(3)	"The bidder shall provision and maintain dedicated Development, Testing, UAT, and Pre-Production environments throughout the contract period."	Kindly clarify whether this requirement applies to all 21 solutions individually, including appliance-based and SaaS-hosted offerings.	Please be guided by the RFP
969	59	7.5.7 Testing- Activities are to be performed by Respective solution OEM (supported by bidder)	7.5.7(3)	"All software, licenses, and other resources required for such environments shall be included…"	Kindly confirm whether these non-production environments need to be maintained for the full five-year support term.	Yes, All environment is to be maintained throughout the contract period
970	60	7.5.7 Testing- Activities are to be performed by Respective solution OEM (supported by bidder)	7.5.7(8)	"support periodic reviews, assessments, audits, and compliance validation activities…"	Kindly clarify expected periodicity/frequency of these recurring activities during O&M.	Statutory/regulatory and RFP-prescribed frequencies shall apply. Other periodic activities shall be performed as per Bank-approved annual/quarterly operational calendar and risk requirements.
971	60	7.7.6.1 Quality Assurance	1(a)	"prepare detailed test plans, test cases, test data, automation scripts…"	Kindly clarify whether detailed testing artifacts are expected per solution for all test types or only where applicable.	Test plans, cases, evidence and reports shall be solution-wise and for each applicable test type to be created by Bidder/OEM and approved by bank
972	60	7.7.6.1 Quality Assurance	2(b)	"Establish and maintain the required test environments…"	Kindly confirm whether the test environments may be shared across domains/solutions where technically feasible.	Please be guided by the RFP
973	61	7.7.6.1 Quality Assurance	4(o)	"Any other testing required to ensure successful implementation and acceptance of the solution"	Kindly clarify whether additional unlisted test types may be introduced during implementation and how such scope will be governed.	Bank may require additional testing reasonably necessary for security, compliance, resilience or acceptance.
974	61	7.5.8 Training- Activities are to be performed by Respective solution OEM (supported by bidder)	7.5.8	"The bidder and respective OEMs shall provide comprehensive product training, knowledge transfer, and certification programs…"	Kindly clarify whether bidder resources are expected to conduct supplementary KT beyond OEM-delivered technical training.	Bidder, on need basis, shall provide supplementary operational/administrative KT required for effective FM, in addition to OEM product training.
975	62	7.5.8 Training- Activities are to be performed by Respective solution OEM (supported by bidder)	Training Table	"Beginner/Foundation Training – 2 Days – 5 Sessions"	Kindly clarify whether this session count applies separately to each of the 21 solutions.	Please refer Addendum 1 for the revised clause. Training shall be solution/product-wise

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
976	62	7.5.8 Training- Activities are to be performed by Respective solution OEM (supported by bidder)	Training Table	"Advanced/Administrator Training – 3 Days – 5 Sessions"	Kindly confirm whether domain-wise combined training by OEM/product family shall be acceptable.	Please refer Addendum 1 for the revised clause. Training shall be solution/product-wise
977	62	7.5.8 Training- Activities are to be performed by Respective solution OEM (supported by bidder)	Training Table	"Backend Administration, Troubleshooting & Maintenance Training – 3 Days – 5 Sessions"	Kindly clarify whether Bank expects hands-on lab environments to be provisioned as part of these training sessions.	Please refer Addendum 1 for the revised clause.
978	62	7.5.8 Training- Activities are to be performed by Respective solution OEM (supported by bidder)	Final Para	"The Bank reserves the right to nominate participants… and request additional refresher or knowledge transfer sessions during the contract period"	Kindly clarify whether such refresher sessions are uncapped and on-demand throughout the contract period.	Please be guided by the RFP, Please refer Addendum 1 for the revised session table.
979	63	7.5.9 Security requirements - Activities are to be performed by Respective solution OEM (supported by bidder)	7.5.9(1)	"comply with the Bank's IT, Information Security, Cyber Security, Data Protection, Privacy, Business Continuity…"	Kindly request the Bank to share the applicable policy set during bid stage or confirm that these will be finalized during post-award requirement analysis.	Policies/documents presently available and releasable may be shared with the successful bidder. Bidder shall comply with the Bank's applicable policies, standards and regulatory requirements communicated during implementation
980	63	7.5.9 Security requirements - Activities are to be performed by Respective solution OEM (supported by bidder)	7.5.9(6)	"All Bank data… shall reside within India."	Kindly clarify whether support telemetry, masked diagnostics, and OEM cloud verdict exchange without identifiable Bank data are permissible.	Please be guided by the RFP
981	64	7.6 Cloud Service Provider Responsibilities	7.6(1)	"establish and manage a dedicated cloud landing zone, including Development, UAT, and Production environments…"	Kindly clarify for which solutions cloud landing zone establishment is expected within bidder scope.	Cloud landing zone shall be required only for solutions explicitly proposed/approved for IaaS/PaaS/cloud deployment under the RFP
982	64	7.6 Cloud Service Provider Responsibilities	7.6(2)	"responsible for provisioning, configuration, administration, monitoring, patching, upgrading, backup, recovery…"	Kindly clarify whether this applies equally to OEM-managed SaaS offerings or only IaaS/PaaS hosted solutions.	Please be guided by the RFP.
983	64	7.6 Cloud Service Provider Responsibilities	7.6(3)	"secure connectivity with the Bank's on-premises infrastructure…"	Kindly clarify whether Bank-provided network connectivity and security gateway services will be available for such hybrid deployments.	Bank shall facilitate connectivity under its control. Bidder shall design and provide solution-side configurations/components required for secure connectivity.
984	64	7.6 Cloud Service Provider Responsibilities	7.6(9)	"support high availability, fault tolerance, disaster recovery, multi-site deployment…"	Kindly clarify whether separate DR region/zone architecture is expected even for SaaS/OEM-hosted services.	Please be guided by the RFP
985	64	7.6 Cloud Service Provider Responsibilities	7.6(11)	"The bidder shall be responsible for sizing all cloud resources…"	Kindly clarify whether bidder is expected to estimate cloud consumption commercially for OEM-hosted managed/SaaS platforms as well.	Bidder shall appropriately size and commercially account for required cloud/SaaS consumption for the proposed solution as applicable.
986	65	7.6 Cloud Service Provider Responsibilities	7.6(15)	"submit compliance against the Technical Specifications – Sheet Name: CSP Compliance Requirements for every solution proposed under IaaS, PaaS, or SaaS…"	Kindly clarify whether one consolidated CSP compliance is acceptable where multiple solutions are hosted on the same OEM/CSP platform.	Bidder to submit the compliance for each solution separately
987	70	7.11 Resource Requirement	7.11 Intro	"resource requirements specified in this RFP represent the minimum onsite deployment obligations."	Kindly confirm whether these are hard minimum named resources irrespective of automation and OEM support model.	Please be guided by the RFP
988	70	7.11 Resource Requirement	Implementation Phase	"The bidder shall deploy a dedicated onsite Project Manager for the implementation phase…"	Kindly clarify whether one onsite PM for the full program is sufficient or whether the Bank expects domain/project leads in addition.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
989	70	7.11 Resource Requirement	Implementation Phase	"shall nominate appropriate OEM and bidder resources for each solution, workstream, milestone, and project activity."	Kindly clarify whether bidder must name solution-wise resources in the bid itself or only submit detailed deployment plan post-award.	Please be guided by the RFP. Refer the clause under Section 7.11: Prior to commencement of implementation activities, the bidder and respective OEMs shall submit a detailed Resource Deployment Plan identifying the proposed resources, roles, responsibilities, certifications, experience, deployment schedules, and solution-wise allocation for Bank approval.
990	70	7.11 Resource Requirement	O&M Phase	"The bidder shall deploy the minimum onsite L1, L2, Project Manager – Operations…"	Kindly clarify when exactly O&M staffing starts—installation, UAT, Go-Live, or post-stabilization.	O&M staffing commences from the date of Go-live of respective solution
991	70	7.11 Resource Requirement	O&M Phase	"The respective OEMs shall provide L3 support resources and subject matter experts from the date of installation…"	Kindly clarify whether OEM L3s are expected full-time onsite from date of installation for every solution.	Refer Section 7.11. OEM L3 support is required from date of installation, not mandatory full-time onsite for every solution.
992	70	7.11 Resource Requirement	O&M Phase	"adequate onsite and offsite SME support…"	Kindly confirm whether offsite SMEs may be shared across domains and shifts.	Refer Section 7.11. Offsite SMEs may be shared across domains and shifts, subject to Bank's service-level requirements.
993	71	7.11 Resource Requirement	Resource Management and Governance	"All deployed resources shall be named resources."	Kindly clarify whether this applies to OEM offsite L3/SME pools also, or only to onsite deployed personnel.	Refer Section 7.11. Applies to onsite deployed personnel
994	71	7.11 Resource Requirement	Resource Management and Governance	"Any replacement, withdrawal, reassignment, or removal of resources shall require prior written approval…"	Kindly clarify whether temporary leave coverage and shift substitutions also require prior written approval.	Prior approval shall not normally be required for routine leave/shift substitution where minimum staffing, competency and SLA coverage are maintained. Bidder to esnure that roaster is pre-approved by bank for any shift subsititution or planned levaes
995	71	7.11 Resource Requirement	Resource Management and Governance	"The Bank may require additional onsite resources during the contract period…"	Kindly clarify whether such additional Bank-requested manpower is chargeable on prorated basis even if beyond the bidder's right-sized model.	Additional resources required due to bidder under-sizing, SLA/performance shortfall or contractual obligations shall be at no additional cost
996	71	7.11 Resource Requirement	Implementation Phase Resource Type 1	"Project Manager – Implementation"	Kindly confirm whether this role is expected to be dedicated full-time onsite from TO till all solution go-lives.	A dedicated Onsite PM shall be available throughout implementation.
997	71	7.11 Resource Requirement	Implementation Phase Resource Type 2	"OEM Implementation Resources… OEM shall submit a detailed resource deployment plan…"	Kindly clarify whether OEM implementation resources must be resident onsite continuously or mobilized by project phase/activity.	OEM resources shall be mobilized based on project phase/activity and shall be onsite for implementation, testing, Go-Live or other activities. Remote access shall not be provided
998	71	7.11 Resource Requirement	Implementation Phase Resource Type 3	"Bidder Implementation Resources… submit a detailed resource deployment plan…"	Kindly clarify whether bidder implementation resources are expected solution-wise, domain-wise, or centralized PMO/architecture/governance roles.	Bidder may propose centralized PMO/architecture/governance resources together with solution/domain resources, provided all contractual responsibilities and coverage are met.
999	71	7.11 Resource Requirement	O&M Resource Type 4	"L1 Security Resources"	Kindly clarify whether L1 resources may be cross-skilled across security domains as long as minimum coverage and SLAs are met.	The Count of Resources provided are minimal
1000	72	7.11 Resource Requirement	O&M Resource Type 5	"L2 Security Resources"	Kindly clarify whether L2 resources are expected as domain leads or product-specific specialists.	The Count of Resources provided are minimal
1001	72	7.11 Resource Requirement	O&M Resource Type 6	"L3/ Project Manager – Operations"	Kindly clarify whether this is one common onsite operations lead or dedicated L3 equivalent expected across domains.	The Count of Resources provided are minimal
1002	72	7.11 Resource Requirement	IT Infrastructure Resource Type 7	"L1 IT Infrastructure Resources"	Kindly clarify whether these resources are for the infrastructure deployed only under this RFP, and not broader Bank infra.	The Resources for the bidder's proposed Infrastructure
1003	72	7.11 Resource Requirement	IT Infrastructure Resource Type 8	"L2 IT Infrastructure Resources"	Kindly clarify whether database, OS, virtualization, network, and backup specialization is expected to be embedded in these infra roles.	The Resources for the bidder's proposed Infrastructure
1004	72	7.11 Resource Requirement	Note	"No remote access shall be provided to any resource"	Kindly clarify how OEM TAC, offsite SME support, and SaaS/cloud administration activities are expected to be handled operationally.	Controlled remote support (on case to case basis) may be allowed by the Bank through approved secure mechanisms, with authorization, logging, monitoring and time-bound access.
1005	72	7.11 Resource Requirement	Note	"respective OEMs are required to provide L3 resource each from the date of IT Security solutions installation."	Kindly confirm whether "each" means one L3 per OEM/product full-time or availability on demand.	L3 support shall be available as required to meet contractual SLAs. Continuous dedicated onsite L3 per OEM/product is not automatically required unless expressly specified.
1006	73	7.11 Resource Requirement	MINIMUM RESOURCE COUNT DEPLOYMENT	"The following table represents the minimum onsite resource deployment requirements."	Kindly confirm whether the prescribed minimum staffing is cumulative across the integrated environment, not per solution or per domain.	The Count of Resources provided are minimal
1007	73	7.11 Resource Requirement	Shifts Table	"Shift A / Shift B / Shift C"	Kindly clarify the exact shift timings and whether the Bank has predefined shift windows.	Details shall be shared with the Successful bidder.
1008	73	7.11 Resource Requirement	Shifts Table	"Bidder to right size"	Kindly clarify whether additional right-sized resources above minimum need not be named in the bid but may be finalized post-award.	Please be guided by the RFP
1009	73	7.11 Resource Requirement	Security Domain Minimum Competency Coverage	"Resources may be cross-skilled and mapped to multiple security domains…"	Kindly confirm that dedicated per-product resource allocation is not mandatory if cross-skilled pooled teams meet SLA and operational requirements.	Please be guided by the RFP
1010	74	7.11 Resource Requirement	Note 4	"The bidder shall augment resources at no additional cost wherever required…"	Kindly clarify whether this clause is intended for bidder underestimation/performance shortfall only, and excludes Bank-driven scope expansion.	The Bidder shall augment resources at no additional cost where required to meet the approved scope, SLAs and contractual obligations
1011	75	7.11 Resource Requirement	Resource Deployment, Replacement and Governance (11)	"Subcontracting of any part of the services under this project shall not be permitted."	Kindly confirm that OEM-deployed personnel on OEM payroll remain permissible as they are explicitly envisaged throughout the RFP.	OEM resources expressly envisaged under the RFP shall be permitted; the Bidder shall remain fully responsible for their performance and compliance.
1012	75	7.11 Resource Requirement	Responsibilities of Project Manager	"Lead and govern the implementation, transition, and operational activities…"	Kindly clarify whether a single PM is expected to cover both transition and implementation or separate PMs may be proposed for implementation and operations.	Bidder may propose one PM or separate implementation/operations PMs,

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
1013	76	7.12 Facilities Management	7.12(1)	"Bidder should manage, monitor, maintain and upgrade all proposed solutions & services on ongoing basis…"	Kindly clarify whether FM scope begins from respective go-live date or from installation date.	Formal FM support for each solution shall commence from its respective Bank-approved Go-Live
1014	76	7.12 Facilities Management	7.12(2)	"All daily routine and standard activities of L1 and L2 to be automated in phased manner from the date of Go-live."	Kindly clarify expected automation targets, milestones, and whether custom automation development is required beyond product-native features.	Automation shall be implemented in a phased manner using product-native/standard capabilities
1015	76	7.12 Facilities Management	7.12(3)	"Bidder shall be responsible to develop and maintain Standard Operating Procedures (SOP)…"	Kindly clarify whether SOPs are expected per solution, per domain, or as an integrated runbook set.	SOPs shall be maintained at the appropriate solution/domain level and consolidated into integrated operational runbooks where interdependencies exist.
1016	76	7.12 Facilities Management	7.12(5)	"onsite personnel… carrying out regular patch management, firmware updates, software upgrades…"	Kindly clarify whether all upgrade execution during O&M is expected from bidder onsite resources or OEM-led with bidder coordination.	Bidder shall own coordination and operational execution. OEM shall perform product-specific activities where required by OEM certification/support conditions.
1017	76	7.12 Facilities Management	7.12(6)	"Monthly Security Certificate to be submitted…"	Kindly clarify whether this certificate is limited to in-scope managed solutions and based on best-effort operational assessment.	Certificate shall cover only in-scope managed solutions and shall be based on actual operational/security activities and evidence available during the reporting period.
1018	77	7.12 Facilities Management	7.12(10)	"Participate and contribute in every DR drill, cyber security drill, tabletop exercises…"	Kindly clarify expected frequency and duration of such exercises for manpower planning.	requencies expressly specified in the RFP shall apply. Other exercises shall be as per Bank-approved annual calendar/risk requirements.
1019	77	7.12 Facilities Management	7.12(11)	"Conduct DR drill of the Security on quarterly interval…"	Kindly clarify whether this applies to each solution independently or as an integrated quarterly security DR exercise.	The Bank may conduct an integrated quarterly security DR exercise, supplemented by solution-specific drills
1020	77	7.12 Facilities Management	7.12(12)	"Develop custom plug-ins, parsers, connectors, agents, adopters for all the systems in the Bank…"	Kindly clarify whether this obligation is limited to systems identified in agreed onboarding scope and roadmap.	Please be guided by the RFP
1021	77	7.12 Facilities Management	7.12(14)	"Perform monthly gap analysis of current levels of logs enabled…"	Kindly clarify whether Bank will provide current logging baseline and target state expectations.	Bank shall provide available baseline information. Bidder shall independently assess gaps and recommend the target logging state based on contractual, security and regulatory requirements.
1022	77	7.12 Facilities Management	7.12(15)	"configure the required rules, AI/ML based analytics, self-learning models & processes…"	Kindly clarify whether separate analytics/data science expertise is expected as part of bidder manpower.	Bidder/OEM shall provide appropriate analytics expertise sufficient to meet the required use cases.
1023	78	7.12 Facilities Management	7.12(17)	"Create new and customize existing reports, dashboards, rules, queries, user interface…"	Kindly clarify whether such recurring changes will be prioritized and governed through a Bank-approved change framework.	All changes shall be governed through the Bank-approved change management process.
1024	78	7.12 Facilities Management	7.12(18)	"Define formats for MIS reporting…"	Kindly clarify whether the Bank has predefined MIS/reporting templates for O&M.	Bidder shall propose formats for Bank approval.
1025	78	7.12 Facilities Management	7.12(22)	"recommendations in the report should be rectified… within a week's time."	Kindly clarify whether this applies only to routine recommendations not involving external dependencies, downtime approvals, or architectural changes.	One-week remediation shall apply to routine recommendations
1026	79	7.12 Facilities Management	7.12(31)	"Feature requests, all critical, showstopper declared by the Bank needs to be implemented within 1 week…"	Kindly clarify whether this applies only to configuration/policy/rule changes within existing capabilities, excluding major product development or OEM roadmap dependencies.	One-week implementation shall apply to configuration/policy/rule changes feasible
1027	79	7.12 Facilities Management	7.12(41)	"Bidder & OEMs should engage data scientists for analytics…"	Kindly clarify whether dedicated data scientist roles are expected to be part of proposed FM manpower.	adequate analytics capability shall be factored
1028	82	7.12.2 DR Drill	7.12.2	"The bidder is responsible for conducting the DR Drill on a regular basis…"	Kindly clarify whether the Bank has a predefined DR drill calendar and whether all solution OEMs are expected to participate each time.	The Bank maintain/approve the DR exercise calendar. Bidder and Relevant OEMs shall participate where their solution is involved or their technical expertise is required.
1029	82	7.12.3 IT Security operations	7.12.3(1)	"manage, monitor, maintain and upgrade all IT SECURITY solutions on ongoing basis…"	Kindly confirm whether "all IT SECURITY solutions" refers only to proposed solutions under this RFP or also interim legacy solutions under transition.	O&M scope shall primarily cover proposed/in-scope solutions under this RFP.
1030	83	7.12.3 IT Security operations	7.12.3(4)	"All daily routine and standard activities of L1 and L2 to be fully automated."	Kindly clarify expected extent of "fully automated" and whether this is a contractual measurable obligation.	"Fully automated" shall mean automation of identified routine and standard activities to the maximum technically feasible extent using approved/native automation
1031	83	7.12.3 IT Security operations	7.12.3(12)	"L3 support executive should be available during Bank's business hours and whenever required…"	Kindly clarify whether one common onsite L3/operations manager supported by offsite SMEs/OEMs will be acceptable.	Please be guided by the RFP
1032	84	7.12.3 IT Security operations	7.12.3(20)	"The bidder should use bank provided Ticketing tool…"	Kindly confirm whether ITSM workflows, dashboards, and approval matrices will be configured by the Bank or by bidder.	The Bank shall provide access to the relevant ITSM platform, along with the approved business requirements, workflow requirements, approval matrices, and integration requirements. The Bidder shall configure the cybersecurity solution-side ITSM integrations, workflows, dashboards, notifications, and operational interfaces within the scope of the proposed solution, in coordination with the Bank and the Bank's designated ITSM service provider. Any configuration required within the ITSM platform itself shall be performed by the Bank or its designated ITSM service provider
1033	86	7.12.4 OEM Services & Deployment (Architecture Assessment)	Assessment List	"List of Solution for which Assessment is to be conducted are…"	Kindly clarify whether annual architecture/performance assessments are limited only to the listed seven solutions under this clause.	Please be guided by the RFP
1034	87	7.12.5 System recovery	7.12.5(2)	"Bidder to ensure that scheduled / unscheduled DR drills is conducted on regular basis…"	Kindly clarify whether unscheduled drills may be invoked without prior planning and how OEM availability will be handled.	Bank may invoke unscheduled drills where security, regulatory or risk considerations warrant. Reasonable notice shall ordinarily be provided where operationally feasible; bidder shall ensure relevant OEM availability as part of support obligations.
1035	88	7.13 IT Infrastructure	7.13(1)	"The bidder shall be responsible for the supply, installation, configuration, integration, testing, commissioning, documentation, warranty, and comprehensive maintenance of the proposed IT infrastructure…"	Kindly clarify whether bidder responsibility is limited to infrastructure procured under this RFP or extends to shared Bank-owned infrastructure hosting these solutions.	Bidder responsibility shall be limited to in-scope infrastructure and solution components expressly covered under the RFP."

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
1036	89	7.13 IT Infrastructure	7.13(5)(ii)	"The bidder/OEM is responsible for supplying, designing, sizing and configuring the Backup Software and Hardware…"	Kindly clarify this with Annexure 21 where backup and retention is stated as "Provided and maintained by bank."	Please refer Addendum 1 for the revised clause.
1037	92	7.13 IT Infrastructure	7.13(11)	"IT infrastructure managed services"	Kindly confirm that infrastructure O&M scope is limited to the solution landscape deployed under this RFP and not the Bank's general enterprise infrastructure.	The IT Infrastructure proposed by the bidder
1038	94	7.14.2 Transition Management	7.14.2(2)	"The bidder shall take over and maintain operations of the bank's existing solutions starting 01.05.2027…"	Kindly clarify whether this date-driven takeover is mandatory irrespective of actual project progress/status of individual solutions.	Takeover shall be aligned to the contractual transition plan and actual readiness/status. The bidder shall support continuity arrangements where delays are attributable to the bidder as stipulated in the RFP.
1039	97	8 CONTRACT PERIOD	8	"Implementation Period + Support period (60 Month Post Go-live)"	Kindly clarify whether FM support charges commence only post go-live or whether pre-go-live transition/interim support is also included within the same commercials.	FM support charges shall commence from respective Go-Live
1040	97	9 PROJECT TIMELINES	9	"Overall Implementation period shall be 5 Months (Start Date is T0) for all solution & services"	Kindly clarify whether phased go-live by solution/domain/workstream within the overall five-month program is acceptable, given the scale of implementation, migration, testing, transition, and OEM coordination involved.	Phased solution/domain/workstream Go-Live shall be permitted, provided the overall implementation milestones & timelines are met & complied
1041	8	KEY INFORMATION	1	Last Date and Time for submission of Bids: 16th September 2026, 3pm	Requesting a 2-week extension on the Bid submission deadline.	Please refer Addendum 1 for the revised clause.
1042	47	7.3.5.1 Identity & Access Management Solution	7	The Bank requires a scalable IDAM solution with capabilities for user lifecycle management, identity governance, SSO support, RBAC enforcement, and integration with MFA, HRMS, ITSM, SIEM, etc., deployed on-premises at DC & DR	What is the source of truth (HRMS) used in the bank?	The Bank shall provide the applicable authoritative HR/user source during requirement finalization.
1043	47	7.3.5.1 Identity & Access Management Solution	7	The Bank requires a scalable IDAM solution with capabilities for user lifecycle management, identity governance, SSO support, RBAC enforcement, and integration with MFA, HRMS, ITSM, SIEM, etc., deployed on-premises at DC & DR	Does the bank have any existing IDAM Solution?	Please refer Annexure 21
1044	47	7.3.5.1 Identity & Access Management Solution	7	The Bank requires a scalable IDAM solution with capabilities for user lifecycle management, identity governance, SSO support, RBAC enforcement, and integration with MFA, HRMS, ITSM, SIEM, etc., deployed on-premises at DC & DR	Does the bank have any existing Access Management (SSO) solution?	Please refer Annexure 21
1045	48	7.2.2.1. Multi Factor Authentication	7	The bank intends to implement a Multi-Factor Authentication (MFA) solution to enhance the security of its digital infrastructure by introducing an additional layer of authentication that goes beyond traditional username and password, ensuring that only authorized users can access critical banking systems, applications, and customer data.	Does the bank have any existing MFA solution?	Please refer Annexure 21
1046	211	7.3.5.1 / Volumetrics Table (15.21.4)	7	Solution Name : IDAM Volumetrics : 12000 scalable to 16000	12,000→16,000 user count, please confirm if this count if for regular employees or if it includes contractors, vendors, third-party, etc.? Does this count also include privileged users?	The stated volumetric shall be treated as the baseline sizing requirement. Final user-category breakup, including employees, contractors, third parties and privileged users, shall be provided during requirement finalization.
1047	47	7.3.5.1 Identity & Access Management Solution	7	The Bank requires an Identity & Access Management (IDAM) solution to establish secure, centralized control over user identities, access rights, and authentication mechanisms across its IT ecosystem	Kindly provide an overview of the current IT Ecosystem: 1) Kindly share the list of applications/sources that are in scope for the IDAM solution? 2) Please provide breakup based on category of applications (ERP application, Web service, database, legacy, CRMs, ITSM, SIEM etc.).	The Bank shall provide the available application/source inventory during discovery.
1048	47	7.3.5.1 Identity & Access Management Solution	7	The Bank requires a scalable IDAM solution with capabilities for user lifecycle management, identity governance, SSO support, RBAC enforcement, and integration with MFA, HRMS, ITSM, SIEM, etc., deployed on-premises at DC & DR	Please clarify if there are any preferred directory services or versions to be integrated (e.g., AD, LDAP, Azure AD), and if cloud directory integration is within scope.	Applicable directory services and versions shall be established during discovery. Integration shall cover Bank-approved directory sources; cloud directory integration shall be included
1049	47	7.3.5.1 Identity & Access Management Solution	7	It should support Single Sign-On (SSO), integration with multiple directories, and enforce role-based access controls while ensuring compliance with regulatory standards.	Kindly provide number of applications to be enabled for SSO, with breakup of SAML, OAuth 2.0, OIDC and any other authentication methods	The Bank shall provide available application inventory and protocol details during SRS
1050	47	7.3.5.1 Identity & Access Management Solution	7	It should support Single Sign-On (SSO), integration with multiple directories, and enforce role-based access controls while ensuring compliance with regulatory standards.	Are there any existing RBAC metrics for the in-scope applications? OR the bidder needs to create the matrix?	Bank shall provide existing RBAC information where available. Bidder shall assess, rationalize and configure RBAC based on approved requirements.
1051	48	7.2.1.2. Privilege Identity Management (PIM)	7	The Bank intends to upgrade its existing Privileged Identity Management (PIM) solution to enhance control and security over privileged access across its critical IT infrastructure and enterprise applications.	Please share details of existing PAM solution & its coverage (architecture, licenses, managed privileged accounts, integrations). Do we need to upgrade the existing solution or need to implement a new solution?	Please refer Addendum 1 for the revised clause.
1052	48	7.2.1.2. Privilege Identity Management (PIM)	7	The upgraded solution must provide comprehensive privileged account management, including secure credential storage (password vaulting), real-time session monitoring, granular access control, and detailed audit trails	1) Kindly confirm the privileged user count is ~1500 (as per RFP), target assets ~4500 (as per RFP). 2) Please confirm the expected session recording retention period for solution sizing and licensing.	Please refer Addendum 1 for the revised clause. The RFP volumetrics shall be treated as the baseline for sizing. Session-recording retention shall comply with the RFP, regulatory requirements and Bank-approved retention policy; bidder shall size accordingly.

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
1053	58	7.5.6 Deployment and Go-Live	7	The bidder and respective OEM shall be responsible for deployment of the solution in the production environment, Go-Live planning, implementation, installation, configuration, finetuning, migration, stabilization, and hyper care support.	Please confirm that as per RFP, L1/L2 resources are required on-site and L3 is to be available during business hours.	Please be guided by the RFP
1054	105	10.2 Eligibility Evaluation Criteria: Clause - 19	10	The proposed OEM solution/product for Privilege Identity/Access Management should have been successfully implemented in at least 2 BFSI in India, out of which at least one (1) BFSI Client should have a deployment covering more than 1,500 privileged users Note: Experience should be during the five-year period preceding the RFP publication date. Even if the installation was completed more than five years ago, it will still qualify, provided the product is currently under maintenance or has been maintained at any time during the five-year period preceding the RFP publication date	Should the Proposed PAM solution implementation also be done by Bidder or the requirement is for bidder to be part of management/upgradation (not necessarily new implementation) of PAM solution in at least 2 BFSI in India. Can we get a relaxation in this criteria - considering implementation for 1 BFSI Client in India	Please be guided by the RFP. The requirement stated in this clause is for the OEM to provide the implementation experience of the mentioned solution. The experience should be of the proposed OEM solution/product for Privilege Identity/Access Management.
1055	31	7 Scope of Work - E. Management Layer and Security	7	IDAM (Identity and Access Management), Multi-Factor Authentication, PIM (Privileged Identity Management)	In RFP, the ask is for IDAM, SSO/MFA and PAM requirements. Is the bank expecting a converged platform with all these capabilities or solutions from different OEMs can be considered?	Please be guided by the RFP
1056	9	9 PROJECT TIMELINES	9	Overall Implementation period shall be 5 Months (Start Date is T0) for all solution & services	Please confirm that this timeline only includes solution implementation (IGA/MFA/IAM) and onboarding of target applications can be done phase-wise subsequently.	Please be guided by the RFP. Clarification: The 5-month Implementation Period covers full deployment, configuration, and integration of the solution, including onboarding/integration with identified target systems and applications
1057	9	9 PROJECT TIMELINES	9	Overall Implementation period shall be 5 Months (Start Date is T0) for all solution & services	Based on the current state assessment of the bank's infrastructure, can the bidder propose their own project implementation timeline?	Refer Section 9 – Project Timelines: the overall Implementation Period is 5 months from T0 for all solutions and services. Detailed phase-wise/solution-wise milestones shall be part of the Project Plan to be submitted by the bidder
1058	Appendix 1A - IDAM	CL 28 - 30 - Access review	Appendix 1A - IDAM	1) Solution must have the capability to perform access reviews on an ad hoc or event-driven basis, such as when a user changes roles. 2) Solution must have capability for a multi-step access review process so that more than one reviewer can verify the user access. 3) Solution must provide governance administration capabilities integrate tightly with the provisioning solution so that any access that is denied is immediately revoked	Kindly clarify on the access certification scope (identities and roles) and frequency.	The solution must support configurable access certification as per the bank's frequency requirements.
1059	Appendix 1A - IDAM	CL 34 - 36 - SoD	Appendix 1A - IDAM	1) Solution should be able to manage segregation of duties in applications. 2) Solution must allow users to quickly and easily create a library of Separation of Duties (SoD) policies from the entitlements and access specific to our environment. 3) Solution must support the ability to define and enforce access policies, including Separation of Duties (SoD) policies, between individual roles, between individual entitlements.	Kindly provide number of applications with existing SOD rules/policies that need to be migrated. Please clarify where bank will provide SOD rule matrix or whether bidder is expected to perform SOD rule discovery and definition	The Bank will provide the necessary assistance during the implementation
1060	Appendix 1A - IDAM	CL 47 - Virtualized Environment	Appendix 1A - IDAM	Solution must run in a virtualized application environment such as VMware	Kindly confirm whether bank will provide the required Infrastructure and hardware for deployment of IDAM solutions.	The bidder shall provide all the necessary infrastructure to meet the RFP requirements.
1061	32	7. Scope of Work : Note	7	1) The implementation of each solution, including design, installation, configuration, integration, migration, testing, and Go-Live, shall be performed by OEM. The bidder shall arrange OEM resources, coordinate implementation activities, and ensure timely project completion. 3) Roles and Responsibilities (Indicative): a. System Integrator (Bidder): Supply the proposed solutions, provide onsite L1/L2/L3 support resources, manage the project, and coordinate with OEMs. b. Solution OEM: Deploy, configure, integrate, test, commission, and migrate data/logs from existing solutions, and ensure successful implementation of the proposed solution.	Is the bidder allowed to cover implementation of all the solutions using their resources instead of employing OEM resources?	No, Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
1062	NA	Generic Request		Additional Clause: Separation of Cryptographic Trust Services and Identity Services	Enterprise Key Management and PKI solutions primarily provide cryptographic trust services, including certificate lifecycle management, cryptographic key generation, storage, rotation, revocation, digital signing, encryption, and HSM integration. In contrast, IDAM, MFA, and SSO solutions focus on identity lifecycle management, authentication, authorization, access governance, user provisioning, federation, and access control. These domains address different security objectives, operational processes, and regulatory controls. Industry standards have been specifically developed to enable interoperability between PKI, Key Management, MFA, and IAM platforms, allowing organizations to deploy best-of-breed solutions. Separation of these domains promotes vendor independence, reduces concentration risk, supports segregation of duties, and enables the Bank to select the most suitable solution in each technology area without compromising security or integration capabilities.	Please be guided by the RFP
1063	PSB_Appendix 1A Functional Specs.xlsx	Point 15		The 2FA solution should support or Integrate with cryptographic modules certified by FIPS 140-2 Level 2 & Level 3 for all cryptographic operations including the encryption of sensitive data at rest (password hashes, PINs, token records, etc.) and sensitive data in transit (server-to-browser, inter-server communication, etc.). All Agents used by the server should be compliant with the aforesaid.	Please chaange this to " The 2FA solution should provide cryptographic modules certified by FIPS 140-2 Level 2 & Level 3 for all cryptographic operations including the encryption of sensitive data at rest (password hashes, PINs, token records, etc.) and sensitive data in transit (server-to-browser, inter-server communication, etc.). All Agents used by the server should be compliant with the aforesaid. The proposed solution shall provide, through the same OEM, a comprehensive range of authentication methods including hardware tokens, software tokens, push-based authentication, FIDO2/WebAuthn, OATH-TOTP, certificate-based authentication and passwordless authentication, managed under a unified authentication platform and administrative framework"	Please be guided by the RFP
1064	PSB_Appendix 1A Functional Specs.xlsx	Point 3		The MFA authentication server must be available in hardware appliance or software form purpose built for 2FA Application by the OEM.	the clause should be changed to "The MFA authentication server shall be offered as a dedicated hardware appliance from the OEM and shall not rely solely on a software-only deployment model running on general-purpose infrastructure. The appliance shall be purpose-built, OEM-owned, OEM-supported, and designed specifically for authentication and security services, ensuring enhanced security hardening, performance predictability, operational resilience, and clear end-to-end accountability for support and maintenance".	Please be guided by the RFP
1065		A	Clause 1	Deployment scope	Kindly specify the intended deployment model for the proposed solution for Day-1 (on-premises, private cloud, India-based public cloud or hybrid) and provide the available infrastructure/compute/storage specifications, if any, for sizing the proposed solution.	SBOM/ CBOM/ AIBOM/ QBOM solution needs to be deployed based on Bidder design and compliance stated in the RFP
1066		A	Clauses 3, 47 & 110	Integration volumetrics	Kindly provide the list and estimated number of enterprise platforms/tools to be integrated, including ManageEngine product/version, vulnerability scanners, VAPT tools, bug bounty platforms, SIEM, GRC and other relevant systems, along with expected API/data exchange volumes.	Details shall be shared with the Successful bidder.
1067		SBOM/CBOM	Clauses 3, 23, 29 & 46	BOM ingestion and exchange volumetrics	Kindly provide the estimated number of SBOM/CBOM documents, applications/products, average and maximum BOM file size, expected ingestion frequency/peak rate, projected annual growth and retention period for sizing storage and processing capacity.	SBOM : 50 Critical Applications CBOM : 10 Cryptographics Critical Applications + 16 HSMs QBOM : 50 Critical Applications AI-BOM :10 AI Application Additional will be sourced on rate card.
1068		SBOM/CBOM	Clauses 4, 11, 25, 27, 28 & 44	Software/code scanning scope	Kindly provide the estimated number of target machines, applications, code repositories, container images, CI/CD pipelines and binary artifacts in scope, along with the target operating systems, package ecosystems and programming languages required for Day-1 support.	SBOM : 50 Critical Applications CBOM : 10 Cryptographics Critical Applications + 16 HSMs QBOM : 50 Critical Applications AI-BOM :10 AI Application Additional will be sourced on rate card.
1069		SBOM/CBOM	Clauses 12–20, 33, 53–61 & 78–88	Cryptographic discovery scope and volumetrics	Kindly provide the estimated count and technology-wise breakup of applications, servers, databases, middleware, APIs, PKI/certificates, HSMs, KMS, network devices, VPNs, containers/Kubernetes and cloud services that are in scope for CBOM generation/discovery.	SBOM : 50 Critical Applications CBOM : 10 Cryptographics Critical Applications + 16 HSMs QBOM : 50 Critical Applications AI-BOM :10 AI Application Additional will be sourced on rate card.
1070		SBOM/CBOM	Clauses 14, 54 & 80	Cryptographic key discovery	Kindly clarify whether cryptographic key discovery is limited to inventorying key metadata and lifecycle information.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
1071		SBOM/CBOM	Clauses 21 & 45	Continuous monitoring and intelligence sources	Kindly specify the mandatory vulnerability intelligence sources/advisories and the expected synchronization or re-correlation frequency, including whether any commercial threat/vulnerability feeds are to be integrated.	Please be guided by the RFP
1072		SBOM/CBOM	Clauses 23 & 24	Vendor portal and external exchange	Kindly provide the expected number of third-party vendors/external users and clarify the required authentication, approval workflow and expected BOM submission/exchange volumes.	Please be guided by the RFP
1073		AI-BOM	Clauses 62–77, 89–104 & 120–123	AI asset discovery scope and volumetrics	Kindly provide the estimated number and technology-wise breakup of AI/ML/GenAI/Agentic AI applications, models, datasets, repositories, vector databases and AI platforms/environments in scope, along with the expected discovery mechanism and data/update frequency.	Please be guided by the RFP
1074		AI-BOM	Clauses 74 & 120–123	AI-BOM formats and standards	Kindly specify the mandatory AI-BOM schema/standard and the AI model file formats required for Day-1.	Please be guided by the RFP
1075		QBOM/PQC	Clauses 124–138	Quantum/PQC discovery scope and volumetrics	Kindly provide the estimated asset counts and environment-wise breakup for QBOM/PQC discovery, including applications, servers, databases, APIs, PKI, certificates, HSMs, KMS, containers/Kubernetes, network devices, VPNs, IoT and cloud services, along with the mandatory Day-1 PQC assessment scope.	Please be guided by the RFP
1076		Platform	Clauses 105–119	Users, concurrency and data retention	Kindly provide the expected number of named users, concurrent users, user roles, expected data retention period, audit-log retention period and projected growth to enable accurate platform sizing.	Please refer annexure 21
1077		Platform	Clauses 114 & 115	HA/DR requirements	Kindly specify the required HA/DR architecture and target RPO/RTO, number/location of DR sites, and any mandatory replication or failover requirements.	Please refer annexure 21
1078		Platform	Clauses 110, 117, 118 & 143	Workflow, reporting and scheduling volumetrics	Kindly provide the expected number of workflows, approval paths, notifications, scheduled reports, email recipients/distribution groups and expected discovery/reporting schedules or peak execution requirements.	Please refer annexure 21
1079		Access Control	Clauses 140–142	Granular application-wise access control	Kindly provide the required role matrix and clarify whether application-wise data visibility based on configured fields requires standard RBAC only or field-level/row-level access control, along with the estimated number of roles and application-owner mappings.	Details shall be shared with the Successful bidder.
1080		Annexure - Functional Compliance (Additional Document 1: 1787133919), Sheet 'Backup Solution' - S.No. 38	Technical / Functional Compliance - Backup Solution	Clause 38 - Backup Solution: "The proposed backup solution must natively support a LAN-Free architecture for all image-level VM backups to prevent performance degradation on production networks. All raw backup data payloads must stream directly from production storage to the backup appliance/storage over a dedicated Storage Area Network (SAN/Fibre Channel/iSCSI) or dedicated storage fabric. Production Ethernet/LAN infrastructure must be completely bypassed, restricting its use strictly to minor control traffic and metadata orchestration."	Request for change as - "The solution shall provide snapshot-based backups to minimize impact on production workloads. It shall support array-integrated and hypervisor snapshots, LAN-free backup transport to reduce backup windows and production overhead."	Please be guided by the RFP
1081	111	10 EVALUATION CRITERIA	10.3 Technical Evaluation Criteria	1. Solution Understanding & Compliance (5 Marks 2. Technical Architecture & Solution Design (25 Marks) 3. Implementation & Migration Methodology (25 Marks) 4. Operations, Managed Services & SLA (10 Marks) 5. OEM Support Model & TAC Availability (5 Marks) 6. Project Management, Team & Certifications (5 Marks) 7. Sizing – IT Infrastructure (15 Marks) 8. Experience of Proposed OEMs (10 Marks)	Please confirm whether the documents mentioned in the given clause are required to be submitted along with the bid at the time of bid submission, or whether they are required to be presented/submitted during the presentation stage. Kindly clarify the requirement to ensure that all necessary documents are submitted at the appropriate stage.	Please be guided by the RFP. Technical presentation shall be part of the submitted bid
1082	136	13.2	Right to Alter quantities	The bank reserves the right, at the time of award of contract and/or during the currency of the contract, to increase or decrease the quantity of goods, licenses, subscriptions, appliances, equipment, services, implementation effort, support services, or any line item covered under the contract by up to twenty five percent (25%) of the quantities specified in the RFP/Contract, without any change in the unit prices, terms and conditions, technical specifications, delivery schedule, warranty obligations, support commitments, or any other contractual conditions.	Due to the ongoing volatility in the pricing of memory components (DRAM/RAM) and SSD/NAND, the IT infrastructure market, particularly for servers, storage systems, and AI/data-center infrastructure, is experiencing significant price fluctuations. In view of the prevailing market conditions, OEMs are currently unable to commit to price validity beyond a few weeks. We therefore request you to kindly consider discussing the matter with the respective OEMs and explore the possibility of securing the maximum possible price validity for the proposed solution. This would help the bidder mitigate the financial risk and commercial exposure arising from unforeseen fluctuations in memory and SSD prices, which are external factors beyond the bidder's reasonable control. We would appreciate your kind consideration and support in this regard	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
1083	32	Scope of Work	Note: Point 1	The implementation of each solution, including design, installation, configuration, integration, migration, testing, and Go-Live, shall be performed by OEM. The bidder shall arrange OEM resources, coordinate implementation activities, and ensure timely project completion.	We understand OEM PS is mandatory for Security Solution/Services defined in the RFP and bidder own technical resources can deploy the underlying IT infrastructure required for Security Solution deployment. We kindly request you to confirm our understanding or provide the necessary clarification on the OEM PS scope for underlying IT infra.	Please be guided by the RFP
1084	32	Scope of Work	Note: Point 6	In case of implementation delays, the bidder shall ensure seamless takeover and transition of in scope existing security solutions and services from the incumbent vendor without disruption to Bank operations at no additional cost to the bank	We understand this clause is only applicable in case of implementation delays by the bidder of current RFP and Bidder is not bound to own the SoW incase implementation delays are on Banks part. We kindly request you to confirm our understanding or provide the necessary clarification on the clause.	Please be guided by the RFP
1085	32	Scope of Work	Note: Point 6	In case of implementation delays, the bidder shall ensure seamless takeover and transition of in scope existing security solutions and services from the incumbent vendor without disruption to Bank operations at no additional cost to the bank	Kindly share the following details, as the same would be important for us to assess and gauge the expected scope of work: - Details of the existing security solutions, including the applicable license/subscription validity. - Details of the OEM support currently available for the existing security solutions. - Details of the underlying IT infrastructure, including the infrastructure model and quantity/configuration details. - Number of technical resources currently engaged in managing and supporting the security solution landscape. - Contract validity/tenure of the incumbent vendor. - Expected decommissioning date(s) of the existing security solutions and the underlying IT infrastructure. The above information will help us better understand the existing environment, assess dependencies, and accurately determine the expected scope of work and associated resource requirements.	Details shall be shared with the Successful bidder.
1086	33	Cyber Security Incident / Data Breach	Point F	All reasonable costs incurred by the Bank for investigation, containment, remediation, restoration, forensic audit, data recovery and other measures necessitated by an incident attributable to the Bidder/OEM/subcontractor shall be recoverable from the Bidder	An uncapped liability for such costs may result in an open-ended financial exposure for the Bidder, We request the Bank to kindly consider prescribing an appropriate upper cap/limit on the aggregate liability arising under this clause.	Please be guided by the RFP
1087	34	7.2 RACI	Testing, UAT & Go-Live	Bidder/OEM responsible for testing, UAT and Go-Live support.	Kindly share the mandatory solutions, features, and functionalities required to be available in the UAT environment. This will help ensure that all bidders provision a consistent and comparable UAT environment and consider the necessary infrastructure, licensing, and associated requirements while preparing their proposals. We request you to kindly provide the details of the mandatory UAT requirements for clarity and uniformity across all bidders.	All the features sought in the RFP is to be provided in the UAT
1088	61	7.5.8	Training- Activities are to be performed by Respective solution OEM (supported by bidder)	The bidder and respective OEMs shall provide comprehensive product training, knowledge transfer, and certification programs for the Bank's IT and Information Security personnel at no additional cost. All technical and product-specific training shall be delivered by OEM.	Kindly confirm whether training from the respective OEMs of the underlying infrastructure is also required as part of the scope. If applicable, we request the Bank to kindly specify the training scope, number of participants, duration, and certification requirements, if any, for each underlying infrastructure component.	Training shall cover the proposed security solutions
1089	69	7.1	Solution/Appliance Warranty, ATS and AMC. Point 5	Warranty, AMC and ATS services shall include OEM support, software updates, upgrades, patches, bug fixes, technical assistance, preventive maintenance, corrective maintenance, replacement of defective components, security updates, and all other activities required to ensure continuous and secure operation of the solution.	Kindly confirm whether Operating System (OS) and Database upgrades are also required to be considered within the scope of work.	Please be guided by the RFP
1090	72	7.11	Resource Requirement	Note: No remote access shall be provided to any resource	Many OEMs provide Technical Assistance Center (TAC) support primarily through remote assistance, and doesn't have on-site support model. Accordingly, we request the Bank to kindly consider amending the relevant clause to permit remote support by the respective OEM TAC/support teams for troubleshooting, diagnostics, and issue resolution, in accordance with the OEM's standard support model.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
1091	82	7.12.2	DR Drills	The bidder is responsible for conducting the DR Drill on a regular basis and as per the frequency decided by the bank in the presence of bank officials. Coordination with the application team, OEMs and bank's team, is the responsibility of the bidder to ensure the successful execution of the DR drill.	We strongly recommend that the Bank kindly specify the required frequency of Disaster Recovery (DR) Drills as part of the RFP requirements. Defining the DR Drill frequency will provide clarity and ensure that all bidders consider consistent requirements, resource efforts, operational activities, and associated costs while estimating the overall scope of work.	DR drill of the Security shall be on quarterly interval or as and when required by the Bank. The periodic DR Drill plan should be submitted in advance to the bank for scheduling the same in presence and approval of the bank.
1092	97	9	PROJECT TIMELINES	Overall Implementation period shall be 5 Months (Start Date is T0) for all solution & services	Due to the prevailing global supply chain constraints and extended OEM lead times, the delivery of certain products may require an additional 16–18 weeks. Accordingly, we request the Bank to consider the implementation timeline starting from the date of actual product delivery, thereby providing adequate time for installation, configuration, integration, testing, and commissioning of the proposed solution. We kindly request the Bank to consider and approve the project timeline as 9 months from T0.	Please be guided by the RFP
1093	88	7.13 IT Infrastructure	4. Supply of IT Infrastructure	Ensure servers include sufficient CPU cores, RAM, and network interface cards (NICs) to handle expected transaction volumes, data processing needs, parallel operation of Backup & Restoration (with Ransomware Protection) and Replication.	We request the Bank to kindly provide clarity on the network zones/VLANs that need to be connected to the proposed servers, including the required number of network interfaces, wherever applicable. This information will enable all bidders to provision the appropriate number and type of NICs/network ports and ensure that the proposed servers are adequately configured and ready for integration with the Bank's existing network architecture. Kindly provide the required network connectivity details to enable accurate sizing, configuration, and commercial estimation by all bidders.	Details shall be shared with the Successful bidder.
1094	212	15.21.4 Deployment & Data Retention	Retention Requirement:	Monthly Full Backup (Post Retention Period) Note: The proposed Backup and Retrieval Solution shall be sized to support the above retention policy. Upon completion of the two (2) month retention period on Backup Storage, Monthly Full Backups shall be migrated to Long-Term Storage (LTS) and retained in immutable Write Once Read Many (WORM) format for the entire contract period.	We request the Bank to kindly confirm whether a unique full backup file for each month is required to be retained on the Long-Term Storage. If yes, kindly confirm whether the Long-Term Storage should therefore be sized to accommodate 60 unique monthly full backup files, corresponding to the specified 60-month retention period. Further, we request the Bank to kindly confirm whether Synthetic Full Backup is acceptable for the Long-Term Storage requirement, as it can help optimize the storage footprint while maintaining the required backup and retention objectives. This clarification will enable all bidders to accurately size the Long-Term Storage capacity and propose an appropriate backup architecture.	The backup storage and the other infra should be sized to support the entire contract duration as per the terms defined in the RFP
1095	88	7.13 IT Infrastructure	Supply of IT Infrastructure - Point 5	Ensure proposed storage Confirm compatibility with servers, database, Backup & Restoration (with Ransomware Protection) Solution and existing infrastructure & software requirements, ensuring expansion options for future scalability.	Kindly provide the existing storage, SAN switch, backup and virtualization platform OEM/model/version details and required connectivity protocols (FC/iSCSI/NFS/SMB, etc.) for interoperability validation.	Details shall be shared with the Successful bidder.
1096	88	7.13 IT Infrastructure	Supply of IT Infrastructure	i The bidder shall supply all hardware, software, operating systems, hypervisors, firmware, appliances, licences, accessories, power cords, optics, transceivers, cables, mounting kits, documentation, and other components required for complete deployment of the proposed solution.	Kindly provide the below Details at each deployment location to enable accurate sizing and BOM preparation. - Rack Dimensions, - Complete racks will be provisioned or segregated as per available free space - power load allocated / available per rack - PDU specifications' - KVM availability	Details shall be shared with the Successful bidder.
1097	88	7.13 IT Infrastructure	Point No 2.6 DC, DR & NDR Implementation	Bidder is responsible for DC, DR & NDR implementation.	Kindly clarify the connectivity and existing Network Architecture between DC, DR and NDR.	The detailed network architecture and connectivity details shall be shared with the successful bidder during the implementation stage

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
1098	88	7.13 IT Infrastructure	Installation and Deployment - Clause 5	The Bidder shall integrate the proposed infrastructure with the Bank's existing IT ecosystem. • The integration scope shall include: • Existing network infrastructure. • Existing storage environment. • Security infrastructure. • Monitoring and management platforms. • Identity and access management systems. • Enterprise applications, wherever applicable. The Bidder shall ensure seamless interoperability and minimum disruption to existing business operations.	Kindly provide details of the existing - server, storage, SAN, network, virtualization, - Backup and database infrastructure with applicable OEM/model/version information to validate interoperability and integration requirements .	Details shall be shared with the Successful bidder.
1099	88	7.13 IT Infrastructure	Supply of IT Infrastructure - Point 5	Ensure proposed storage Confirm compatibility with servers, database, Backup & Restoration (with Ransomware Protection) Solution and existing infrastructure & software requirements, ensuring expansion options for future scalability.	Kindly provide the - existing storage, -SAN switch, -backup and virtualization platform OEM/model/version details -required connectivity protocols (FC/iSCSI/NFS/SMB, etc.) These details are very crucial for interoperability validation.	Details shall be shared with the Successful bidder.
1100	92	7.13 IT Infrastructure	Clause 10	Bank would provide the following IT Hardware components, sizing of which shall be provided by bidder in their technical proposal: 1. TOR Switch 2 .Racks	As per the RFP Bank will provide the Rack and ToR Switches along with Power Connectivity at designated Racks . Kindly confirm on below Points : - ToR Switches Bandwidth (1G/10G) Copper / Fiber along with available Ports . - Management Switches will be provided by Bank . - optics, transceivers, patch cords and rack accessories will be provided by Bank.	Bank will provide the ToR switches and Rack. Xxx
1101	94	7.14.Other In-Scope services	Point No 13	The hosting Space and Power arrangement shall be provided by the Bank at DC and DRC. However, the bidder is required to factor in the requisite racks in order to successfully operationalize the proposed hardware	Basis RFP inputs, We Understand that basis sizing shared by bidder, Bank will provide the Racks along with UPS power and TOR Switches. We kindly request you to confirm our understanding or provide the necessary clarification on the clause.	Bank will provide the ToR switches and Rack. Xxx
1102	1 - Technical Compliances	Primary Storage	5	Proposed storage solution should be offered with minimum 2 controllers with minimum 256 GB DRAM Cache memory on the entire storage Solution. The solution should scale to at least 512GB Cache memory by adding additional controller.	Kindly Change the Clause to : Proposed storage solution should be offered with minimum 2 controllers with minimum 128 GB DRAM Cache memory on the entire storage Solution. The solution should scale to at least 256GB Cache memory by adding additional controller. Explanation: Cache ask should be Reduced as cache of 64GB or less per controller (128GB total) is enough as the latest CPUs, high-speed memory, and Gen 5 PCIe cards deliver the required performance efficiently. Modern storage controllers optimize cache usage, and industry benchmarks confirm that asked performance can be achieved with lower memory. This reduction not only meets technical needs but also decreases hardware, power, and cooling costs, resulting in a lower TCO for the solution	Please be guided by the RFP
1103	2 - Technical Compliances	Backup Solution	16	The proposed disk-based storage/appliance must interoperate with industry-leading server platforms and operating systems, and must ingest backup data over a secure, API-based disk-to- disk (D2D) connection.	Kindly Change the Clause to : The proposed disk-based storage/appliance must interoperate with industry-leading server platforms and operating systems, and must ingest backup data using standard Data protocols such as FC, ISCI, NFS, S3 Explanation: This specific ask qualifies only specific backup appliance not any target storage as enterprise storage do not support data ingestion using API rather leverage protocols such as FC, ISCI, NFS , S3.	Please be guided by the RFP
1104	3 - Technical Compliances	Backup Solution	25	The Proposed Appliance/Backup Storage must provide verification of the Metadata and actual data of the file with strong Checksum Mechanism	Kindly Change the Clause to :The Proposed Appliance/Backup Solution must provide verification of the Metadata and actual data of the file with strong Checksum Mechanism Explanation: Proposed ask should be from Solution instead of storage as any storage does not offer file-level checksum reporting for backup files. This is typically a function of the backup software (e.g., Commvault, Veeam) that stores backups on storage.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
1105	4 - Technical Compliances	Long Term Storage	4	Additional Point Request	Kindly Change the Clause to : Long Term Storage should support WORM (Write Once, Read Many) capability to have Data Immutability. Explanation: We recommend implementing WORM (Write Once, Read Many) capability for long-term backup storage to ensure data is protected against accidental deletion and ransomware attacks. Additionally, WORM functionality is required to comply with regulatory guidelines for banking institutions. Since backup storage is expected to provide WORM capability, long-term backup storage should also comply with this requirement to maintain robust data protection .	Please be guided by the RFP
1106	5 - Technical Compliances	1.Primary Storage 2.Backup Storage 3.Long Term Storage		New Point request	Kindly Change the Clause to : The proposed storage systems (for all 3 storage requirements), should have launch dates within past 3 years Explanations: We recommend qualifying storage systems with a launch date within the past three years. This approach ensures a better return on investment and reliable long-term support for a period of 7 to 10 years, as required by the bank. Some OEMs are currently offering systems that are over six years old and lack a clear roadmap or support commitment, which poses a risk to long-term operational stability and longevity.	Please be guided by the RFP
1107	1 - Technical Compliances	Primary Storage	3	The proposed array should be an unified storage which support both SAN & NAS	The proposed array should be an unified / SAN / NAS storage which support both either SAN & OR NAS OR Both based on the proposed solution	Please be guided by the RFP
1108			7	The proposed array should support FC, iSCSI , (NFS v4.0 or above)/ (SMB 3.1 or above), NVMe/TCP, NVMe/FC from day one.	The proposed array should support FC, iSCSI / (NFS v4.0 or above) / (SMB 3.1 or above) / NVMe/TCP, NVMe/FC from day one.	Please be guided by the RFP
1109			8	The proposed array should be configured with at least 8 x 32Gbps & 8 x 10Gbps optical front-end ports & Proposed storage should support 100GbE backend.	The proposed array should be configured with at least 8 x 32Gbps & 8 x 10Gbps optical front-end ports & Proposed storage should support 100GbE backend.	Please be guided by the RFP
1110	1 - Technical Compliances	Backup Solution	38	The proposed solution must support LAN-Free (SAN/FC/iSCSI) transport for image-level VM backups on supported block-storage hypervisor platforms, and must ensure that on all other platforms backup data traverses a dedicated backup network/fabric isolated from production LAN traffic, such that no backup payload transits the production Ethernet infrastructure.	Justification: SAN transport carries its own risk. Direct SAN Access requires production LUNs to be presented to the backup proxy; a misconfigured Windows proxy can initialise/sign a production LUN. Many banks deliberately restrict SAN transport for this reason, which is worth mentioning if the Bank asks why the clause should be softened.	Please be guided by the RFP
1111	1 - Technical Compliances	Backup Solution	40	Backup storage/Appliance capacity expansion - whether by adding disks, adding an enclosure, or adding scale-out nodes - must be non-disruptive, and no additional storage-side licence shall be required to consume the expanded capacity where the backup software's protected-capacity licence already covers the data being protected.'	Is the backup software required to be licensed strictly on a capacity basis, or is an instance/workload-based licence (per VM, per physical server, per database instance, per NAS TB) also acceptable? Justification : Veeam offers Node based licensing with unlimited capacity. While capacity-based licensing is still prevalent in the industry, we have seen a gradual shift to other licensing models which are more flexible and makes procuring the software more cost effective like Instance or Node based model. By giving option for Node -based licensing your overall TCO would reduce dramatically.	Please be guided by the RFP
1112	97	Timeline	Sec. 9	Review is to be conducted annually, from year 2 onwards (Post go-live of respective solutions) on a yearly basis- within 15 days of bank notifying the bidder to initiate the assessment.	Kindly clarify the expected scope and deliverable of this annual Architecture Assessment Review (e.g., is it a formal third-party security architecture audit, or an internal bidder/OEM review), and confirm whether the associated cost/resourcing should be factored into the Facility Management BOM or quoted separately.	Please be guided by the RFP Refer Section 11.2 – OEM Services Cost (Payment Milestones – Architecture Assessment).
1113	3	Anti-DDoS	Compliance Sheet - Anti-DDoSSr. 2	Sr.2: System should have 5 Gbps of clean/legitimate throughput which can scale upto 10 Gbps on the same H/w. System should support more then 20 MPPS. System should be factored on clean/legitimate license throughput. Sr.74/77: DDoS Cloud Mitigation via ISP clean pipe with sinkholing/scrubbing.	With reference to Sr. 2, which specifies 5 Gbps clean throughput scalable up to 10 Gbps on an on-premises appliance, and Sr. 74/77, which specifies DDoS cloud mitigation through ISP clean-pipe/scrubbing and sinkholing, kindly clarify whether the solution is required to be strictly on-premises appliance-based, or whether a hybrid deployment comprising an on-premises DDoS appliance along with ISP/cloud-based scrubbing for large-scale volumetric attacks is acceptable. Further, if cloud/ISP-based scrubbing is permitted, kindly confirm whether the scrubbing infrastructure and associated traffic processing must be located within India to comply with Sr. 46, which states that “no data/information shall leave the Indian sub-continent.”	On Premise DDoS mitigation solution should send signal to ISP for volumetric attack. Scrubbing of DDoS traffic should be done in backbone of upstream service provider (ISP) when DDoS attack become volumetric and chokes last mile. On Premise DDoS mitigation solution should send cloud signal to scrubber in backbone of Service Provider for handoff of traffic. Yes, On Premise DDoS mitigation device should send Cloud signal to ISP/OEM scrubber
1114	5		Compliance Sheet - Anti-DDoS, Sr. 74	Protection from all attacks like UDP Flooding, ICMP Flooding, Spoofed packet Flooding,SYN Floods, fragmented packet attacks, Ping od Death, Smurf, GET/POST floods, Zero Day DDoS etc.		Please be guided by the RFP.
1115	5		Compliance Sheet - Anti-DDoS, Sr. 77	Anti-DDoS Solution should enable and provide features like null routing, sinkholing, scrubbing, IP masking, DNS name server protection from NXDomain attacks, with uptime SLA of 99.99%		Please be guided by the RFP.

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
1116	4	Anti-DDoS	Compliance Sheet - Anti-DDoS, Sr. 34	Support minimum 20 K SSL CPS on TLS 1.3 with selective decryption and TLS fingerprinting. Also System should have ability to scale SSL CPS capacity via external SSL appliance retaining proposed DDoS appliance (CPS: Connections Per Second)	Since SSL Orchestrator with Packet Broker is separately proposed as a dedicated line item for SSL decryption/inspection, kindly clarify whether the Anti-DDoS appliance is expected to perform independent SSL decryption, or whether it may consume already-decrypted traffic from the SSL Orchestrator to avoid duplicate SSL-inspection licensing/hardware.	The proposed DDoS hardware should have an inbuilt SSL/TLS decryption and inspection capability to effectively detect and mitigate SSL/TLS-based DDoS attacks.
1117	3	Anti-DDoS	Compliance Sheet - Anti-DDoS, Sr. 2	System should have 5 Gbps of clean/legitimate throughput.	Kindly share the Bank's current/expected peak internet-facing bandwidth (DC & DR) to enable right-sizing of the Anti-DDoS appliance, since sizing/volumetric baselines (referenced in RFP Annexure 21) have not been made available with the bid documents.	Please be guided by the RFP
1118	14	DNS Protection	Compliance Sheet - IPAM, Sr. 36	The IPAM solution component must perform host discovery using a variety of methods not limited to ping, Address Resolution Protocol (ARP) via SNMP protocol for 3000 number of L3 and L2 devices	Kindly confirm whether the 3000-device count covers DC + DR only, or the Bank's entire network including all branches/offices, as this materially affects IPAM/DDI sizing and licensing.	Please be guided by the RFP
1119	13	Web Gateway	Compliance Sheet - Web Gateway, Sr. 1	Sr.1: The solution should be on premise appliance based and must Provide Web Proxy, Caching, Web based Reputation filtering, URL filtering, Antivirus, Antimalware, Enterprise Data protection control with minimum 1500 templates inbuilt with English Language support, Application Visibility & control, Detail Reporting and Management. . Load balancing should be inbuilt in the appliance or should work with Bank's existing load balancer with no additional cost.		Please be guided by the RFP
1120	14		Compliance Sheet - Web Gateway, Sr. 34	Sr.34: Solution should support natively integrate with Data protection tool offered in the RFP and must be able provide predefined template including region & Industry specific, India IT Act , Aadhaar No, PCI-DSS, Data Theft Indicator templates, templates to identify Disgruntled employees, templates to identify suspected emails to self, Templates for Cyberbullying and self destructive patterns, passwords files and suspicious behavior that is indicative of malicious activity, suspicious User Activity like detects data sent at an unusual time and must support multiple languages not only limited to English and Hindi etc.	Kindly confirm whether Hindi-language DLP/content-inspection templates are a mandatory Day-1 requirement, or a desirable enhancement, since Sr.1 specifies only English support as the baseline.	Please be guided by the RFP
1121	21	Zero-Day/Anti-APT	Compliance Sheet - Zero-Day Attack Protection, Sr. 29	Sr.29: The proposed solution should be able to run at least 50 parallel sandboxes for analysis of payload and on premise customized sandbox solution should have the capability to allow manual submission of suspicious files for analysis	Kindly share the Bank's expected daily file-submission volume / email & web traffic EPS baseline to validate that the specified sandbox concurrency and storage sizing are adequate, since no volumetric baseline has been provided.	Please refer Addendum 1 for the revised clause.
1122	21		Compliance Sheet - Zero-Day Attack Protection, Sr. 32	Sr.32: Sandbox appliance should have redundant power supply, 2 TB or more storage capacity (or as per OEM recommendatin meeting the requirement mentioned in the RFP) with dedicated management port		Please refer Addendum 1 for the revised clause.
1123	24	ZTNA	Compliance Sheet - ZTNA, Sr. 26	Solution should support extensive coverage with in-built Data types like Aadhar card, PII, etc with different File Types etc. Solution should support extensive coverage with 100+ in-built Data types with minimum 200 File Types.	This data-classification/DLP capability appears to overlap with the separately procured DLP solution's content-detection requirements. Kindly clarify the functional boundary between ZTNA-embedded DLP policy enforcement and the standalone DLP solution to avoid duplicate licensing of the same capability under two BOM line items.	Please refer Addendum 1 for the revised clause.
1124	25	DLP	Compliance Sheet - DLP, Sr. 4	All endpoints including desktops (Windows and non-Windows) and VPN laptops of the Bank should be monitored / managed through a single On-premises hosted orchestrator / management Server and console only.	Kindly share the total endpoint count (desktops, laptops, VDI), server count, and mailbox count (for Email DLP) at DC/DR/branches, since this baseline is required for accurate DLP agent licensing and is not included in the RFP as shared.	Relevant details shall be shared with the succesfull bidder
1125	36	WAF	Compliance Sheet - WAF, Sr. 12	Solution must support dedicated 5 Gbps of WAF throughput (HTTP/HTTPS) with public documentary/evidence-based proof of throughput.	Kindly share the Bank's expected peak concurrent transaction volume / API call volume across internet-banking, mobile-banking and other web-facing applications, to validate whether 5 Gbps dedicated throughput is the correct sizing baseline.	Please be guided by the RFP
1126	47	MFA	Compliance Sheet - MFA, Sr. 11.8	The authentication agents must support platforms including 'Epic Hyperdrive'.	Epic Hyperdrive' is a specialized US healthcare EHR access platform and does not appear applicable to a banking IT environment. Kindly confirm whether this entry is intended, or is a template/drafting artifact that may be disregarded for the purpose of technical compliance scoring.	Please refer Addendum 1 for the revised clause.
1127	57	DAM	Compliance Sheet - DAM, Sr. 7	Solution should monitor, detect and prevent breaches/anomalies for MySQL, MS SQL, PostgreSQL, Oracle DB, Maria DB and 'any other DBs'.	Kindly share the Bank's actual database landscape (database engines, versions, and approximate instance count across Core Banking/Finacle, satellite applications, DC & DR) to enable accurate DAM agent-based licensing and OEM compatibility assessment.	Relevant details shall be shared with the succesfull bidder
1128	69	DNS Security (Cloud)	Compliance Sheet - DNS Security, Sr. 44	20 Domains of PSB are to be considered for the purpose of sizing.	Kindly confirm whether this domain count of 20 includes only registered root/second-level domains, or also encompasses subdomains, for the purpose of accurate BOM sizing and licensing.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
1129		General / Sizing	RFP ToC Ref. 15.21	Annexure 21: Sizing/Volumetrics, Data Retention and Current Infrastructure (Existing & Envisaged Stack, Existing IT Security Solution Details, Current IT Assets, Deployment & Data Retention) is referenced in the RFP Table of Contents.	Kindly share the completed/populated Annexure 21 (or equivalent sizing datasheet covering user counts, endpoint counts, branch count, transaction volumes, mailbox count, database inventory, existing security stack, and data-retention requirements), as this baseline is essential for accurate technical solutioning and BOM sizing across nearly all 21 solution categories, and has not been included with the documents shared for this RFP.	Please be guided by the RFP
1130	48	Functional Requirements	7.2.1.2. Privilege Identity Management (PIM)	The Bank intends to upgrade its existing Privileged Identity Management (PIM) solution to enhance control and security over privileged access across its critical IT infrastructure and enterprise applications. The upgraded solution must provide comprehensive privileged account management, including secure credential storage (password vaulting), real-time session monitoring, granular access control, and detailed audit trails to meet regulatory and internal compliance requirements. The objective is to enforce least privilege access, enhance visibility, and ensure accountability of privileged activities across the Bank's IT ecosystem, helping to mitigate insider threats and prevent misuse of elevated privileges	The Bank intends to upgrade its existing PIM solution. Kindly confirm whether bidders are permitted to propose a new OEM solution, including migration/replacement of the existing PIM/PAM solution, provided that the proposed solution meets all the technical, functional, integration and security requirements specified in the RFP.	Please refer Addendum 1 for the revised clause.
1131	ATC 116	11.1 Product (Software) Cost	Payment Terms	Product License Cost On successful delivery of the licenses which would be considered delivered once the software (with OOTB features) is made available for view and review of the bank on the proposed hardware.	We request the Bank to kindly release 90% of the Product License Cost upon successful delivery of the licenses, once the software with OOTB features is made available for view and review by the Bank on the proposed hardware. Justification The Product Licenses are procured from the OEM, and the OEM requires substantial payment in advance for provisioning and activation of the licenses. The vendor is therefore required to make significant upfront financial commitments before the licenses can be delivered and made available to the Bank. Releasing 90% of the Product License Cost upon successful delivery will help align the payment milestone with the OEM's commercial terms and support timely license provisioning and project execution.	Please be guided by the RFP
1132	116	Payment Terms	11.1 Product (Software) Cost	On successful UAT Signoff of the respective product	We request the Bank to kindly release the remaining 10% of the Product License Cost upon successful UAT Sign-off of the respective product. Justification This milestone links the balance payment directly to the successful completion and acceptance of UAT. It provides a clear and mutually agreed payment milestone while ensuring that the final payment is released only after successful validation and sign-off of the respective product by the Bank.	Please be guided by the RFP
1133	116	Payment Terms	11.1 Product (Software) Cost	Subscription Cost (One time license Cost) On successful delivery of the Licenses which would be considered delivered once the software (with OOTB features) is made available for view and review of the bank on the proposed hardware.	We request the Bank to kindly release 90% of the Subscription Cost (One-time License Cost) upon successful delivery of the Licenses, once the software with OOTB features is made available for view and review by the Bank on the proposed hardware. Justifiaction The subscription/licenses involve upfront OEM commitments and provisioning costs that need to be incurred by the vendor prior to delivery. Release of 90% of the cost upon successful delivery will help align the payment milestone with the OEM's commercial terms and ensure timely provisioning and deployment of the licenses.	Please be guided by the RFP
1134	116	Payment Terms	11.1 Product (Software) Cost	On successful UAT Signoff of the respective product	We request the Bank to kindly release the remaining 10% of the Subscription Cost (One-time License Cost) upon successful UAT Sign-off of the respective product. Justification This milestone ensures that the balance payment is linked to the successful completion and acceptance of UAT. It provides a clear and mutually agreed payment structure, while ensuring that the final 10% payment is released only after successful validation and sign-off of the respective product by the Bank.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
1135	117	Payment Terms	11.3 Hardware Cost	Appliance Cost On successful Delivery of the Appliance which would be considered delivered once the solution (with OOTB features) is made available for view and review of the bank.	We request the Bank to kindly release 90% of the Appliance Cost upon successful delivery of the Appliance, Justification The Appliance is procured from the OEM, and the OEM requires substantial payment in advance to initiate the procurement and delivery process. The vendor is therefore required to make significant upfront financial commitments before delivery. Releasing 90% of the Appliance Cost upon successful delivery will help align the payment milestone with the OEM's commercial terms, support timely procurement and deployment, and ensure uninterrupted project execution without impacting the Bank's interests.	Please be guided by the RFP
1136	117	Payment Terms	11.3 Hardware Cost	On successful UAT Signoff of the respective product	We request the Bank to kindly release the remaining 10% of the Appliance Cost upon successful UAT Sign-off of the respective product. Justification The proposed milestone will ensure that the final payment is linked to the successful completion and acceptance of UAT. This will provide a clear and mutually agreed payment milestone while ensuring that the vendor receives the balance payment upon successful validation and sign-off of the solution by the Bank.	Please be guided by the RFP
1137	117	Payment Terms	11.3 Hardware Cost	Hardware Cost (Other than Appliances) Delivery (power on) of hardware and submission of invoice with Proof of Delivery and other documents of the hardware supplied. Bank may at its discretion verify the details before releasing the payment (This verification, if required, shall be completed within 1 month of delivery of the hardware on the bank's premises).	We request the Bank to kindly release 90% of the Hardware Cost upon successful delivery (power-on) of the hardware at the Bank's premises, along with submission of the required invoice, Proof of Delivery, and other applicable documents. Justification Hardware procurement involves significant upfront financial commitments towards OEMs and suppliers, including procurement, manufacturing, logistics, and delivery costs. Release of 90% of the Hardware Cost upon delivery will help align the payment milestone with the vendor's upfront procurement obligations and ensure timely availability and deployment of the required hardware, without impacting the Bank's right to verify the supplied hardware and supporting documents.	Please be guided by the RFP
1138	117	Payment Terms	11.3 Hardware Cost	On successful installation of proposed solutions on the hardware - 50% of the sought product/solutions	We request the Bank to kindly release the remaining 10% of the Hardware Cost upon successful installation of the proposed solutions on the hardware. Justification Successful installation demonstrates that the supplied hardware has been appropriately deployed and is ready for solution implementation. Releasing the remaining 10% at this milestone provides a clear payment linkage to successful installation and supports the vendor in meeting the associated deployment and implementation commitments.	Please be guided by the RFP
1139	118	Payment Terms	11.5 Facility Management (FM) Cost:	FM Manpower Cost Submission of SLA report and Submission of attendance record/register of Onsite resources on Quarterly basis	We request the Bank to kindly modify the payment terms from quarterly in arrears to monthly in advance for FM Manpower Cost. Justification FM manpower involves continuous deployment of dedicated onsite resources and recurring costs such as salaries, statutory benefits, and other employee-related expenses. These costs are incurred by the vendor on a monthly basis irrespective of the quarterly billing cycle. Monthly advance payment will help align the payment cycle with the vendor's recurring manpower obligations, ensure timely salary and statutory payments, and support uninterrupted availability of resources throughout the contract period.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
1140	ATC 135 & ATC 142	Liquidated Damages	12.2 & 13.19	Installation & Implementation Delay in installation, configuration, integration, testing, commissioning, migration, implementation, Go-Live, or any project milestone approved by the Bank., the Bank shall, without prejudice to its other remedies under the Contract, deduct from the Contract Price, as liquidated damages, a sum equivalent to 1% per week or part thereof of the respective Product Cost subject to maximum deduction of 10% of the total contract value, until actual delivery and implementation as per related clauses mentioned in RFP. ATC Pg no. 142 Clause no. 13.19 LD For Supply & Delivery If the bidder fails to deliver any or all of the products and/or systems and/or services solutions within the time period(s) specified in the Delivery Schedule or installation, the Bank shall, without prejudice to its other remedies under the Contract, deduct from the Contract Price, as liquidated damages, a sum equivalent to 0.5 percent per week or part thereof of Contract Price subject to maximum deduction of 10% of the total contract value, until actual delivery, installation or performance as per related clauses mentioned in RFP. Once the maximum deduction is reached, the Bank may consider termination of the Contract at its discretion. In the event of Bank agreeing to extend the date of delivery at the request of successful bidder(s), it is a condition precedent that the validity of Bank guarantee shall be extended by further period as required by Bank immediately. Failure to do so will be treated as breach of contract.	We request the Bank to kindly combine the Supply & Delivery and Installation & Implementation LD provisions into a single clause. We further request that the LD be applicable at 0.5% per week or part thereof, subject to a maximum deduction of 5% of the total Contract Value. Justification Since Supply & Delivery and Installation & Implementation are interdependent activities forming part of the overall project delivery, having separate LD provisions may result in multiple LDs being imposed for delays arising from the same underlying event. A single consolidated LD clause with a rate of 0.5% per week or part thereof, capped at 5% of the total Contract Value, would provide a fair, reasonable, and proportionate mechanism for managing project delays. This approach will also avoid duplication or overlapping LDs for the same delay while continuing to adequately protect the Bank's interests.	Please be guided by the RFP
1141	74	AI Gateway	Appendix 1A Functional Specification	The Proposed solution's all components (on-prem HW or Software if any) should connect to management plane within India for any kind of monitoring/health checks of components. The proposed solution should have CSA STAR, SOC 2, CIS, ISO 27001, ISO 27017, ISO 27018 certification and must be a part of Microsoft Active Protections Program (MAPP)	Requesting bank to revise the certification requirements by removing CSA STAR, CIS, ISO 27017, ISO 27018, and the requirement for Microsoft Active Protections Program (MAPP) membership, and instead include ISO 42001 (Artificial Intelligence Management System). SOC 2 and ISO 27001 already provide comprehensive assurance of an organization's information security governance and operational controls, while the other certifications largely represent overlapping or domain-specific requirements. Further, MAPP is a vendor-specific program rather than an internationally recognized security certification. Considering the requirement pertains to "AI Securtiy" solution, inclusion of ISO 42001 would better align the RFP with globally accepted best practices for responsible AI governance while encouraging wider participation from qualified solution providers without compromising security.	Please refer Addendum 1 for the revised clause.
1142	149	14.2 APPENDIX 1B: Technical	Compliance Sheet DDoS S. No. 2	System should have 5 Gbps of clean/legitimate throughput which can scale upto 10 Gbps on the same H/w. System should support more then 20 MPPS. System should be factored on clean/legitimate license throughput. Suggetsed Clause: System should have 5 Gbps of clean/legitimate throughput which can scale upto 10 Gbps on the same H/w. Mitigation Throughput 10Gbps from day1 and scale to 20Gbps. System should support more then 12 MPPS. System should be factored on clean/legitimate license throughput.	If we consider an average packet size of 64 bytes (minimum packet size), 9 Mpps is equivalent to approximately 5 Gbps of throughput handling. Based on our experience deploying our solution at major Public Sector Banks, including leading/top-tier banks, 12–14 Mpps is more than sufficient to cater to a 10 Gbps clean traffic environment. Additionally, the mitigation throughput should also be considered to ensure effective mitigation of attacks in both ingress and egress traffic directions.	Please be guided by the RFP
1143	149	14.2 APPENDIX 1B: Technical	Compliance Sheet DDoS S. No. 73	The proposed solution shall support PQC readiness and migration capability, including identification of quantum-vulnerable cryptographic algorithms and support for PQC-enabled or quantum-resistant cryptographic standards, wherever applicable to the solution. Suggested Clause: The proposed solution shall support TLS 1.3 with hardware acceleration for encrypted traffic protection.	The technical specifications requested for TLS inspection already cover full SSL/TLS inspection as an in-built capability of the DDoS mitigation hardware. Therefore, specifying the latest cipher suites and TLS 1.3 with hardware-based acceleration should be considered as a technology-neutral requirement to enable wider OEM participation, rather than mandating any specific requirement.	PQC readiness is intended to cover applicable cryptographic functions, communication interfaces, authentication mechanisms, APIs, certificates and other security components of the proposed solution and support migration to quantum-resistant standards. DDoS vendor need to submit their roadmap or approach on PQC

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
1144	149	14.2 APPENDIX 1B: Technical	Compliance Sheet WAF S. No. 12	The proposed solution must support dedicated 5 Gbps of WAF throughput (HTTP/HTTPS). The bidder must provide evidence of throughput through publicly available documents /evidence based document supporting the same which needs to be submitted along with the proposal and same needs to showcased if asked by bank during Presentation & UAT (Undertaking from the OEM is not accepted in this case). Suggested Clause: The proposed solution must support dedicated 5 Gbps of WAF throughput (HTTP/HTTPS) or 25 Gbps of L7 throughput. The bidder must provide evidence of throughput through publicly available documents (Undertaking from the OEM is also accepted in this case).	Not every OEM publishes WAF throughput as a standard performance parameter. However, leading vendors in the WAF and API Protection space do publish Layer-7 throughput capabilities as part of their product specifications. Therefore, vendors that can demonstrate equivalent L7/WAF and API protection performance should also be considered to ensure wider OEM participation and a technology-neutral evaluation process.	Please be guided by the RFP
1145	149	14.2 APPENDIX 1B: Technical	Compliance Sheet WAF S. No. 81	The client component (JavaScript) should be downloaded from the same domain as the application (first party). It is not allowed to use external locations to upload the script. Suggested Clause: The client component (JavaScript) should be downloaded from the same domain as the application (first party).	Every OEM may use its own architecture and methodology to achieve the required functionality. Therefore, the evaluation should be functionality- and outcome-based rather than implementation-method-based. The specified clause should not be restrictive, provided that the proposed solution meets the intended security and functional requirements.	Please be guided by the RFP
1146	149	14.2 APPENDIX 1B: Technical	Compliance Sheet WAF S. No. 90	The proposed WAF solution must support high availability in both Layer 2 and Layer 3 deployments. It must include either an inbuilt bypass switch or be supplied with an external bypass switch to ensure uninterrupted traffic flow during maintenance or failure. Suggested Clause: The proposed WAF solution must support high availability in both Layer 2 and Layer 3 deployments.	Fail-open/Bypass is not relevant in the context of a stateful security solution, as maintaining session and connection state is essential to its intended operation. If fail-open functionality is considered a mandatory requirement, it should be applied consistently across the complete network security architecture and applicable network devices. Specifying fail-open only for a single stateful solution does not provide meaningful operational value and may unnecessarily restrict wider OEM participation.	Please refer Addendum 1 for the revised clause.
1147	149	14.2 APPENDIX 1B: Technical	Compliance Sheet WAF S. No. 92	The solution must have bypass segments to ensure that fail open in case of hardware failure Suggested Clause: The solution must support high availability	Fail-open/Bypass is not relevant in the context of a stateful security solution, as maintaining session and connection state is essential to its intended operation. If fail-open functionality is considered a mandatory requirement, it should be applied consistently across the complete network security architecture and applicable network devices. Specifying fail-open only for a single stateful solution does not provide meaningful operational value and may unnecessarily restrict wider OEM participation.	Please be guided by the RFP
1148	105	Eligibility Criteria/Clause	19	The proposed OEM solution/product for Privilege Identity/Access Management should have been successfully implemented in at least 2 BFSI in India, out of which at least one (1) BFSI Client should have a deployment covering more than 1,500 privileged users We recommend the Bank to consider the below points that will help the bank for the OEM Eligibility Criteria: A) We recommend the clause to be added as- The Proposed OEM Solution/ Product for Privilege Identity/Access Management should have been successfully implemented and Running for More than 2 Years. (This Clause will help the Bank to understand that the Client is using the Solution till Date) B) We recommend the Clause to be added as- The Proposed OEM solution/product for Privilege Identity/Access Management should have been successfully implemented in at least 3 BFSI in India, out of which minimum (2) BFSI Client should have a deployment covering more than 1,500 privileged users	We recommend the Bank to consider the below points that will help the bank for the OEM Eligibility Criteria: A) We recommend the clause to be added as- The Proposed OEM Solution/ Product for Privilege Identity/Access Management should have been successfully implemented and Running for More than 2 Years. (This Clause will help the Bank to understand that the Client is using the Solution till Date) B) We recommend the Clause to be added as- The Proposed OEM solution/product for Privilege Identity/Access Management should have been successfully implemented in at least 3 BFSI in India, out of which minimum (2) BFSI Client should have a deployment covering more than 1,500 privileged users	Please be guided by the RFP
1149	Generic	Eligibility Criteria			We recommend if the Bank can add the Below Points for the PIM/PAM Eligibility Criteria: A) Proposed PIM/PAM Solution should have the Presence in India for more than 10 Years B) Proposed PIM/PAM OEM by the Bidder should have the Annual Average Turover for last three Years should be more than INR 60Cr. C) The offered PAM OEM Solution must be certified for Common Criteria Certificate EAL 2+ and supporting certificate document should be submitted during the bid submission.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
1150	88-92	7.13 (9)	IT Infrastructure	Bidder's need to provide the Sizing on the bank's provided configuration mentioned in Appendix 2: Masked Bill of Material and Appendix 3: IT Infrastructure Virtual to Physical mapping. Bidders need to provide sizing, which is required for DC, DR and Non-Production environment.	Request the Bank to share the Appendix 2 (Masked BoM) and Appendix 3 (V2P Mapping) Excel files along with the pre-bid response so that bidders can perform accurate infrastructure sizing. Are these files published on GeM / Bank's website, or will they be shared separately?	Bidder can download the excel files from the bank's portal https://punjabandsind.bank.in/module/tender-list
1151	88	7.13	IT Infrastructure — Supply	Ensure servers include sufficient CPU cores, RAM, and NICs to handle expected transaction volumes, data processing needs, parallel operation of Backup & Restoration (with Ransomware Protection) and Replication.	To enable accurate compute sizing, please share: (a) Current and expected peak Events Per Second (EPS) / Transactions Per Second (TPS) across all proposed security solutions. (b) Current log generation rate (GB/day) from all log sources. (c) Expected data growth rate (%) per annum over the 5-year contract period. (d) Peak concurrent user sessions expected for solutions like IDAM, MFA, PIM, ZTNA, and Web Gateway.	Please be guided by the RFP
1152	92	7.13	IT Infrastructure — Bank-provided components	Bank would provide the following IT Hardware components: 1. TOR Switch, 2. Racks.	(a) Please confirm the number of racks available/allocated for the proposed IT Security infrastructure at DC, DR, and NDR respectively. (b) What is the per-rack unit (RU) capacity, available power (kW per rack), and cooling capacity (BTU) at each site? (c) What TOR switch model/OEM is proposed, and how many 1G/10G/25G ports will be available for the security infrastructure? (d) Will the Bank provide SAN switches and FC ports, or should the bidder factor these into the proposal?	Please be guided by the RFP- Bank would provide the following IT Hardware components (As per 7.13 IT Infrastructure Point 10), sizing of which shall be provided by bidder in their technical proposal:
1153	88	7.13	IT Infrastructure — Installation & Deployment	The Bidder/OEM shall perform complete installation and deployment of the proposed infrastructure at the Bank's Data Centre (DC), Disaster Recovery (DR) site, Near DR site, or any other designated locations.	(a) Please provide the physical addresses and access procedures for DC (Mumbai), DR (Noida), and NDR sites. (b) Are the DC and DR Bank-owned facilities or co-located data centres? If co-located, are there any restrictions on vendor access, working hours, or equipment movement? (c) What is the process and lead time for obtaining physical access passes for bidder/OEM engineers at each site?	The details shall be shared with the successful bidder
1154	203	15.21	Sizing/Volumetrics — Non-Production Environment	For appliance-based solutions, the bidder shall design and propose an appropriate non-production environment. For VM-based solutions, the non-production environment shall be sized at a minimum of 10% of the Production (DC) environment.	(a) For appliance-based solutions (Anti-DDoS, SSL Orchestrator, WAF, Web Gateway, etc.), should the non-production environment be a separate physical appliance, a virtual instance, or can it be a lower-specification model? (b) Should the non-production environment be provisioned at DC only, or at both DC and DR? (c) Is the non-production environment expected to support UAT, SIT, development, and training simultaneously, or sequentially?	Please be guided by the RFP
1155	89	7.13	IT Infrastructure — Storage Sizing	Storage installation and configuration, RAID and storage pool configuration, Logical volume creation, Storage provisioning, SAN zoning and host mapping, Multipathing configuration, Storage performance optimization.	(a) Please share the existing storage OEM, model, type (SAN/NAS/Object), and protocol (FC/iSCSI/NFS/CIFS) deployed at DC and DR. (b) What is the available usable capacity on the existing storage, and will the Bank allocate storage from the existing pool, or should the bidder propose dedicated storge? (c) What SAN fabric (switch OEM, model, port count, available ports) is deployed at DC and DR? (d) What IOPS and throughput targets should the bidder design for — especially for high-write solutions like DAM, DLP, HIPS, and packet capture?	Details shall be shared with the Successful bidder.
1156	88	7.13	IT Infrastructure — Backup & Restoration	The bidder/OEM is responsible for supplying, designing, sizing and configuring the Backup Software and Hardware (with Ransomware Protection). The backup solution configuration should comply with bank's policy for secure data backup.	(a) The RFP mentions backup infrastructure is 'Provided and maintained by bank' (Annexure 21.4, S.No. 22). However, Section 7.13 states the bidder is responsible for backup software & hardware. Please clarify — should the bidder propose a separate dedicated backup solution, or will the Bank's existing centralized backup infrastructure be used? (b) If the Bank's existing backup is to be used, please share: Backup OEM/product name, available capacity, supported protocols, and backup window timings. (c) Please share the Bank's data backup policy document referenced in the RFP.	Please refer Addendum 1 for the revised clause.
1157	27	7	Scope of Work	The Bank is undertaking a comprehensive enhancement across its Data Centre (Mumbai), NDC, Disaster Recovery Centre (Noida), NDR, Cloud environments, and branch/office network.	(a) Please clarify the role, scope, and physical location of NDC (Near Data Centre) and NDR (Near DR). Are these co-located with DC/DR or at separate physical sites? (b) What is the network connectivity (bandwidth, latency, link type — MPLS/Dark Fibre/Leased Line) between DC-DR, DC-NDC, and DR-NDR? (c) For solutions requiring HA at both DC and DR, should the NDC and NDR also have any deployment, or are they out of scope for the proposed security solutions?	Long term storage will be hosted at NDC and NDR.

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
1158	207-212	15.21.4	Deployment & Data Retention	All solutions require HA (N+N Active-Active) deployment at DC and DR.	For solutions deployed in N+N Active-Active mode at both DC and DR: (a) Should each site be sized to independently handle 100% of the production load (i.e., full-capacity failover), or is a shared-load model (e.g., 50%-50%) acceptable? (b) For Active-Active deployments, is the traffic distribution mechanism (GSLB/DNS-based routing) provided by the Bank, or should the bidder factor this into the solution? (c) For inline appliances (Anti-DDoS, SSL Orchestrator, WAF), will the Bank provide the necessary network path changes (asymmetric routing handling, return traffic routing) during DC-DR failover?	(a) Please be guided by the RFP, (b) Please be guided by the RFP, refer section 7.13 IT Infrastructure (c) Please be guided by the RFP
1159	128	12.1	DR Instance Availability — SLA	RPO: 15 minutes, RTO: 60 minutes. 100% Compliance (Instance-wise).	(a) For achieving RPO of 15 minutes and RTO of 60 minutes across all 21+ security solutions, please confirm whether dedicated replication links between DC and DR will be provided by the Bank for security infrastructure, or should the bidder size and propose the bandwidth requirement for replication? (b) What is the existing DR replication mechanism/tool used by the Bank (e.g., storage-level replication, application-level, database-level)? (c) For appliance-based solutions with local configurations and policies, is policy synchronization via the management plane considered sufficient for RPO compliance, or is data-level replication also mandated?	(a) Bank will provide replication bandwidth (b) Bank to provide (c) Data level replication is mandated.
1160	82	7.12.2	DR Drill	The bidder is responsible for conducting the DR Drill on a regular basis (quarterly or as required). Ensure DC & DR are exact replica of each other in every manner.	(a) During quarterly DR drills, will the Bank perform a full site failover (all applications and security infrastructure simultaneously), or will DR drills for security solutions be conducted independently? (b) What is the expected duration of each DR drill? (c) Will the Bank provide a maintenance window for planned DR drills, or should solutions support zero-downtime DR switchover? (d) Is a 'swing DR' model (where DR becomes primary post-drill) in scope, or is fallback to DC always expected after drill completion?	Details shall be shared with the Successful bidder.
1161	89	7.13	Network Infrastructure	Switch configuration, VLAN configuration, Routing configuration, High Availability configuration, Port configuration, Access control configuration.	(a) Please provide the existing network architecture diagram (L2/L3 topology) at DC and DR including firewall zones (DMZ, MZ, Server Zone, Management Zone), VLAN structure, and available switch port capacity (1G/10G/25G/40G). (b) How many available network ports (copper/fibre) are there at DC and DR for connecting proposed security appliances? (c) Are dedicated management network ports / out-of-band management VLAN available for the proposed security infrastructure?	Details shall be shared with the Successful bidder.
1162	208	15.21.4	DNS Protection — Deployment Zones	DHCP will be used for internal client networks, not in the DMZ. Recursive DNS will be hosted in DMZ. DHCP and IPAM services will be deployed in MZ.	(a) Please confirm the number of distinct network zones/segments (DMZ, Internet Zone, Server Zone, Management Zone, Branch Zone, Cloud Zone) where security appliances/agents need to be deployed. (b) Will the Bank provide necessary firewall rule openings between zones for communication between security solution components (management servers, agents, collectors, log forwarders)? (c) What is the current DNS infrastructure (authoritative and recursive) — OEM, model, and query volume (queries per second)?	Please be guided by the RFP
1163	206	15.21.3	Current IT Assets — Branch Network	Routers & Switches: 7200.	(a) Are the 7200 routers and switches at branches within scope for log forwarding to the proposed security solutions? (b) What is the WAN link bandwidth at each branch (MPLS/SD-WAN/Internet), and what is the average available bandwidth for security log transmission? (c) Will the DLP endpoint agents and HIPS agents on branch desktops communicate directly with the centralized management servers at DC/DR, or is there a local proxy/collector at each branch?	Please be guided by the RFP
1164	88	7.13	IT Infrastructure — Stack Deployment	Stack Deployment and Commissioning including virtualization if required.	(a) Please share the existing virtualization platform (VMware vSphere / Microsoft Hyper-V / Red Hat KVM / OpenStack) and version deployed at DC and DR. (b) Should the bidder propose a separate/dedicated hypervisor cluster for the security solutions, or will the Bank provide virtualization resources (CPU, RAM, storage) from the existing virtual environment? (c) If the Bank provides the virtualization platform, please confirm the available compute capacity (vCPU, vRAM) that can be allocated to the proposed security solutions. (d) Are container-based deployments (Docker/Kubernetes) supported in the Bank's environment?	Details shall be shared with the Successful bidder. Bidder to right size and design the solution and accordingly propose the platform as well sa the infrastructre

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
1165	63-65	7.6	Cloud Service Provider Responsibilities	The requirements apply to all cloud-hosted solutions proposed under IaaS, PaaS, or SaaS delivery models.	(a) Does the Bank have an existing empaneled Cloud Service Provider (CSP)? If yes, please share the CSP name, region, and available services. (b) For solutions with cloud/hybrid deployment options (CASB, DNS Security Services, ZTNA, AI Security, SBOM/CBOM), does the Bank prefer on-premises deployment, or is cloud/hybrid deployment acceptable? (c) If cloud deployment is acceptable, should the cloud infrastructure (IaaS) cost be included in the bidder's commercial proposal, or will the Bank procure cloud resources separately? (d) What is the Bank's current cloud connectivity mechanism (Direct Connect / ExpressRoute / VPN) from DC and DR to cloud environments?	a) Bidder to propose the solution and proposed deployment b) Bidder based on their solution design propose & factor the architecture complying with the terms of the RFP c) Bidder based on their solution design propose & factor the architecture complying with the terms of the RFP d) Bidder based on their solution design propose & factor the architecture complying with the terms of the RFP
1166	205	15.21.2	Existing IT Security Solution Details	13 existing security solutions listed with OEM Make and Model.	For the 13 existing solutions listed in Annexure 21.2: (a) Please share the current hardware/appliance specifications (CPU, RAM, storage, throughput, form factor) for each solution at DC and DR. (b) What are the current license quantities and license expiry dates for each solution? (c) Can the existing hardware (post-migration) be repurposed for non-production/test environments? (d) What is the current data/log volume stored in each solution (in GB/TB)? (e) Please share the existing solution architecture diagrams (logical and physical) for each of the 13 solutions.	Please be guided by the RFP, relevant details will be shared and discussed with the successful bidder
1167	94	7.14.2	Transition Management	The bidder shall take over and maintain operations of the bank's existing solutions starting 01.05.2027 and continue doing so until the new proposed solution goes live.	(a) Will the incumbent vendor provide a formal knowledge transfer/handover period before 01.05.2027? If yes, what is the expected duration? (b) Who will bear the ATS/AMC cost of existing security solutions during the transition period (01.05.2027 until new solution go-live)? The RFP states the Bank shall not be liable for ATS/AMC costs, but the existing solutions need to remain operational. (c) Will the Bank provide access to existing OEM support portals, TAC credentials, and license entitlements for the transition period? (d) Are there any existing L1/L2/L3 resources from the incumbent vendor who may be available for absorption?	Bank will assist, however end to end responsibility lies with the bidder.
1168	52-54	7.5.1	Migration	The bidder shall be responsible for migrating all applicable data, configurations, and operational components from the existing solution to the proposed platform.	(a) For each of the 13 existing solutions, what is the volume of historical data/logs (in TB) that needs to be migrated to the proposed platform? (b) Is there a requirement to maintain access to historical data from the old platform during the parallel run period? If yes, for how long? (c) For configuration/policy migration (e.g., DLP policies, WAF rules, HIPS baselines, PIM privileged accounts), will the existing vendor/OEM provide export tools or APIs for data extraction? (d) What is the acceptable downtime window for cutover from existing to proposed solutions for each security layer?	Details will be shared with the successful bidder
1169	212	15.21.4	Backup & Retention	Retention: Daily Incremental Backup (1 Week), Weekly Full Backup (2 Weeks), Monthly Full Backup (2 Months), Monthly Full Backup post retention — Long-Term Storage (LTS) for entire contract duration in WORM format.	(a) The Long-Term Storage (LTS) requirement is for the 'entire duration of the contract' (~7 years including extension) in immutable WORM format. Please confirm whether the LTS infrastructure (hardware + software) should be proposed by the bidder, or will the Bank provision LTS from its existing infrastructure. (b) What is the estimated aggregate daily data generation (in GB) across all 21 proposed security solutions for backup sizing? (c) Should the LTS be on-premises (tape/object storage) or can cloud-based archival (e.g., S3 Glacier equivalent with data residency in India) be proposed? (d) Is deduplication and compression acceptable for backup and LTS storage sizing?	(a) (b) (c)
1170	207	15.21.4	Data Retention — Primary Storage	All solutions: 1 Month (Logs and Data Storage on Appliance / Primary Storage).	(a) The 1-month retention on primary storage — does this refer to hot/online searchable data, or can it include warm/nearline storage? (b) After the 1-month primary retention period, are the logs automatically moved to the Bank's centralized backup, or should each solution have its own archival mechanism? (c) For appliance-based solutions with limited local storage, if the 1-month data exceeds the appliance's native storage capacity, should the bidder provision external storage (NAS/SAN) attached to the appliance?	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
1171	127	12.1	Performance Measurements — Hardware Utilization	Daily peak utilization of CPU, memory (RAM), network interfaces (NIC), storage I/O exceeds 75% for more than 5 consecutive minutes — each subsequent block of 5 minutes treated as separate incident. 100% Compliance required.	The 75% CPU/RAM utilization threshold with a 5-minute measurement window is extremely stringent for security appliances that inherently handle burst/spike traffic patterns (e.g., Anti-DDoS during attack mitigation, SSL Orchestrator during peak SSL traffic, WAF during web traffic surges). (a) Request the Bank to consider increasing the threshold to 85% for appliance-based solutions, with burst tolerance up to 90% for periods not exceeding 15 consecutive minutes. (b) Alternatively, request that the utilization threshold be measured on a 15-minute average rather than a 5-minute snapshot, aligned with industry monitoring standards. (c) Please clarify whether the threshold applies to individual CPU cores or the aggregate CPU utilization of the appliance.	(a) Please be guided by the RFP (b) Please be guided by the RFP (c) Threshold applies to the CPU utilization of the appliance. Bidder to submit regular reports to the bank
1172	127-128	12.1	Performance Measurements — Storage Utilization	Daily peak storage utilization exceeds 80% for more than 5 consecutive minutes — treated as separate incident.	(a) Does the 80% storage utilization threshold apply to: individual appliance local storage, centralized SAN/NAS storage provisioned for solutions, or both? (b) For appliance-based solutions where the OEM has optimized the local storage and the solution operates efficiently at >80% utilization (e.g., circular logging), request the Bank to consider an exception for appliance local storage with a threshold of 90%. (c) For primary storage (SAN/NAS), is the 80% threshold on raw capacity or usable capacity after RAID overhead?	(a) Utilization percentage applies to both appliance and proposed storage. Bidder to submit reports to the bank at regular intervals. (b) Please be guided by the RFP (c) 80% threshold on raw capcity
1173	124	12.1	Availability SLA	All solutions: 99.99% availability. For every 0.01% reduction, penalty equivalent to 1% of the Monthly Maintenance Cost (MMC).	99.99% availability allows only ~4.3 minutes of downtime per month. (a) Please confirm whether planned/scheduled downtime (approved by the Bank) for firmware upgrades, OS patching, signature updates, and hardware maintenance is excluded from the availability calculation. (b) For solutions deployed in HA (Active-Active), if one node of the HA pair fails but the surviving node continues to serve traffic without service interruption, is this classified as downtime? (c) For appliance-based solutions, OEM-recommended firmware upgrades may require a brief service restart (typically 2-5 minutes per node in HA). Please confirm whether rolling upgrades (one node at a time) with momentary failover will be excluded from downtime calculation.	(a) Please be guided by the RFP, refer Section 12.1 Clause 12 (b) Availability continues to be measured for each solution and any individual component, per Annexure 21/Section 12.1. Failure of a redundant node/component, even where the surviving node/component maintains service without functional or performance degradation, shall be tracked and penalized under Incident Response & Resolution Compliance (per the applicable Criticality Table timelines), rather than being excluded from measurement. Any failure of redundant node/ component shall be considered as a critical incident (c) Details of service level mapping and scheduled downtime will be discussed with the successful bidder. Bidder to align the solution as per the requirements specified in the RFP.
1174	206	15.21.3	Current IT Assets	Servers: 2500, Databases: 300, Applications: 200, Desktops: 12000, Routers & Switches: 7200. Note: Count is tentative.	For accurate infrastructure sizing of agent-based solutions (HIPS, DLP, DAM, IDAM, MFA), please provide: (a) Breakdown of 2500 servers by OS type (Windows/Linux/AIX/Solaris) and version. (b) Breakdown of 300 databases by type (Oracle/MS SQL/MySQL/PostgreSQL/DB2) and version. (c) Breakdown of 12000 desktops by OS type (Windows 10/11, Mac) and location (DC/DR/branches/HO). (d) Number of servers hosted on physical vs. virtual infrastructure. (e) Number of servers/VMs in the Bank's cloud/VPC environment.	Details will be shared with the successful bidder
1175	210	15.21.4	HIPS — Volumetrics	3000 VMs/Servers scalable to 4500 VMs/Server.	For HIPS covering 3000 VMs/Servers (scalable to 4500): (a) What is the breakdown of 3000 by OS type (Windows Server / Linux / AIX / Solaris)? (b) Are all 3000 servers/VMs at DC/DR, or are some at branches or cloud? (c) For application change control, please share the approximate number of applications and executables (binaries) per server that need to be baselined. (d) Will the Bank provide a central software distribution mechanism (SCCM/Ansible) for HIPS agent deployment, or should the bidder factor in a separate deployment mechanism?	Details will be shared with the successful bidder
1176	209	15.21.4	DAM — Volumetrics	150 Application Databases at DC and 150 Application Databases at DR.	For DAM covering 300 databases (150 DC + 150 DR): (a) What is the breakdown by database type (Oracle/MS SQL/MySQL/PostgreSQL/DB2/others)? (b) What is the average query volume (queries per second) across all monitored databases? (c) Are database connections primarily via local access, application-layer queries, or both? (d) What is the average database size and the number of privileged database users/accounts?	Details will be shared with the successful bidder

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
1177	69	7.10	Warranty, ATS and AMC	The proposed solution, hardware/appliances and software shall include a comprehensive warranty for a period of three (3) years. Bidder needs to provide the comprehensive ATS & AMC separately for Year 4 and Year 5.	(a) For hardware appliances with a standard OEM warranty of 1 year (extendable to 3 years at additional cost), should the 3-year warranty extension cost be included within the appliance/hardware unit price, or quoted as a separate line item? (b) For software-only solutions deployed on Bank-provided virtual infrastructure, does the 3-year warranty apply to the software license only, or also to the underlying OS and database? (c) For Year 4 and Year 5, should the AMC for hardware and ATS for software be quoted as a combined line item or separate line items per solution?	(a) Refer Clause 7.10 (Solution/Appliance Warranty, ATS and AMC, the quoted price shall be inclusive of 3 year warranty. (b) Please be guided by the RFP. Refer Clause 7.10 (Solution/Appliance Warranty, ATS and AMC), Point 5 The bidder is responsible for right-sizing and supplying all software, including OS and database licenses, required for the proposed solution (c) Bidder to fill BoM as per the format provided.
1178	97	8	Contract Period — End of Sales / End of Support	The bidder must ensure that any equipment supplied should not have reached or announced end of sales as on the date of supply or end of support for at least duration of the contract (including 2-year extension).	The total contract duration is Implementation (5 months) + Support (60 months) + 2-year extension = approximately 87 months (~7.25 years). (a) Should the proposed hardware platform have at least 87 months of remaining OEM support life from the date of delivery, or from the date of Go-Live? (b) If during the contract period, the OEM announces end-of-sale (but not end-of-support) for the supplied model, will the Bank require hardware replacement, or is continued OEM support sufficient? (c) For software/subscription-based solutions, does the end-of-support clause apply to the specific version deployed, or to the product family?	Please be guided by the RFP, Refer Section 8.
1179	120	12.1	SLA — Hardware Replacement	If any critical component becomes non-functional, the bidder and OEM shall, within four (4) hours, either repair, replace, or provide a standby replacement at no additional cost. The bidder shall maintain adequate inventory of spare and standby components.	(a) For the 4-hour hardware replacement SLA, should the bidder maintain spare inventory at both DC (Mumbai) and DR (Noida), or is a centralized spare depot acceptable? (b) For specialized/high-value security appliances (e.g., Anti-DDoS, SSL Orchestrator, WAF hardware appliances), maintaining a cold standby at each site significantly increases project cost. Will the Bank accept an OEM next-business-day replacement with a temporary workaround (e.g., traffic bypass) as an alternative for non-HA-impacting component failures? (c) Please clarify whether 'critical component' means the entire appliance or individual components (PSU, fan, hard disk, memory module).	Please be guided by the RFP
1180	114	10.4	Commercial Evaluation — Hardware Cost	The Bidder shall be solely responsible for sizing the IT Infrastructure. If the Bank observes that the proposed sizing is inadequate, the Bidder shall revise the sizing and update the Masked BoM accordingly.	(a) If the bidder proposes an infrastructure sizing that is technically validated during evaluation but needs augmentation during the contract period due to organic growth (new applications, new branches, regulatory changes), will such growth-related augmentation be treated as additional procurement at contracted rates, or will it be at the bidder's cost? (b) The RFP states the Bank reserves the right to increase/decrease quantities by up to 25% (Section 13.2). Does this 25% variation clause apply to infrastructure hardware (servers, storage, network) as well, or only to software licenses and manpower?	(a) Please be guided by the RFP Refer annexure 21 and Sectio 7.13. Clarification: Organic growth (new applications, branches, regulatory changes) falls within the bidder's sizing responsibility, which explicitly requires accounting for projected growth over the entire contract period. Augmentation necessitated by inadequate sizing or failure to account for such growth shall be at the bidder's own cost, per Section 7.13. This is distinct from Bank-initiated quantity increases under Section 13.2, which are at contracted rates. (b) Please be guided by the RFP Refer Section 13.2
1181	66	7.8	Delivery, Installation & Commissioning	Delivery, installation, configuration, integration, testing, commissioning, and operationalization shall be completed within the timelines specified — overall 5 months.	(a) What is the expected lead time for infrastructure delivery to the Bank's DC/DR sites after Purchase Order acceptance? Global supply chain lead times for specialized security appliances can be 8-12 weeks. Request the Bank to confirm whether the 5-month implementation timeline starts from T0 (PO acceptance) or from the date of hardware delivery at site. (b) Will the Bank provide customs clearance and logistics support for imported hardware, or is this entirely the bidder's responsibility? (c) Are there any specific 'Make in India' hardware preferences or restrictions for the proposed infrastructure?	(a) Please be guided by the RFP. Refer Section 9 (Project Timelines). The overall implementation period is five (5) months from T0, and T0 is defined as the date of acceptance of the Purchase Order (b) Please be guided by the RFP. (c) Please be guided by the RFP, refer the "Make in India" clause and Annexure 7 (Minimum Local Content Certification)
1182	93	7.14.1	Other Scope Activity	The hosting Space and Power arrangement shall be provided by the Bank at DC and DRC. However, the bidder is required to factor in the requisite racks.	(a) What is the maximum power availability (in kW) per rack that the Bank can provide at DC and DR? (b) Is redundant power (A+B feed) available at both sites? (c) What type of power connectors are available (C13/C19/C14/C20)? (d) Is the Bank's DC/DR facility Uptime Institute Tier-III or Tier-IV certified? (e) What is the maximum heat dissipation (BTU/hour) per rack that the cooling infrastructure can support?	Details will be shared with the successful bidder

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
1183	97	9	Project Timelines	Overall Implementation period shall be 5 Months (Start Date is T0) for all solutions & services.	The RFP requires 21 security solutions + IT infrastructure to be implemented within 5 months at both DC and DR in HA mode. (a) Is the Bank open to a phased implementation approach where solutions are grouped by priority/dependency and implemented in waves within the 5-month window? (b) Can the Bank share the priority/sequence of solutions for implementation? (c) Will the Bank provide concurrent access to DC and DR for parallel deployment, or should implementation be sequential (DC first, then DR)? (d) For infrastructure procurement (servers, storage, appliances), is the Bank willing to issue a Letter of Intent (LOI) prior to PO to enable early procurement and reduce delivery lead time impact on the 5-month timeline?	(a) Integration shall be phased and based on the approved implementation plan within the defined timelines. (b) The Bank will identify priority systems during SRS stage. Bidder to design the deployment plan. (c) Please be guided by the RFP
1184	76	7.12	Facilities Management — IPv6	Proposed solution should be compatible with IPv6 scheme, and there shall be no functional or performance impact on security monitoring due to switch over to IPv6 schema.	(a) Has the Bank initiated or planned the migration to IPv6? If yes, what is the expected timeline? (b) Is the current DC/DR infrastructure running on IPv4-only, dual-stack (IPv4+IPv6), or a mix? (c) Should the proposed security appliances and infrastructure be sized for dual-stack (IPv4+IPv6) traffic from Day 1, or is IPv4-only sufficient with IPv6 readiness as a future capability?	Details will be shared with the successful bidder
1185	Page no 206 & 39			Point no 4 on Page 206 & 5 on page no 39	Kinldy confirm if NAC solution is in scope and if yes, kindly sahre the details of NAC solution, make model, OEM details number of applaince etc	Please be guided by the RFP for the scope, any additional details will be shared with the successful bidder
1186	Page no 51			Point no 9	Kinldy confirm if IPS/IDS is in scope and if yes, kindly share the details of IPS/IDS, make model, OEM details number of applaince etc	Please be guided by the RFP for the scope, any additional details will be shared with the successful bidder
1187	Page no 120			Point no 16	Kindly confirm if Core and perimeter firewalls are in scope and if Yes, kindly share the details of Core and perimeter firewall, make model, OEM details number of applaince etc	Please be guided by the RFP for the scope, any additional details will be shared with the successful bidder
1188	Page no 40			7.3.2	Kinldy confirm if end point security is in scope and if yes, kindly share the details of end point security solution make model, OEM details number of applaince etc and number of end points for same	Please be guided by the RFP for the scope, any additional details will be shared with the successful bidder
1189	47			7.3.5.1 Management Layer Security Identity & Access Management Solution	The RFP specifies 12,000 users scalable to 16,000 users. Please provide the user categorization across employees, contractors, outsourced staff, privileged users, service accounts, and any other identity types expected to be governed through the IDAM solution.	Details will be shared with the successful bidder
1190	47			7.3.5.1 Management Layer Security Identity & Access Management Solution	Please confirm whether the scope is limited to internal workforce identities only or if partner, vendor, B2B, and customer identities are also expected to be managed through the proposed IAM platform.	Please be guided by the RFP
1191	47			7.3.5.1 Management Layer Security Identity & Access Management Solution	Please provide details of the authoritative source(s) for user identity lifecycle management (HRMS, Active Directory, Oracle HCM) and the expected integration architecture	Details will be shared with the successful bidder
1192	203			15.21 Annexure 21: 15.21.3 Current IT assets	Annexure 21 references approximately 200 applications. Please confirm scope for IAM integration: Number of applications to be onboarded during implementation. Number of applications expected in subsequent phases. Critical applications identified for Phase 1 onboarding.	Details will be shared with the successful bidder
1193	203			15.21 Annexure 21: 15.21.3 Current IT assets	Kindly confirm the number of applications requiring: 1.Provisioning/deprovisioning 2. SSO 3. Only Password synchronization Access certification Role-based access controls.	Details will be shared with the successful bidder
1194	47			7.3.5.1 Management Layer Security Identity & Access Management Solution	Please clarify the scope of Access Certification campaigns: 1. User Access Reviews 2. Privileged Access Reviews 3. Application Owner Reviews 4. SoD Reviews. What is the expected certification frequency and estimated review population?	Please be guided by the RFP
1195	48			7.3.5.1 Management Layer Security Identity & Access Management Solution	The RFP includes both Identity & Access Management (IDAM) and Privileged Identity Management (PIM/PAM) as separate solution components. Kindly clarify whether the scope of the IDAM solution is limited to identity lifecycle management, governance etc, or whether it is also expected to include privileged access use cases like privileged access request workflows, JIT access, password vaulting, session management etc.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
1196				7.3.5.1 Management Layer Security Identity & Access Management Solution	Please confirm whether migration is required from any existing IAM solution and provide current platform details. Existing PAM (ARCON) is mentioned, however IAM product details are not provided.	Please be guided by the RFP
1197	40			7.3.2.2 - Data Loss Prevention	Kindly provide details of the existing DLP deployment, including current OEM/version, deployed modules, endpoint coverage, policy count, annual incident volume and known operational challenges. Please share the requested existing-environment details to enable accurate migration, sizing and policy-transition planning.	Please be guided by the RFP for the scope, any additional details will be shared with the successful bidder
1198	40			7.3.2.2 - Data Loss Prevention	Please confirm whether the proposed DLP must cover endpoint, network, email, web, USB/removable media and SaaS channels, and identify any additional channels in scope. Please publish the definitive list of mandatory DLP channels and corresponding user/device volumes.	Please be guided by the RFP, relevant details will be shared and discussed with the successful bidder
1199	40			7.3.2.2 - Data Loss Prevention	Please confirm the Microsoft 365 workloads to be protected, including Exchange Online, SharePoint Online, OneDrive and Teams, and whether API-based and inline enforcement are required. Please specify workload-wise coverage, enforcement mode and licensing quantities.	Relevant details shall be shared with the succesfull bidder
1200	40			7.3.2.2 - Data Loss Prevention	Kindly share the existing DLP policies, custom dictionaries, exact-data-match datasets, regex patterns and exception workflows that must be migrated. Please provide the migration inventory and clarify whether migration of all existing policies and incidents is mandatory.	Relevant details shall be shared with the succesfull bidder
1201	40			7.3.2.2 - Data Loss Prevention	Please clarify whether OCR-based inspection of images and scanned documents is mandatory and provide estimated daily document volume and supported languages. Please define OCR scope, languages, throughput and accuracy expectations for sizing.	Please be guided by the RFP
1202	40			7.3.2.2 - Data Loss Prevention	Please confirm whether discovery and remediation of sensitive data across file shares, NAS, endpoints, databases and cloud repositories are included in the DLP scope. Please identify repositories, approximate data volumes, scan frequency and required remediation actions.	Please be guided by the RFP
1203	41			7.3.2.2 / 7.3.2 - DLP and Information/Digital Rights Management	Kindly share the Bank-approved data classification policy, label taxonomy, classification levels and handling rules to be implemented. Please provide the classification policy and approved label-to-control matrix before requirement finalization.	Relevant details shall be shared with the succesfull bidder
1204	41			7.3.2.2 / 7.3.2 - DLP and Information/Digital Rights Management	Please confirm whether any classification or sensitivity labels are currently deployed in Microsoft Purview or another platform, and whether they must be retained or migrated. Please publish the current platform, label inventory, adoption levels and migration expectations.	Relevant details shall be shared with the succesfull bidder
1205	41			7.3.2.2 / 7.3.2 - DLP and Information/Digital Rights Management	Please clarify whether classification is required through manual labelling, automated content inspection, user recommendations, or a hybrid approach. Please define mandatory classification methods for each information channel and repository.	Please be guided by the RFP
1206	41			7.3.2.2 / 7.3.2 - DLP and Information/Digital Rights Management	Please provide the expected count and definitions of sensitive information types, custom classifiers, dictionaries, fingerprints and exact-data-match datasets. Please provide the classification-rule inventory and representative sample patterns for sizing and effort estimation.	The detailed inventory and definitions of Bank-specific sensitive information shall be shared with the successful bidder during the SRS stage, subject to the Bank's security and confidentiality requirements with the successful bidder
1207	41			7.3.2.2 / 7.3.2 - DLP and Information/Digital Rights Management	Please confirm whether classification labels must drive enforcement across DLP, DRM, CASB, email, collaboration platforms and AI Security. Please publish the required label inheritance, interoperability and enforcement workflow across in-scope solutions.	Details of the Bank-specific classification criteria and categories will be shared with the successful bidder during the SRS stage, in accordance with the Bank's security requirements. The bidder shall accordingly provision and design the proposed solution to support the Bank's classification requirements
1208	41			7.3.2.2 / 7.3.2 - DLP and Information/Digital Rights Management	Please confirm whether multilingual classification is required for English, Hindi, Punjabi or other languages, including OCR and unstructured-content classification. Please specify languages, document types, expected accuracy and test corpus for acceptance.	Please be guided by the RFP
1209	41			7.3.2 - Information/Digital Rights Management	Kindly provide details of the existing BlackBerry Workspaces deployment, including version, user base, protected content volume, integrations and content to be migrated. Please provide the existing DRM inventory and define the mandatory migration scope.	Relevant details shall be shared with the succesfull bidder
1210	41			7.3.2 - Information/Digital Rights Management	Please confirm whether integration with Microsoft 365, Microsoft Purview sensitivity labels, Exchange, SharePoint, OneDrive and Teams is required. Please identify mandatory integrations and define whether native label-based protection must be preserved.	Relevant details shall be shared with the succesfull bidder
1211	41			7.3.2 - Information/Digital Rights Management	Please define mandatory rights controls, including view, edit, copy, print, screen capture, forwarding, offline access, expiry, watermarking and revocation. Please publish the minimum rights-control matrix by data classification level.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
1212	41			7.3.2 - Information/Digital Rights Management	Please clarify external-sharing scenarios and estimated numbers of external users, vendors, auditors and regulators requiring protected access. Please provide user categories, authentication methods and licensing quantities for external recipients.	Please be guided by the RFP
1213	41			7.3.2 - Information/Digital Rights Management	Please confirm whether persistent protection must remain enforceable after files are downloaded, copied to removable media or shared outside the Bank network. Please clarify offline enforcement, revocation behaviour and supported file formats.	Please be guided by the RFP
1214	41			7.3.2 - Information/Digital Rights Management	Please provide the estimated number of administrators/policy creators, protected users and monthly protected documents/emails for licensing and sizing. Please publish authoritative volumetrics and annual growth assumptions.	Please be guided by the RFP
1215	40			7.3.2.1 - Cloud Access Security Broker	Kindly provide the Bank's current cloud and SaaS application inventory, including Microsoft 365, Azure, AWS, GCP and other sanctioned services. Please publish the in-scope cloud services, tenants, subscriptions/accounts and user population.	Please be guided by the RFP
1216	40			7.3.2.1 - Cloud Access Security Broker	Please confirm whether CASB is required in API mode, forward/reverse proxy mode, log-discovery mode, or a combination of these deployment modes. Please define the mandatory operating modes and use cases for each cloud service.	The bidder shall propose, design, size and factor the complete solution architecture based on its proposed solution, ensuring full compliance with all requirements, specifications, performance, security and other terms of the RFP. Any components, capacity or resources required to meet the RFP requirements shall be included in the bidder's scope
1217	40			7.3.2.1 - Cloud Access Security Broker	The RFP specifies 50 cloud users scalable to 100. Please confirm whether this represents the complete CASB user estate or only an initial use case. Please confirm final Day-1 and scalable licensing quantities, including administrators and service accounts.	The specified 50 cloud users represents the Day-1 requirement, scalable up to 100 users during the contract period. The bidder shall design and size the complete CASB solution to support the scalable requirement and shall factor all required licenses, including administrators, service accounts and other technical accounts, as applicable to the proposed solution
1218	40			7.3.2.1 - Cloud Access Security Broker	Please clarify whether Shadow IT discovery must consume logs from the existing/proposed Secure Web Gateway, firewalls and endpoint agents. Please identify mandatory log sources, retention and discovery coverage.	Relevant details shall be shared with the succesfull bidder
1219	40			7.3.2.1 - Cloud Access Security Broker	Please confirm whether inline upload/download controls and SaaS-to-SaaS DLP enforcement are required, including quarantine and remediation workflows. Please define mandatory enforcement channels and remediation actions.	Please be guided by the RFP
1220	40			7.3.2.1 - Cloud Access Security Broker	Please confirm whether CASB must discover and control public Generative AI applications and integrate with the proposed AI Security platform. Please define the division of scope and required policy integration between CASB and AI Security.	The bidder shall propose, design, size and factor the complete solution architecture based on its proposed solution, ensuring full compliance with all requirements, specifications, performance, security and other terms of the RFP. Any components, capacity or resources required to meet the RFP requirements shall be included in the bidder's scope
1221	45			7.3.4.3 - Centralized Key Management Solution	Kindly provide details of the existing HSM estate, including make, model, quantity, firmware, partitions and current integrations. Please publish the HSM inventory and supported integration interfaces for KMS design.	Please be guided by the RFP
1222	45			7.3.4.3 - Centralized Key Management Solution	Please provide the inventory and estimated count of cryptographic keys to be onboarded, categorized by application, key type, algorithm and environment. Please share Day-1 key volumes, annual growth and migration expectations.	Please be guided by the RFP
1223	45			7.3.4.3 - Centralized Key Management Solution	Please identify all applications, databases, storage platforms, security tools and cloud services that must integrate with the centralized KMS. Please publish the integration inventory, protocols and responsible application owners.	Please be guided by the RFP
1224	45			7.3.4.3 - Centralized Key Management Solution	Please confirm whether KMIP support is mandatory and specify the required KMIP version and any proprietary interfaces that must be supported. Please define protocol/version requirements and acceptance criteria for interoperability.	Please be guided by the RFP
1225	45			7.3.4.3 - Centralized Key Management Solution	Please clarify whether the scope includes generation and management of data-encryption keys, application keys, tokenization keys, TLS keys and code-signing keys. Please publish the definitive key classes and lifecycle operations in scope.	Please be guided by the RFP
1226	45			7.3.4.3 - Centralized Key Management Solution	Please define requirements for key backup, escrow, archival, destruction and secure DC-DR synchronization, including RPO and RTO. Please specify key-recovery controls, DR test scenarios and audit requirements.	Please be guided by the RFP
1227	46			7.3.4.4 - Certificate Lifecycle Management	Kindly provide the approximate current certificate inventory by certificate type, issuing CA, environment and ownership. Please publish Day-1 certificate volumes, annual growth and discovery scope for sizing.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
1228	46			7.3.4.4 - Certificate Lifecycle Management	Please share the existing PKI architecture, CA hierarchy and integrations with Microsoft AD CS, HSMs, public CAs and application platforms. Please provide current-state PKI and certificate-enrolment architecture.	Relevant details shall be shared with the succesfull bidder
1229	46			7.3.4.4 - Certificate Lifecycle Management	Please identify the servers, network/security devices, applications, APIs, containers, Kubernetes clusters and cloud services requiring certificate discovery. Please publish asset counts and mandatory discovery methods for each technology class.	Relevant details shall be shared with the succesfull bidder
1230	46			7.3.4.4 - Certificate Lifecycle Management	Please confirm whether automated issuance and renewal through ACME, SCEP, EST and vendor-specific APIs are mandatory, and identify target systems. Please define mandatory protocols, integrations and workflow volumes.	Relevant details shall be shared with the succesfull bidder
1231	46			7.3.4.4 - Certificate Lifecycle Management	Please clarify whether code-signing, document-signing, client-authentication and machine-identity certificates are included in scope. Please provide the complete list of certificate/use-case categories and associated volumes.	Please be guided by the RFP
1232	46			7.3.4.4 - Certificate Lifecycle Management	Please confirm whether CLM must identify weak algorithms and quantum-vulnerable certificates and support migration to hybrid/PQC certificates when standards and products permit. Please clarify PQC-readiness deliverables, acceptance criteria and relationship with CBOM/QBOM.	Please be guided by the RFP
1233	42			7.3.3.1 - Database Activity Monitoring	Kindly provide the database inventory by platform, version, operating system, environment and deployment model, including cloud databases. Please publish the authoritative database inventory for compatibility and sizing.	Relevant details shall be shared with the succesfull bidder
1234	42			7.3.3.1 - Database Activity Monitoring	The RFP references 150 application databases at DC and 150 at DR. Please confirm whether these are replicated instances or 300 separately monitored databases. Please clarify the licensable database/instance count and DC-DR topology.	Please be guided by the RFP
1235	42			7.3.3.1 - Database Activity Monitoring	Please provide peak transactions/queries per second, audit-event rates and daily log volumes by major database platform. Please publish performance and event volumetrics with annual growth assumptions.	Please be guided by the RFP
1236	42			7.3.3.1 - Database Activity Monitoring	Please confirm whether agent-based monitoring is permitted for all databases and identify databases requiring agentless/network-based monitoring. Please define permitted collection method by database platform and criticality.	Please be guided by the RFP
1237	42			7.3.3.1 - Database Activity Monitoring	Please clarify whether database vulnerability assessment, configuration assessment, sensitive-data discovery and virtual patching are mandatory modules. Please identify mandatory DAM modules, scan frequency and remediation responsibility.	Please be guided by the RFP
1238	42			7.3.3.1 - Database Activity Monitoring	Please confirm the required monitoring coverage for privileged users, local access, application/service accounts and encrypted database traffic. Please define mandatory activity sources, decryption dependencies and acceptance use cases.	Please be guided by the RFP
1239	46			7.3.4.5 - S-BOM, C-BOM, AI-BOM & QBOM	Kindly provide the list and technology stack of the initial 50 applications, scalable to 150, to be onboarded for BOM discovery. Please publish application criticality, ownership, deployment model and source availability.	Relevant details shall be shared with the succesfull bidder
1240	46			7.3.4.5 - S-BOM, C-BOM, AI-BOM & QBOM	Please provide the source-code repositories, artifact repositories, CI/CD tools, container registries and Kubernetes platforms to be integrated. Please publish tool names, instance counts, access method and integration responsibilities.	Relevant details shall be shared with the succesfull bidder
1241	46			7.3.4.5 - S-BOM, C-BOM, AI-BOM & QBOM	Please confirm the required machine-readable standards and versions for SBOM exchange, including CycloneDX and SPDX. Please define mandatory formats, versions, export frequency and validation criteria.	Relevant details shall be shared with the succesfull bidder
1242	46			7.3.4.5 - S-BOM, C-BOM, AI-BOM & QBOM	Please define the required CBOM scope, including cryptographic libraries, algorithms, certificates, keys, protocols, HSMs and embedded cryptography. Please publish the mandatory cryptographic asset classes and discovery depth.	Please be guided by the RFP
1243	46			7.3.4.5 - S-BOM, C-BOM, AI-BOM & QBOM	Please identify the 10 AI applications and provide the AI models, datasets, libraries, APIs and development platforms expected within AI-BOM scope. Please provide AI asset inventory and define required provenance, dependency and risk attributes.	Relevant details shall be shared with the succesfull bidder
1244	46			7.3.4.5 - S-BOM, C-BOM, AI-BOM & QBOM	Please clarify the expected QBOM and quantum-readiness outputs, including quantum-vulnerable asset identification, prioritisation and PQC migration planning. Please define QBOM schema, risk-scoring method, deliverables and acceptance criteria.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
1245	50			7.3.5.3 - AI Security	Kindly provide details of the 10 enterprise AI applications, underlying models, hosting locations, APIs and approved business use cases. Please publish the current and planned AI estate for architecture and licensing.	Relevant details shall be shared with the succesfull bidder
1246	50			7.3.5.3 - AI Security	Please confirm whether the solution must govern Microsoft Copilot and public GenAI services in addition to internally hosted LLMs and AI agents. Please identify all in-scope AI services, tenants and access channels.	Please be guided by the RFP
1247	50			7.3.5.3 - AI Security	Please clarify whether all AI traffic must pass through an AI gateway and provide expected peak and average prompt/API transaction volumes. Please publish throughput, concurrency, latency and availability requirements.	Please be guided by the RFP
1248	50			7.3.5.3 - AI Security	Please define mandatory inspection and enforcement controls for prompts and responses, including prompt injection, jailbreak, sensitive-data leakage, masking and malicious output. Please publish the minimum control set and acceptance test cases.	Please be guided by the RFP
1249	50			7.3.5.3 - AI Security	Please clarify the integration and policy ownership between AI Security, DLP, CASB, IDAM, SIEM/SOAR and the BOM platform. Please provide the target integration architecture and event/remediation workflows.	Details of the Bank-specific classification criteria and categories will be shared with the successful bidder during the SRS stage, in accordance with the Bank's security requirements. The bidder shall accordingly provision and design the proposed solution to support the Bank's classification requirements
1250	50			7.3.5.3 - AI Security	Please confirm whether AI red teaming, model security testing, model risk assessment and continuous posture monitoring are included in the implementation or managed-service scope. Please define testing frequency, deliverables, responsibility and acceptance criteria.	Please refer Addendum 1 for the revised clause.
1251	204			15.21.1 Existing and Envisaged Stack	Please share details of existing Vulnerability Management solution used by Punjab & Sind Bank. Please confirm if Bidder needs to manage this existing solution or propose a new solution ?	Please be guided by the RFP
1252	204			15.21.1 Existing and Envisaged Stack	If vulnerability scanning is in scope, please share the scan frequency and no of assets, IPs, servers for scanning ?	Please be guided by the RFP
1253	204			15.21.1 Existing and Envisaged Stack	Please share details of existing Application Security testing tool. Please confirm if Bidder needs to manage this existing solution or propose a new solution ?	Please be guided by the RFP
1254	204			15.21.1 Existing and Envisaged Stack	If SAST, DAST is in scope, please share the no. of applications, APIs that needs testing and the release cycle ?	Please be guided by the RFP
1255	204			15.21.1 Existing and Envisaged Stack	Please confirm if Punjab & Sind Bank's applications need Penetration testing ? If yes, please share the no. of applications and testing frequency and share details of existing solution if available.	Please be guided by the RFP
1256	68			7.9.3	Does PSB have an established Data Privacy Framework which is compliant with local data privacy laws with defined policies and processes that we need to follow?	Please be guided by the RFP
1257	68			7.9.1	Does PSB have well defined processes to perform DPIAs and Third party privacy assessments? Is there a need to perform these assessments?	Please be guided by the RFP
1258	68			7.3.4.5	As AI governance is mentioned under Key Deliverables, Does PSB have an existing AI Governance Framework including, policies, standards, procedures, control requirements, validation and approval workflow, responsible AI Validation gate process, model validation gate process, etc. in place?	Please be guided by the RFP
1259	46			7.3.4.5	Will PSB provide access to existing AI governance artifacts, including risk assessment process, governance standards, model documentation requirements, and control checklists?	Please be guided by the RFP
1260	46			7.3.4.5	Does PSB maintain an AI Risk Taxonomy and AI Risk Register that should be leveraged as part of the assessment process?	Please be guided by the RFP
1261	RFP No. PSB/HOIT/RFP/53/2026-27 Bid Number:GEM/2026/B/7936763 Appendix 1A Functional Specification	DNS Protection	General	As Document talks about Hardware based DDI solution but there is no guideline for the security of Hardware.	so to make sure the hardware is complient on a security standards please include the point mentioned below: "The DDI solution should be certified to Common Criteria 2, EAL2 or IC3S." This will help to get a proper hardware based solution.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
1262	20	Web Gateway	46	The proposed solution shall support PQC readiness, including support for secure cryptographic mechanisms and standards that facilitate future migration to quantum-resistant cryptography, wherever applicable to the solution	We understand that OEM product roadmap or equivalent supported cryptographic mechanisms will be acceptable. Kindly confirm.	Please be guided by the RFP
1263	27	DLP	73	The solution should be capable to fingerprint the data generated from specific applications, Web URLs, Data Repositories, Network Shares	Need clarity on the use case	Please be guided by the RFP
1264	42	Appendix 1 - Technical Specifications	Certificate Lifecycle Management, Clause #7	The Certificate Lifecycle Management provider should be a Global Certificate Authority for SSL and Licensed CA authorized agency by CCA, Govt. of India and shall comply with existing and future Information Security Guidelines.	Enterprise cybersecurity best practices, including principles derived from CERT-In and RBI guidelines on cyber resilience, strongly advocate for avoiding vendor lock-in and ensuring cryptographic agility. Mandating that the CLM software provider must also be the Certificate Authority (CA) restricts the Bank to a single-vendor ecosystem. Leading enterprise architecture requires a CA-Agnostic CLM platform that separates the management plane from the issuance plane, allowing the Bank to centrally manage certificates across multiple Global and CCA-licensed CAs. We request the bank to remove the clause or amend this clause to: 'The Certificate Lifecycle Management (CLM) solution must be CA-Agnostic and capable of integrating with and automating certificates issued by Global Certificate Authorities and CCA-authorized agencies	Please be guided by the RFP
1265	42	Appendix 1 - Technical Specifications	Certificate Lifecycle Management, Clause #10	Solution Should Continuous assessment to identify and remediate potential key and certificate-related vulnerabilities. Ability to manage access through blacklisting/whitelisting of devices, applications, and APIs.	Does 'blacklisting/whitelisting of devices, applications, and APIs' refer to Certificate Revocation List (CRL/OCSP) management and policy-based REST API access control, or endpoint application control?	The proposed solution shall identify, report and remediate Vulnerable cryptographic Keys that do not meet the RBI approved security baseline
1266		HIPS	Appendix 1A Functional Specification	The solution should include a Log Inspection module capable of capturing and analyzing system logs, providing audit evidence to meet PCI DSS or internal requirements within your organization. Additionally, the solution should have the ability to forward suspicious events to an SIEM system or centralized logging server for correlation, reporting, and archiving purposes.	Trendmicro specific	Please refer Addendum 1 for the revised clause.
1267		HIPS	Appendix 1A Functional Specification	Solution should support ant-tampering of agent for both windows and Linux based operating systems	Trendmicro specific	Please be guided by the RFP
1268		ZeroDay	Appendix 1A Functional Specification	Solution should integrate with Endpoint, Email and Server Security Solution for better Security posture and sharing of IOCs automatically, both user defined as well as the ones analyzed by sandbox	Please change to "Solution should integrate with Endpoint, Email and Server Security Solution for better Security posture and sharing of IOCs automatically in case if it cannot function in an inline mode for automatic sample submission " , this change will help in broader participitation	Please be guided by the RFP
1269				RFP Section 7.13, pages 88–93	Please confirm that the bidder's supply scope includes complete underlay infrastructure—compute/x86 servers, GPU servers, primary storage, SAN switches, backup software, backup appliance/storage, long-term storage, OS, virtualization, licences, FC HBAs, NICs, SFPs/optics, cables, rails, power cords, and all associated accessories—at DC, DR and NDR/non-production environments.	All passive components required for successful integration and deployment is also to be factored in by the bidder.
1270				RFP Section 7.13.10, page 92	The RFP states that the Bank will provide only TOR switches and racks, while the bidder must provide their sizing. Please confirm that no other infrastructure hardware will be supplied by the Bank.	Please be guided by the RFP
1271				RFP Section 7.13 vs. deployment table for "Backup & Retention", page 212	Section 7.13 requires the bidder to supply backup hardware/software, whereas the deployment table describes "Backup & Retention" as "Provided and maintained by bank." Please clarify whether backup software, backup appliance/storage and long-term storage are to be supplied by the bidder or are already available with the Bank.	Please refer Addendum 1 for the revised clause.
1272				RFP Section 7.13.9, page 92	Please provide Appendix 2—Masked Bill of Material—and Appendix 3—IT Infrastructure Virtual-to-Physical Mapping in editable format, with workload-wise resource requirements for DC, DR and non-production environments.	Bidder can download the excel files from the bank's portal https://punjabandsind.bank.in/module/tender-list
1273				Underlay Specs – GPU Servers	Please confirm the exact quantity, placement and intended workload/application requirement for GPU servers at DC, DR and non-production locations. Please also confirm whether the 94 GB GPU-memory requirement is per GPU or aggregate GPU memory per server.	Please be guided by the RFP
1274				Underlay Specs – Server OS and Virtualization	Please specify the prefferd OS and virtualization platform for each server/workload. Where Windows Datacenter is mandated, please confirm the required licensing metric and whether all physical cores of the proposed hosts need to be licensed.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
1275				Underlay Specs – Primary Storage Replication	Please confirm the replication topology between DC and DR: one-way, bidirectional, active-active, or active-passive. Please provide the required RPO, RTO, WAN bandwidth/latency and expected replication data-change rate.	Please be guided by the RFP
1276				Underlay Specs – FCIP requirement	The specification requires FCIP routers to be included in the BOM if separate FCIP routers are required, with minimum two units per site. Please confirm whether the Bank has existing IP/MPLS/WAN connectivity capable of supporting native IP-based storage replication, or whether FCIP equipment must be proposed.	Please be guided by the RFP
1277				RFP Section 7.13.10 – TOR Switches	As TOR switches will be supplied by the Bank, please share make/model, software version, number of available ports, port speeds, optic type, routing/VLAN design, MLAG/stacking architecture and available uplink/downlink capacity.	Relevant details will be shared with the successful bidder
1278				RFP Section 7.13.10 – TOR Switches	Please confirm whether the Bank will provide all TOR-switch ports, licences, network uplinks and compatible optics required for the proposed compute, storage and backup infrastructure, or whether bidder-supplied optics/DACs are required at both ends.	Please be guided by the RFP
1279				RFP Section 7.13.10 – Racks	Please provide rack details for DC, DR and NDR/non-production: rack size, available U-space, front/rear mounting standard, load-bearing capacity, airflow direction, cable-management arrangement, available A/B power feeds and PDU outlet type/quantity.	Relevant details will be shared with the successful bidder
1280				RFP Section 7.14.1, page 95	The RFP states that the Bank will provide hosting space and power, while bidder must factor racks. Please clarify whether this means the Bank will provide existing racks only, or whether the bidder must include new racks in its pricing. This should be reconciled with Section 7.13.10, which states that racks will be Bank-provided.	Please be guided by the RFP
1281				Underlay Specs – Backup Solution	Please confirm whether backup and recovery coverage is required for only the solutions supplied under this RFP or for the Bank's entire existing IT estate, including existing applications, databases, virtual machines, endpoints, security appliances and cloud workloads.	Please be guided by the RFP
1282				Underlay Specs – Backup Retention	Please confirm the exact retention policy to be used for commercial sizing. The Underlay Specs refer to daily incremental retention of two weeks and weekly full retention of four weeks, while the RFP deployment table indicates one-week daily and two-week weekly retention. Please confirm the final applicable retention schedule.	Please refer Addendum 1 for the revised clause.
1283				Underlay Specs – Long-Term Storage	Please clarify the contract period to be used for long-term storage sizing and whether all monthly full backups are to be retained for the entire contract period at both DC and DR.	Please be guided by the RFP
1284				Underlay Specs – Backup Architecture	Please clarify whether the Bank requires separate backup appliances/storage at DC and DR, or whether a centralized architecture with replicated backup copies is acceptable.	Please be guided by the RFP
1285				Underlay Specs – Backup Replication	Please provide the WAN bandwidth, latency, replication windows and RPO requirement for replication of deduplicated backup data between DC and DR.	Details to be shared with successful bidder
1286				Underlay Specs – Backup Integration	Please provide the make, model, version and configuration of the existing storage systems, hypervisors, databases, operating systems, Kubernetes/container platforms and cloud environments with which the proposed backup solution must integrate.	Details to be shared with successful bidder
1287				Underlay Specs – Backup Immutability	Please confirm the required immutability/retention-lock period for backup data and long-term archived data, and whether a separate cyber-recovery/air-gapped copy is required.	Details to be shared with successful bidder
1288				Underlay Specs – Storage/Server Disk Failure	The specification states that the Bank will not return defective disks. Please confirm whether bidders must include non-returnable disk retention/destruction support in the base warranty for servers, primary storage, backup storage and long-term storage.	Please be guided by the RFP
1289				Underlay Specs – OEM Experience	Please clarify whether the specified OEM experience in two scheduled commercial banks with at least 1,500 branches must be demonstrated separately for each category—server, primary storage, SAN switch, backup solution, backup appliance and long-term storage—or whether combined OEM references are acceptable.	Please be guided by the RFP
1290				RFP Section 7.13.3	Please confirm the expected high-availability architecture for DC, DR and non-production environments, including whether N+1 capacity, N+N redundancy, spare hosts/controllers, dual SAN fabrics and dual-path connectivity are mandatory.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
1291				RFP Section 7.13.4–5	Please confirm the required integration scope with the Bank's existing network, storage, security, monitoring, ITSM, IAM, PAM, SIEM/SOC and enterprise applications, including responsibility for any modification to the existing Bank environment.	Please be guided by the RFP
1292				RFP Section 7.13.4–5	Please provide the Bank's applicable infrastructure-security baseline/configuration standards for server hardening, storage encryption, OS configuration, patching, logging, privileged access, antivirus/EDR, vulnerability management and audit logging.	Please be guided by the RFP
1293				RFP Section 7.13.5	Please confirm who will provide IP addresses, VLANs, DNS records, NTP, PKI certificates, firewall rules, load-balancer configuration, Active Directory integration, service accounts and privileged credentials required for deployment.	Please be guided by the RFP
1294				RFP Section 7.13.5	Please confirm whether the bidder is responsible for supplying any additional network switches, management switches, KVM, console servers, PDUs, environmental sensors or out-of-band management connectivity required for complete deployment.	Please be guided by the RFP
1295				RFP Section 7.13.6	Please confirm the warranty/ATS/AMC term applicable to the supplied infrastructure. Underlay Specs indicate five-year support, whereas the RFP mentions three-year OEM support with separate Year-4 and Year-5 ATS/subscription in certain licensing clauses.	Please be guided by the RFP
1296				RFP Section 7.13.6	Please provide the final SLA for hardware support, including severity definitions, response time, onsite support, resolution/replacement time, availability targets and penalties for compute, storage, SAN and backup infrastructure.	Please be guided by the RFP
1297	136		13.1 Assignment & Subcontracting	The selected bidder shall not subcontract/JV/Consortium or permit anyone to perform any of the work, service or other performance required under the contract (excluding Proposed OEM personnels). All bidder's personnel proposed for the bank shall be on bidder's Payroll. Bank will seek relevant documentation from the bidder to validate the same.	Request Bank to please permit for subcontracting of H&F support	Please be guided by the RFP
1298	97		9 PROJECT TIMELINES	Overall Implementation period shall be 5 Months (Start Date is T0) for all solution & services The bidder shall submit a comprehensive Project Plan, within 7 days of T0 covering each proposed product/solution & Services, detailing all project phases, milestones, tasks, sub-tasks, activities, timelines, dependencies. The bidder shall submit the detailed Project Plan within seven (7) days from T0 for the Bank's review and approval. Any Liquidated Damages (LD) for delays in project execution shall be calculated based on the bank's approved Project Plan. In the event the bidder fails to submit the Project Plan within seven (7) days from T0, the Bank reserves the right to levy applicable Liquidated Damages for each day of such delay. If the delay in submission	> Request the project plan submission deadline be extended from 7 days to 1 month > Request the implementation timeline be extended from 5 months to 12 months	Please be guided by the RFP
1299	97	8	Contract Period	The bank may, at its sole discretion, extend the contract for an additional period of two years, in oneyear increments tranches. The Bank may extend the support services for an additional period of up to two (2) years beyond the original contract period. The pricing applicable during the extension period shall be mutually agreed and shall not exceed 110-120% of last year's AMC/ATS/Facility management rates quoted by the Selected Bidder.	It is requested that the annual rates of the support components shall be negotiated and agreed upon mutually.	Please be guided by the RFP
1300	136	13.1	Assignment & Subcontracting	The selected bidder shall not subcontract/JV/Consortium or permit anyone to perform any of the work, service or other performance required under the contract (excluding Proposed OEM personnels). All bidder's personnel proposed for the bank shall be on bidder's Payroll. Bank will seek relevant documentation from the bidder to validate the same.	We request that subcontracting be allowed given the scope of services.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
1301	136	13.2	Right to Alter Quantities	The bank reserves the right, at the time of award of contract and/or during the currency of the contract, to increase or decrease the quantity of goods, licenses, subscriptions, appliances, equipment, services, implementation effort, support services, or any line item covered under the contract by up to twentyfive percent (25%) of the quantities specified in the RFP/Contract, without any change in the unit prices, terms and conditions, technical specifications, delivery schedule, warranty obligations, support commitments, or any other contractual conditions.	It is clarified that in case of any repeat order or additional order after issuance of the initial PO, additional cost will be attracted and the prices for the same shall be determined at that time. However, any reduction in the number of hardware/software/licenses will have no effect on the prices. In other words, there shall be no reduction in the prices.	Please be guided by the RFP
1302	136	13.3	Delay in Bidder's performance	The bidder must strictly adhere to the schedule, as specified in the purchase contract/purchase order, executed between the Parties for performance of the obligations, arising out of the purchase contract and any delay in completion of the obligations by the Bidder will enable Bank to resort to any or both of the following: 1. Claiming Liquidated Damages 2. Termination of the purchase agreement fully or partly and claim liquidated damages. 3. Execution of Bid Declaration Form / Invoking EMD or Performance Bank Guarantee	We request that a notice cum cure period of atleast 30 days be provided to the bidder to rectify any breach/delay.	Please be guided by the RFP
1303	137	13.5	Dispute Resolution	If any dispute, difference or claim arises between the parties hereto in connection with the validity, interpretation, implementation or alleged breach of the terms of this Agreement or anything done or omitted to be done pursuant to this Agreement, the Parties shall attempt in the first instance to resolve the same through negotiation. If the dispute is not resolved through negotiation within 30 (thirty) days after commencement of discussions, then, the parties shall be at liberty to approach competent court of law at Delhi for adjudication of the disputes.	We request that the any dispute arising between the parties under the RFP/agreement be referred to arbitration, and the arbitration proceedings be conducted in accordance with the Arbitration and Conciliation Act,1996 and the Rules thereunder (as amended from time to time). Further, the arbitration be conducted by a sole arbitrator to be appointed mutually by the Parties. The seat and venue of arbitration be New Delhi, and the arbitral proceedings be conducted in English. We request changes in the clause to indicate the above.	Please be guided by the RFP
1304	138	13.8	Digital Personal Data Protection Compliance	The successful bidder shall indemnify and hold the Bank harmless against any loss, liability, penalty, or damage arising out of any breach or non-compliance with the Digital Personal Data Protection Act, 2023.	We request deletion of this clause on indemnity. The bidder shall remain contractually liable for this breach. Moreover, the liability of the bidder for breach of confidentiality is uncapped.	Please be guided by the RFP
1305	140	13.13	Indemnity	The bidder agrees to indemnify and keep indemnified the Bank against all losses, damages, costs, charges and expenses incurred or suffered by the Bank due to or on account of any breach of the terms and conditions contained in this RFP or Service Level Agreement to be executed.	We request deletion of this clause on indemnity. The bidder shall remain contractually liable for this breach.	Please be guided by the RFP
1306	140	13.13	Indemnity	The Bidder shall indemnify, defend and hold harmless the Bank, its directors, officers, employees and representatives against all losses, damages, liabilities, claims, demands, actions, proceedings, penalties, costs and expenses (including reasonable legal expenses, forensic investigation costs, remediation costs and costs incurred in responding to regulatory/customer claims) arising out of or relating to: (a) breach of the Contract/RFP/SLA; (b) negligence, gross negligence, fraud, willful misconduct or omission of the Bidder/OEM/subcontractor; (c) breach of confidentiality or data protection obligations; (d) cyber security incident, data breach, unauthorised access, loss or disclosure of Bank/customer data attributable to the Bidder/OEM/subcontractor; (e) infringement of intellectual property rights; (f) violation of applicable law, regulatory directions or statutory requirements attributable to the Bidder/OEM/subcontractor; (g) third-party/customer claims arising from the acts or omissions of the Bidder/OEM/subcontractor; and (h) any loss suffered by the Bank in consequence of failure of the Bidder to perform the services in accordance with the Contract.	We request a revision in the clause to be read as follows: The Bidder shall indemnify, defend and hold harmless the Bank, its directors, officers, employees and representatives against all losses, damages, liabilities, claims, demands, actions, proceedings, penalties, costs and expenses (including reasonable legal expenses, forensic investigation costs, remediation costs and costs incurred in responding to regulatory/customer claims) arising out of or relating to: (a) negligence, gross negligence, fraud, willful misconduct or omission of the Bidder/OEM/subcontractor; (b) breach of confidentiality obligations; (c) infringement of intellectual property rights; (d) violation of applicable law, regulatory directions or statutory requirements attributable to the Bidder/OEM/subcontractor. Apart from the above, the bidder shall remain contractually liable for all other breaches.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
1307	143	13.21	Limitation of Liability	The aggregate liability of bidder in connection with this Agreement, in respect of any claims, losses, costs or damages arising out of or in connection with this RFP/Agreement shall not exceed the total Project Cost. Under no circumstances shall either Party be liable for any indirect, consequential or incidental losses, damages or claims including loss of profit, loss of business or revenue. The limitations set forth herein shall not apply with respect to: 1. claims that are the subject of indemnification pursuant to infringement of third-party Intellectual Property Right, 2. damage(s) occasioned by the Gross Negligence or Willful Misconduct of Service Provider, 3. damage(s) occasioned by Service Provider for breach of Confidentiality Obligations, 4. Regulatory or statutory fines imposed by a government or Regulatory agency for noncompliance of statutory or regulatory guidelines applicable to the Bank, provided such guidelines were brought to the notice of Service Provider.	Please confirm that the Bidder's liability from indirect, consequential or incidental losses shall be excluded notwithstanding the exceptions given under point nos. 1-4, and that the Bidder shall not be liable for any indirect, consequential or incidental losses under any circumstances.	Please be guided by the RFP
1308	144	13.22	Order Cancellation	Bank's Right to terminate the entire/ unexecuted part of the Purchase Order on Convenience 1) The Bank reserves its right to cancel the entire unexecuted part of the Purchase Order at any time on its convenience without assigning any reason/s whatsoever by giving 'one 'month notice to the other party. 2) In the event of termination of the Agreement for the Bank's convenience, bidder shall be entitled to receive payment for the Services rendered (delivered) up to the effective date of termination.	We request that a period of atleast 90 days be given before termination of the contract for convenience. Also, please confirm that PSB shall additionally pay to the Bidder for all work done till the date of termination, as well as for the orders already placed with OEMs/Licensors, which orders cannot be cancelled with the OEMs/Licensors, cancellation costs, if any, levied by the OEMs/Licensors, and logistical and administrative expenses, if any, incurred by the Bidder on account of such cancellations, which expenses shall be billed on actuals. Further, if the Bidder is providing any products/goods on opex or lease model, then PSB shall pay the Bidder the residual value of the products.	Please be guided by the RFP
1309	144	13.22	Order Cancellation	Then the Bank shall have the right to recover from the Bidder any amounts already paid by the Bank in respect of the product (including respective hardware) and/or services after adjusting for the penalties already levied and recovered by the Bank for that specific product/ service. Further, where the Bidder is able to provide satisfactory evidence that the delay or default was not attributable to the Bidder, such portion shall be excluded from the scope of recovery.	We request that any dues paayble only be recovered/adjusted with any liquidated damages or penalties levied against the bidder, and not against any other amount payable to the bidder for the services rendered.	Please be guided by the RFP
1310	124		SERVICE LEVELS & PENALTIES	For every 0.01% reduction, or part thereof, below the prescribed availability level of 99.99%, a penalty equivalent to 1% of the Monthly Maintenance Cost (MMC) shall be levied	Kindly confirm that, where an availability breach is attributable to failure/unavailability of a specific appliance, software tool, subscription, or solution component, the 1% penalty per 0.01% availability reduction shall be calculated only on the applicable monthly AMC/ATS/subscription cost of the affected solution/device, and shall not be calculated on the total consolidated MMC, including FM/O&M manpower cost and the AMC/ATS/subscription costs of unaffected solutions.	Please be guided by the RFP
1311	121		Critical/High incident — 15-minute response and 45-minute resolution timeline.	The RFP requires acknowledgement/response within 15 minutes and resolution of a Critical/High incident within 45 minutes. Critical incidents include major business disruption, production-component failure, security incidents, and failure of key infrastructure such as application, web, database, solution, storage, backup, and network components.	Kindly consider revising the High, Medium and Low incident resolution timeline to 2 hours, 4 hours and 12 hours. while retaining the 15-minute acknowledgement/response commitment.	Please be guided by the RFP
1312	73–75		7.11 – Resource Requirement	Resources are required to work in rotational shifts, extended hours, weekends, holidays and critical situations. The bidder must maintain backup resources, succession planning and cross-skilling.	Please clarify whether the prescribed resource numbers represent active shift resources only, excluding relievers for weekly offs, leave, training, and absenteeism. Kindly specify the expected reserve/backup staffing factor for 24×7×365 coverage.	Please be guided by the RFP. The prescribed resource numbers represent the minimum onsite shift deployment requirement
1313			Day-2 resource model		Please confirm whether the minimum L1, L2, L3/Project Manager, and IT Infrastructure resource counts are to be deployed per location (DC, DR, SOC, IT Security Office) or as a centralized pooled deployment across all locations.	Please be guided by the RFP. Refer Section 7.11 (Resource Requirement). The prescribed minimum resource counts (L1, L2, L3/Project Manager, IT Infrastructure) represent the aggregate minimum onsite shift-wise deployment for the engagement
1314	120–121		12 – Penalty Recovery and Cap	Penalties may be recovered from quarterly AMC, ATS or FMS payments; the RFP provides that only the highest applicable penalty shall be levied for the same event and specifies an overall cap for SLA penalties and LDs.	Please confirm that no overlapping or multiple penalties will be imposed for the same underlying event—for example, availability SLA breach, incident resolution delay, and device failure—and only the highest applicable penalty shall apply, subject to the overall contractual penalty cap.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
1315	124		12 – Monthly Maintenance Cost	MMC includes Total FM (O&M) Manpower Cost, total AMC cost of infrastructure/appliances, and total ATS or subscription cost of software/tools. Quarterly Maintenance Cost is derived from the same components.	Please clarify that FM/O&M manpower cost and charges for unaffected solutions will be excluded from the penalty base for a device- or solution-specific availability failure. Further, please confirm that Quarterly Maintenance Cost is only a payment/recovery basis and not the penalty base for a monthly availability breach.	Please be guided by the RFP.
1316	130–131		12 – Manpower Availability	Minimum manpower must be maintained at 100%; a shortfall attracts a penalty of ₹25,000 per resource per week or part thereof until the required manpower strength is restored.	Kindly allow a reasonable cure period for temporary absences caused by medical emergency, resignation, or circumstances beyond bidder control, provided an equivalent or higher-skilled replacement is deployed promptly. Please also clarify whether a penalty applies where an approved reliever provides the required shift coverage.	Please be guided by the RFP
1317	5	Functional Specs-Anti DDOS	70	The proposed solution shall support on-premises appliance-based, cloud-based/service-provider-hosted (scrubbing center), or hybrid architectures combining on-premises and cloud-based mitigation, as applicable to the Bank's deployment requirements.	Clarification required : We understand the Hybird solution of On-Prim Appliance and Cloud Signaling to Upstream ISP fulfills the requirement (refer to Clause #46)	Please be guided by the RFP
1318	DNS Protection	General			As Document talks about Hardware based DDI solution but there is no guideline for the security of Hardware. so to make sure the hardware is complient on a security standards please include the point mentioned below: "The DDI solution should be certified to Common Criteria 2, EAL2 or IC3S." This will help to get a proper hardware based solution. Adding this requirement establishes an independently assessable security baseline for the proposed hardware-based DDI platform. It provides assurance that core security controls have been evaluated against a recognized assurance framework, reduces the risk of deploying hardware with insufficient protection, and gives the evaluation team an objective compliance criterion.	Please be guided by the RFP
1319	RFP No. PSB/HOIT/RFP/53/2026-27 Bid Number:GEM/2026/B/7936763 Appendix 1A Functional Specification	Architectural Requirements Point No:65	The threat intelligence must be consumed from on-premises for Authoritative, Recursive and Caching DNS	As the Recursive DNS response comes from the public internet and queries has to go out to internet its better to use hybrid deployment where Authoritative Remains on-premises & Caching happens on- premises but Recursive DNS security happens on cloud (SAAS). Please update the point as: The threat intelligence must be consumed In a hybrid mode on-premises for Authoritative, on cloud for Recursive and Caching should happend on-premises.	A hybrid requirement aligns the security control with the different risk and performance characteristics of authoritative and recursive DNS. Keeping authoritative DNS and caching on premises preserves direct control of internal services and cached data, while cloud-based protection for recursive traffic enables scalable inspection of internet-bound queries. This avoids forcing all DNS functions into one deployment model and supports resilience, operational flexibility, and policy-based data handling.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
1320	RFP No. PSB/HOIT/RFP/53/2026-27 Bid Number:GEM/2026/B/7936763 Appendix 1A Functional Specification	Security RequirementsPoint No: 73		73The solution must be able to prevent infections, blocking the DNS requests towards malware distribution domains or drive-by domains, and contain the pre-existing infections, blocking the DNS requests towards command and control infrastructures. The solution should support following Feeds : 73.1Base Hostnames 73.2Anti-malware 73.3Ransomware 73.4Bogon 73.5Malware Ips/Domains 73.6Bot IPs/Domains 73.7Exploit Kit IPs/Domains 73.8Malware DGA hostnames 73.9TOR Exit Node IPs/Domains 74.10 Extended Base & anti-malware Hostnames 74.11 Extended malware IPs /Domains 74.12Extended TOR Exit Node IPs /Domains 74.13Extended Ransomware IPs /Domains 74.14Extended Exploit Kits IPs/Domains 74.15SpamBot IPs/Domains 74.16Spambot IPs DNSB/Domains	As we are talking about DNS protection and there are multiple feeds are mentioned but we are missing on specific feeds which are critical for India so suggesting to add the same here "EECN IP (EECN_IP)". Please update the point as: 73The solution must be able to prevent infections, blocking the DNS requests towards malware distribution domains or drive-by domains, and contain the pre-existing infections, blocking the DNS requests towards command and control infrastructures. The solution should support following Feeds : 73.1Base Hostnames 73.2Anti-malware 73.3Ransomware 73.4Bogon 73.5Malware Ips/Domains 73.6Bot IPs/Domains 73.7Exploit Kit IPs/Domains 73.8Malware DGA hostnames 73.9TOR Exit Node IPs/Domains 74.10 Extended Base & anti-malware Hostnames 74.11 Extended malware IPs /Domains 74.12Extended TOR Exit Node IPs /Domains 74.13Extended Ransomware IPs /Domains 74.14Extended Exploit Kits IPs/Domains 74.15SpamBot IPs/Domains 74.16Spambot IPs DNSB/Domains 74.17 EECN IP (EECN_IP) Adding this feed improves coverage of IP indicators associated with regionally relevant malicious infrastructure and reduces blind spots in DNS-based protection. Listing it as an explicit supported source also makes vendor responses comparable and enables the organization to verify that the threat-intelligence input can be consumed and enforced by the solution.	Please be guided by the RFP
1321	RFP No. PSB/HOIT/RFP/53/2026-27 Bid Number:GEM/2026/B/7936763 Appendix 1A Functional Specification	Management Requirements Point No:93	The vendor must have support center in India	Make in India gives more control and localization capability so please request you to modify the point. Please update the point as: The vendor must have Development Center and support center in India	Requiring both development and support capability in India strengthens local accountability across the full service lifecycle. It can improve escalation speed for product defects and security issues, support coordination during incidents, and help address localization, regulatory, and operational requirements; the specification should therefore distinguish development capability from support presence.	Please be guided by the RFP
1322	RFP No. PSB/HOIT/RFP/53/2026-27 Bid Number:GEM/2026/B/7936763 Appendix 1A Functional Specification	Management Requirements		Additional	As a best practies all the solution must use two factor authentication so please include this point The solution must support two factor authentication Two-factor authentication adds a second verification control for administrative access, reducing the likelihood that a compromised password alone can be used to change DNS security policies or weaken protections. Making it a mandatory solution capability establishes a minimum access-security baseline for management interfaces and remote administration.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
1323		2.1	2.1 - SSL Orchestrator	System must support 150 K SSL offload CPS on RSA 2 K Key and 90 K SSL offload CPS on ECDHE cipher	"System must support SSL/TLS decryption throughput on RSA 2K Key and ECDHE cipher sufficient to handle peak encrypted traffic at the deployment point at full line rate, with all inspection policies active. " "SSL Offload CPS" measures how many SSL sessions a device can terminate per second — where each client session is decrypted, processed, and a brand-new SSL session is re-initiated toward the backend server (two separate TCP/SSL connections per client). This is an ADC / Server Load Balancer (SLB) metric, not an SSL Orchestrator metric. SSLo delivers high-throughput inline Decrypt-Inspect-Re-Encrypt (DIRE) at line rate — the correct metric is SSL/TLS inspection throughput (Gbps) and maximum concurrent SSL sessions, not session termination CPS.	Please be guided by the RFP
1324		2.2	System must support 50 K SSL CPS for SSLo	"System must support SSL/TLS inspection throughput for SSLo sufficient to handle peak encrypted traffic at the deployment point at full line rate, without packet loss or session drops. "	SSL CPS (Connections Per Second) as framed here is borrowed from ADC/SLB terminology for session termination rate. An SSL Orchestrator intercepts existing SSL sessions in-flight — it does not establish new SSL sessions in the ADC sense. The correct performance metric for an SSLo is throughput (Gbps of SSL/TLS traffic inspected) and maximum concurrent SSL sessions under DIRE mode. SSLo measures performance by SSL/TLS inspection throughput (Gbps) and maximum concurrent SSL sessions under DIRE mode — not connection establishment rate.	Please be guided by the RFP
1325		2.3	Technical Specifications	System must support 64 million concurrent IP sessions and 2 M SSL sessions	"64 million concurrent IP sessions" is a stateful connection table metric of Firewalls, NAT/PAT devices, and Load Balancers that track per-flow entries for address translation or load distribution. A Network Packet Broker (NPB) operates at wire speed WITHOUT maintaining IP session state tables — this metric is fundamentally inapplicable to an NPB. Even for the SSLo component, "64M IP sessions" reflects firewall/ADC session capacity, not SSL visibility capacity. "64 million concurrent IP sessions" is a native feature of Firewall / NAT / ADC (stateful connection table) — not applicable to SSLO/NPB. Kindly request you to omit this from the SSLO/NPB. SSLo supports configurable concurrent SSL/TLS inspection sessions — ensuring all encrypted traffic is decrypted and inspected at scale without requiring IP-level session state tables.	Please be guided by the RFP
1326		2.4		System must support L7 Connections per second - At least 3 Million	L7 Connections Per Second (L7 CPS) is a native feature of ADC / Load Balancer (L7 connection ownership and proxying) — not applicable to SSLO/NPB. Kindly request you to omit this from the SSLO/NPB. L7 Connections per second (L7 CPS) is a benchmark metric of ADCs and Load Balancers that proxy, terminate, and forward HTTP/HTTPS connections (maintaining the full SYN/ACK L7 connection lifecycle, HTTP multiplexing etc.). An SSL Orchestrator does NOT own or proxy L7 connections — it decrypts SSL sessions transparently for inspection and forwards the same connection. SSLo provides L7-aware traffic classification and steering — directing decrypted flows to the right inline tool based on URL, domain, or application attributes, without owning or proxying the L7 connection.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
1327		3.1		System must support 30 Partition/Virtual Context keeping in view that One virtual partition will do decryption and another will do re-encryption	"One virtual partition for decryption, another for re-encryption" is an ADC/SLB architectural pattern (notably ADC platforms with virtual server-based SSL offload architecture) where SSL offloading splits the flow between two virtual domains on the same device — each session is terminated at one context and re-originated at another. This is the session-termination/ADC model. SSLo performs Decrypt-Inspect-Re-Encrypt (DIRE) as a single unified inline pipeline — no partition split is needed or architecturally valid. Virtual partition-based decryption/re-encryption split is a native feature of ADC / SLB — not applicable to SSLO/NPB. SSLo performs Decrypt-Inspect-Re-Encrypt (DIRE) as a single unified inline pipeline; no partition split is needed. Kindly request you to omit this from the SSLO/NPB. SSLo performs DIRE as a single unified inline pipeline — eliminating the partition-based session split entirely while delivering the same decryption outcome at higher efficiency.	Please be guided by the RFP
1328		3.2		System must support dedicated configuration file for each Virtual context	Dedicated per-context configuration files are an ADC multi-tenant virtualization feature where each virtual partition maintains its own independent routing tables, certificate stores, and policy files — a concept specific to ADC platforms with per-virtual-partition configuration management. An SSL Orchestrator/NPB manages traffic through a unified inspection policy framework with profile-based SSL certificate and policy management across all traffic segments. Dedicated per-context configuration files are a native feature of multi-tenant ADC platforms — not applicable to SSLO/NPB. SSLo/NPB uses a unified inspection policy framework for all traffic segments. Kindly request you to omit this from the SSLO/NPB. SSLo provides a unified policy framework with profile-based SSL certificate and inspection management across all traffic — simplifying operations without per-context configuration overhead.	Please be guided by the RFP
1329		3.3		System must support resource allocation to each context including throughput, CPS, Concurrent connection, SSL throughput	Per-context resource allocation (throughput caps, CPS quotas, concurrent connection limits per virtual partition) is an ADC multi-tenancy QoS feature used in shared-hardware service-provider environments. The inclusion of "CPS" as a per-context allocation parameter further confirms this is an SLB/ADC concept. NPB/SSLo platforms handle all traffic globally across available hardware — they do not carve resources per virtual partition. Per-context resource quota allocation (throughput, CPS, concurrent connections) is a native feature of ADC / SLB multi-tenant deployments — not applicable to SSLO/NPB. SSLo/NPB handles all traffic globally across available hardware resources. Kindly request you to omit this from the SSLO/NPB. SSLo delivers policy-based traffic classification and inspection prioritisation — optimising global hardware utilisation across all flows without per-partition resource carving.	Please refer Addendum 1 for the revised clause.
1330		3.4		System must be able to modify the resource allocation on the fly without restarting/rebooting any context	Dynamic live modification of per-partition resource quotas (throughput caps, CPS limits) without context restart is an ADC operational feature for multi-tenant virtual partition management. This concept does not apply to SSLo/NPB. The equivalent operational requirement for an SSLo/NPB is hot-update of inspection policies without traffic interruption. Live per-partition resource reallocation without context restart is a native feature of ADC — not applicable to SSLO/NPB. SSLo supports hot-update of SSL inspection policies, bypass rules, and service chain configurations — achieving zero-downtime policy changes without any partition or context restart.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
1331		3.5		All the virtual context must be available from day-1	Virtual context day-1 availability is tied to ADC per-context licensing models. An SSLo/NPB does not have virtual context licensing. All inspection, decryption, and steering capabilities are available at deployment under the base license. Per-virtual-context day-1 availability is an ADC licensing construct — not applicable to SSLO/NPB. All SSLO/NPB inspection, decryption, and steering features are available from Day-1 under the base license. Kindly request you to omit this from the SSLO/NPB. SSLomakes all decryption, inspection, and steering capabilities fully operational from Day-1 under the base licence — no phased activation or per-context licencing required.	Please be guided by the RFP
1332		4.3		System must support protection from Land Attack	Land Attack protection (DoS attack where source IP = destination IP, causing TCP stack loopback) is a stateful Layer 3/4 DDoS mitigation feature of Firewalls, IPS, and Anti-DDoS appliances. An SSLo/NPB is a visibility and traffic steering platform — it forwards traffic to inline security tools (IPS, Firewall, Anti-DDoS) which are responsible for attack mitigation. The SSLo/NPB decrypts and steers; it does not enforce attack protection itself. Land Attack protection is a native feature of Firewall / IPS — not applicable to SSLO/NPB. The inline Firewall/IPS chained through the SSLo is responsible for this protection. Kindly request you to omit this from the SSLO/NPB. SSLo ensures all traffic — including SSL-encrypted flows — is decrypted and steered to the inline Firewall/IPS, enabling Land Attack detection on sessions that would otherwise remain hidden within encryption.	Please be guided by the RFP
1333		4.4		System must support protection from Packet Deformity Layer 3	Layer 3 Packet Deformity protection (malformed IP header detection and dropping) is a stateful Firewall/IPS protocol enforcement function. NPB/SSLo devices process and forward packets for visibility — Layer 3 protocol conformance enforcement is the responsibility of inline security tools in the inspection chain. Layer 3 Packet Deformity protection is a native feature of Firewall / IPS — not applicable to SSLO/NPB. Kindly request you to omit this from the SSLO/NPB. SSLodecrypts and forwards all traffic to the inline Firewall/IPS — enabling Layer 3 packet deformity enforcement to apply equally to clear-text and previously encrypted flows.	Please be guided by the RFP
1334		4.5		System must support protection from Packet Deformity Layer 4	Layer 4 Packet Deformity protection (malformed TCP/UDP segment detection) is a stateful Firewall/IPS function. An NPB/SSLo passes traffic to inline security tools — Layer 4 protocol conformance enforcement is the responsibility of those downstream tools. Layer 4 Packet Deformity protection is a native feature of Firewall / IPS — not applicable to SSLO/NPB. Kindly request you to omit this from the SSLO/NPB. SSLo decrypts and forwards all traffic to the inline Firewall/IPS — enabling Layer 4 packet deformity enforcement to cover encrypted sessions that would otherwise bypass inspection.	Please be guided by the RFP
1335		4.6		System must support protection from Ping of Death	Ping of Death protection (blocking oversized/malformed ICMP packets used in DDoS attacks) is an Anti-DDoS/Firewall feature. An SSLo/NPB is a visibility device — DDoS mitigation is performed by the inline Anti-DDoS or Firewall chained through the SSLo/NPB. Ping of Death protection is a native feature of Anti-DDoS / Firewall — not applicable to SSLO/NPB. Kindly request you to omit this from the SSLO/NPB. SSLo ensures all traffic — including encrypted — is visible to the inline Anti-DDoS/Firewall, enabling Ping of Death mitigation across the full traffic stream.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
1336		4.7		System must support protection from TCP No Flag	TCP No Flag detection (null scan — TCP packets with no flags set, used in stealthy port scanning) is a TCP protocol anomaly detection feature of IPS/Firewall systems. This is not a function of an SSLo or NPB, which forward traffic to inline security tools for such detection and blocking. TCP No Flag (null scan) detection is a native feature of IPS / Firewall — not applicable to SSLO/NPB. Kindly request you to omit this from the SSLO/NPB. SSLo decrypts all flows before forwarding to the inline IPS/Firewall — enabling null scan detection to operate on fully decrypted traffic and closing the encrypted blind spot.	Please be guided by the RFP
1337		4.8		System must support protection from TCP Syn Fin	TCP SYN+FIN simultaneous flags (inherently invalid per RFC 793, used in TCP stack probing and IDS evasion attacks) is a Firewall/IPS protocol anomaly protection feature. Detection and dropping of such crafted packets is a Firewall/IPS enforcement function — not an NPB/SSLo function. TCP SYN+FIN flag anomaly detection is a native feature of Firewall / IPS — not applicable to SSLO/NPB. Kindly request you to omit this from the SSLO/NPB. SSLo decrypts and steers all flows to the inline Firewall/IPS — enabling TCP flag anomaly enforcement on both clear-text and previously encrypted sessions.	Please be guided by the RFP
1338		4.9		System must support protection from TCP Syn Frag	TCP SYN packet fragmentation protection (defending against fragmented SYN packets used to evade stateful firewall inspection) is a Firewall/IPS anti-evasion feature. While an NPB can reassemble IP fragments before forwarding to inspection tools (Packet Grooming — covered in Section A.11), actively blocking TCP SYN fragmentation attacks is a Firewall/IPS function. TCP SYN fragmentation attack protection is a native feature of Firewall / IPS — not applicable to SSLO/NPB. Note: NPB supports IP fragment reassembly (Packet Grooming) as a pre-processing step before forwarding to inspection tools, which is distinct from SYN fragmentation attack blocking. Kindly request you to omit this from the SSLO/NPB. SSLo performs IP fragment reassembly (Packet Grooming) before forwarding to the inline IPS/Firewall — ensuring SYN fragmentation evasion attempts are fully visible to and handled by the downstream security tool.	Please be guided by the RFP
1339		4.10		System must support connection limit based on source IP	Per-source-IP connection limiting is a Layer 4 DDoS defense feature of Firewalls, ADC/Load Balancers, and Anti-DDoS appliances that maintain per-source-IP connection state tables for enforcement. An NPB/SSLo operates at wire speed without per-source connection state — this is a Firewall/ADC enforcement function. Per-source-IP connection limiting is a native feature of Firewall / Anti-DDoS / ADC — not applicable to SSLO/NPB. Kindly request you to omit this from the SSLO/NPB. SSLo decrypts and forwards all traffic to the inline Firewall/Anti-DDoS — enabling per-source-IP connection limiting to cover encrypted sessions that would otherwise bypass enforcement.	Please be guided by the RFP
1340		4.11		Per-source-IP connection rate limiting is a native feature of Anti-DDoS / Firewall — not applicable to SSLO/NPB. Kindly request you to omit this from the SSLO/NPB.	Connection rate limiting per source IP (SYN rate throttling for SYN flood mitigation) is a stateful Layer 4 Firewall/Anti-DDoS feature requiring per-source rate counters and enforcement logic. This is outside the functional scope of an SSL Orchestrator or Packet Broker. SSLo ensures all decrypted traffic is forwarded to the inline Anti-DDoS/Firewall — enabling SYN rate throttling to apply to all flows, including SSL-wrapped flood attempts.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
1341		4.12	System must support request rate limit based on source IP	L7 request rate limiting per source IP is a native feature of WAF / ADC — not applicable to SSLO/NPB. Kindly request you to omit this from the SSLO/NPB.	L7 request rate limiting per source IP is an application-layer DDoS mitigation feature of WAFs, ADCs, and application-aware firewalls — requiring HTTP/HTTPS request parsing and per-source accounting. The SSLo decrypts traffic for forwarding to downstream tools; L7 request rate limiting is performed by the WAF/Application Firewall in the inspection chain. SSLo decrypts HTTPS traffic and forwards it to the inline WAF — enabling L7 request rate enforcement to apply to all HTTP/S traffic, including encrypted requests.	Please be guided by the RFP
1342		6.14	System must support TCL based scripts for custom rules	Suggested Change : "System must support programmable traffic steering and SSL inspection policy customization via an open standard mechanism (e.g., REST API, Python, Lua, or vendor-supported scripting language) for defining custom interception, bypass, and forwarding rules."	"TCL-based scripts for traffic rules" (vendor-proprietary scripting rules) is a feature exclusive to a specific ADC/proxy vendor's platform. . No other SSL visibility/orchestration vendor uses TCL as their scripting interface. This specification should be replaced with an open, vendor-neutral programmability requirement. SSLo provides open REST API and Python/Lua-based scripting for fully customisable interception, bypass, and forwarding rules — through vendor-neutral interfaces accessible to any automation framework.	Please be guided by the RFP
1343		7.1	System must support VRRP based redundancy	VRRP is a gateway redundancy protocol for Router / Firewall / L3 Switch — not applicable to SSLO/NPB. SSLo/NPB achieves HA through dedicated appliance-level clustering with heartbeat-based active-active or active-standby failover. Kindly request you to omit this from the SSLO/NPB.	VRRP (Virtual Router Redundancy Protocol, RFC 5798) is a network-layer gateway redundancy protocol designed for routers, L3 switches, and default-gateway devices to provide IP gateway failover. SSL Orchestrators and NPBs achieve HA through dedicated appliance-level mechanisms — heartbeat-based active-active or active-standby clustering with dedicated HA interconnect links and sub-second failover. VRRP is architecturally designed for routing/gateway failover, not for SSL inspection appliance HA. SSLo achieves HA through dedicated appliance-level heartbeat clustering (active-active or active-standby) with sub-second failover — purpose-built for inline SSL inspection continuity.	Please refer Addendum 1 for the revised clause.
1344		7.4	System must support dynamic VRRP priority by traffic interface, server, next hop and routes	Dynamic VRRP priority management is a native feature of Router / Firewall — not applicable to SSLO/NPB. SSLo/NPB HA failover is driven by inline tool health, port link state, and inspection pipeline availability. Kindly request you to omit this from the SSLO/NPB.	Dynamic VRRP priority management (adjusting VRRP master election priority based on upstream interface health, route availability, or next-hop reachability) is a router/firewall cluster management feature for L3 gateway HA scenarios. For an SSLo, HA failover decisions should be driven by SSL inspection pipeline health, inline tool availability, and traffic port link state — not by routing protocol (VRRP) priority manipulation. SSLo drives HA failover based on SSL inspection pipeline health, inline tool availability, and port link state — ensuring resilience is tied directly to visibility continuity, not routing protocol metrics.	Please refer Addendum 1 for the revised clause.
1345	`	8.5	System must support REST-style XML API (aXAPI) for all functions	Suggested Change : "System must support a standard, fully documented REST API (JSON and/or XML over HTTPS) for all configuration, monitoring, and management functions. Complete API documentation must be provided as part of the solution delivery."	"aXAPI" is a specific vendor's proprietary REST-style XML management API, exclusive to their ADC product line. No other SSL visibility/orchestration vendor uses TCL as their scripting interface. This specification should be replaced with an open, vendor-neutral programmability requirement. SSLo offers a fully documented standard REST API (JSON/XML over HTTPS) for all configuration, monitoring, and management functions — accessible to any standard API client or automation platform.	Please refer Addendum 1 for the revised clause.
1346	Page 7	1	Bid validity	180 days from the date of opening of the bid.	We request you to change this to 15 days or as per validity given by OEMs	Please be guided by the RFP
1347	Page 16	6.2	Bid Currency & Price Structure	Prices shall be expressed in the Indian Rupees only. The bidder must quote price exclusive of all applicable GST. The cost will not depend on any variation in the dollar exchange rate/change in tax structure.	Bidder will quote based on the current cost price of the quoted products and current exchange rate. Due to the current global uncertainty concerning the proposed US tariffs, and the fluctuating foreign exchange rates, our quoted price will subject to change based on the then current exchange rate and any associated vendor price increases at the time of invoicing. Pls confirm	Please be guided by the RFP
1348	Page 97	8	Contract Period	The bank may, at its sole discretion, extend the contract for an additional period of two years, in one year increments tranches. The Bank may extend the support services for an additional period of up to two (2) years beyond the original contract period. The pricing applicable during the extension period shall be mutually agreed and shall not exceed 110-120% of last year's AMC/ATS/Facility management rates quoted by the Selected Bidder.	Over a five-year period, market conditions may change significantly. Extending the contract on the same commercial and legal terms may not reflect the prevailing market realities at the time of extension, potentially leading to financial unviability for the service provider hence we request PSB to mutually discuss and agree upon the terms and commercials at the time of extension or renewal.	Please be guided by the RFP

SNo.	Page no	Section	RFP Clause	Clause Technical Specification	Bidder's Query	Clarification
1349	Page 136	13.2	Right to Alter quantities	The bank reserves the right, at the time of award of contract and/or during the currency of the contract, to increase or decrease the quantity of goods, licenses, subscriptions, appliances, equipment, services, implementation effort, support services, or any line item covered under the contract by up to twenty five percent (25%) of the quantities specified in the RFP/Contract, without any change in the unit prices, terms and conditions, technical specifications, delivery schedule, warranty obligations, support commitments, or any other contractual conditions. The Bidder/Vendor shall be bound to accept such variation and execute the order at the same rates and on the same terms and conditions as agreed under the contract.	We request that any increase in scope, quantities, quantity of goods, licenses, subscriptions, appliances, equipment, services, implementation effort, support services, or any line item covered under the contract in the RFP be treated as a change request and be priced separately. Any increase shall be undertaken at mutually agreed rates prevailing at the time of such increase.	Please be guided by the RFP
1350	Page 136	13.2	Right to Alter quantities	The bank reserves the right, at the time of award of contract and/or during the currency of the contract, to increase or decrease the quantity of goods, licenses, subscriptions, appliances, equipment, services, implementation effort, support services, or any line item covered under the contract by up to twenty five percent (25%) of the quantities specified in the RFP/Contract, without any change in the unit prices, terms and conditions, technical specifications, delivery schedule, warranty obligations, support commitments, or any other contractual conditions. The Bidder/Vendor shall be bound to accept such variation and execute the order at the same rates and on the same terms and conditions as agreed under the contract.	Our commercial quote is based on a minimum committed quantity. A reduction in order size impacts pricing viability. Hence, we request that the minimum committed quantity not be reduced, or that any reduction be done only with mutual consent.	Please be guided by the RFP
1351	Page 142	13.19	Liquidated Damages	If the bidder fails to deliver any or all of the products and/or systems and/or services solutions within the time period(s) specified in the Delivery Schedule or installation, the Bank shall, without prejudice to its other remedies under the Contract, deduct from the Contract Price, as liquidated damages, a sum equivalent to 0.5 percent per week or part thereof of Contract Price subject to maximum deduction of 10% of the total contract value, until actual delivery, installation or performance as per related clauses mentioned in RFP.	Request Bank to amend the LD clause as follows: "Liquidated Damages shall be levied at 0.5% per week of value of the delayed portion of the deliverables, subject to a maximum of 5% of the value of the affected milestone. Delays attributable to the Bank, its agents, third parties, OEM dependencies, force majeure events, site readiness issues, delayed approvals/sign-offs, or reasons beyond the bidder's reasonable control shall be excluded for computation of LD."	Please be guided by the RFP
1352	Page 1	1	Bid Offer Validity (GEM)	30 (Days)	We request you to change this to as per Bid offer validity given by OEMs	Please be guided by the RFP
1353	Page 144	13.17	Order Cancellation	Bank shall serve the notice of termination to the bidder at least 30 days prior of its intention to terminate services without assigning any reasons.	We request Bank if the contract is terminated for convenience ,PSB shall additionally pay to the Bidder for all work done till the date of termination, as well as for the orders already placed with OEMs/Licensors, which orders cannot be cancelled with the OEMs/Licensors, cancellation costs, if any, levied by the OEMs/Licensors, and logistical and administrative expenses, if any, incurred by the Bidder on account of such cancellations, which expenses shall be billed on actuals. Further, if the Bidder is providing any products/goods on opex or lease model, then PSB shall pay the Bidder the residual value of the products.	Please be guided by the RFP
1354	DLP Sheet	Appendix 1A Functional Specification	Section B- CONTENT DETECTION & CLASSIFICATION, Point 27-	Provides the capability to automatically add headers, footers or watermarks in Office documents as well as PDF documents when users classify them.	Please change to "Provides the capability to automatically add headers, footers or watermarks in Office documents hen users classify them." this will help in broader participation	Please be guided by the RFP
1355	DLP Sheet	Appendix 1A Functional Specification	Section B- CONTENT DETECTION & CLASSIFICATION, Point 35-	The solution should have levels of actions Force, Warn, Log & Ignore classification and must provide the details of the user who classified the file and if any user is allowed to change classification, this change should be logged.	Specific OEM point	Please be guided by the RFP
1356	DLP Sheet	Appendix 1A Functional Specification	Section B- CONTENT DETECTION & CLASSIFICATION, Point 41	Administrators should be able to customize the threshold for suggestions that are based on AI/ML confidence levels, so that suggestions are made only when AI/ML is more than X% confident of a particular label.	Specific OEM point	Please be guided by the RFP
1357	DLP Sheet	Appendix 1A Functional Specification	Section C- ENDPOINT DLP, Point 74	DLP solution should provide version details which can be used with Bank's Network Access Control (NAC) solution for compliance.	Request to remove this point as DLP do not contrbute pro-active posture assesment of endpoint health	Please be guided by the RFP