Sr. No.	RFP page No.	RFP Clause No.	Existing Clause	Query / Suggestions	Accepted (Y/N)	Clarification
1	60	gibility Crite	Bidder should have experience of minimum five years in providing the Deception Technology Software Solution/services.	Kindly please relax this clause as- Bidder/OEM should have experience of minimum five years in providing the Deception Technology Software Solution/services.	Accepted	OEM experience may be considered subject to valid authorization letter and supporting documents. Clause stands revised as "Bidder/OEM should have experience of minimum five years in providing the Deception Technology Software Solution/services".
2	98	Illustration Table	% D	What is the " D" mentioned in the E & F Coloumn	Explained	D' stands for Final Price (INR) in reverse auction, 'E' stands for min price and 'F' stands for max price. The prices
3	106	4(g)	Uptime Penalties for SLA uptime where services are impacted	Why the penalty clauses are very high can be reconsidered with minimum values	Rejected	No change. SLA penalty clauses will remain as per RFP to ensure strict

Sr. No.	RFP page No.	RFP Clause No.	Existing Clause	Query / Suggestions	Accepted (Y/N)	Clarification
4			Suggetions	The deception module must include a custom threat intelligence generation capability derived from interactions with the decoys, providing actionable data on attacker IPs including the following: - Attacker Engagement Time - If the attacker IP is a VPN - If the attacker IP belongs to Tor - Must provide malicious score of the attacker IP - Abuse velocity of the attacker IP - If the attacker IP is an active VPN IP - If the attacker IP is an active tor IP - If the attacker IP was involved in recent abuse behavior - If the attacker IP is a botnet - If the attacker IP is a frequent attacker - If the attacker IP is involved in high risk attacks - If the attacker IP is a security scanner - If the attacker IP belongs to a trusted network - If the attacker IP uses dynamic or shared connection - If the attacker IP belongs to a mobile device - If the attacker IP is a crawler - Information like country, city, latitude,	Rejected	Deception module must include provision for custom threat decoys. Incorporated in Appendix-C (Technical Specifications). The mentioned capabilities are expected to be the basic capabilities.

Sr. No.	RFP page No.	RFP Clause No.	Existing Clause	Query / Suggestions	Accepted (Y/N)	Clarification
5	64	Appendix C	Suggetions	The module must provide an recommendation engine for automated rule creation that can be integrated with the SOAR platform, enabling real-time blocking and response actions against attacker IPs based on threat intelligence gathered through decoy engagement. For example, if the IP has a certain malicious score, the IP is to be blocked for 1 day.	Rejected	The Bank may, at its sole discretion, consider inclusion of the point post discussion and approval of the Committee; however, the Bank shall not be under any obligation to incorporate the same
6	64	Appendix C	Suggetions	The solution must feature a customized Generative AI Model that is dedicated to the threats observed within Client's decoys, enabling security analysts to interact with the system and receive contextual insights, suggestions, and investigative support.	Rejected	The Bank may, at its sole discretion, consider inclusion of the point post discussion and approval of the Committee; however, the Bank shall not be under any obligation to incorporate the same
7	64	Appendix C	Suggetions	The data collected from the decoys must provide information on TTPs of the attackers and analysts should be able to provide analysis of the attack using the customized Generative AI Model.	Rejected	The Bank may, at its sole discretion, consider inclusion of the point post discussion and approval of the Committee; however, the Bank shall not be under any obligation to incorporate the same
8	64	Appendix C	Suggetions	The solution must provide Tactics, Techniques, and Procedures (TTP) mapping for all attacks in the decoys using the MITRE ATT&CK Framework, including deep-dive contextual information on each observed technique, such as associated threat actor behaviors, technique descriptions, affected systems, and detection/recommendation guidance within the customized Generative AI Model, enabling comprehensive threat understanding and alignment with industry-standard frameworks.	Rejected	The Bank may, at its sole discretion, consider inclusion of the point post discussion and approval of the Committee; however, the Bank shall not be under any obligation to incorporate the same

Sr. No.	RFP page No.	RFP Clause No.	Existing Clause	Query / Suggestions	Accepted (Y/N)	Clarification
9	64	Appendix C	Suggetions	The Generative AI must not be a typical chatbot that connects with tools like ChatGPT/Gemini via API and gives responses.	Rejected	The Bank may, at its sole discretion, consider inclusion of the point post discussion and approval of the Committee; however, the Bank shall not be under any obligation to incorporate the same
10	64	Appendix C	Suggetions	The Generative AI model must allow security analysts with the investigations for threats in the SOC by effectively analyzing the existing Deception Data generated.	Rejected	The Bank may, at its sole discretion, consider inclusion of the point post discussion and approval of the Committee; however, the Bank shall not be under any obligation to incorporate the same
11	64	Appendix C	Suggetions	The Generative AI model must not connect to any API over the cloud. It must be deployed on-prem in a appliance provided by the OEM.	Rejected	The Bank may, at its sole discretion, consider inclusion of the point post discussion and approval of the Committee; however, the Bank shall not be under any obligation to incorporate the same
12	72	62	The solution should integrate with existing SIEM, SOC and other security solutions out of the box with or without custom parser. Bi-directional integration with SIEM solutions deployed in SBI	Kindly confirm which existing security solutions (SIEM, EDR, SOAR, firewalls) the deception platform must integrate with.	Explained	The solution is expected to provide out-of-the-box integration capabilities with industry-standard SIEM, SOC, EDR, SOAR, and firewall solutions etc. The Bank will provide details of the existing solutions to the selected bidder at the time of implementation. The implementation should be either
13	63	1	The proposed and presented solution should have capability to host Centralized Management & Control System and should have the capability to host off-premises architecture for multiple SBI Data centres / locations.	Could you please confirm on the deployment model, Is it an on-premise deployment, or is a SaaS/Cloud-based deployment also acceptable?	Explained	The Centralized Management & Control shall be deployed strictly in a Cloud/SaaS-based model. On-premise deployment will not be considered. The Cloud deployment must comply with the Bank's security, regulatory, and data residency requirements, and the

Sr. No.	RFP page No.	RFP Clause No.	Existing Clause	Query / Suggestions	Accepted (Y/N)	Clarification
14	29	28	System integration testing will be followed by user acceptance testing, plan for which has to be submitted by Service Provider to the Bank. The UAT includes functional tests, resilience tests, benchmark comparisons, operational tests, load tests etc. SBI staff / third Party vendor designated by the Bank will carry out the functional testing. This staff / third party vendor will need necessary on-site training for the purpose and should be provided by Service Provider. Service Provider should carry out other testing like resiliency/benchmarking/load etc. Service Provider should submit result log for all testing to the	What is the detailed process and acceptance criteria for UAT? Will the Bank provide test cases or should the bidder propose them?	Explained	The detailed UAT process and acceptance criteria will be finalized jointly between the Bank and the selected Service Provider prior to commencement of UAT, in line with the requirements defined under Appendix-I of the RFP. The Service Provider shall be responsible for preparing and proposing detailed UAT test cases, including functional, resilience, benchmark, operational, and load test scenarios, for Bank's review and approval. The Bank and/or its designated third-party vendor will validate and execute the approved test cases. Issuance of the UAT sign-off letter by the competent authority shall be subject to successful completion of all agreed test cases to the Bank's
15	88	10 (Scalability requirements	Hardware should have support capacity of minimum 3 lac endpoints, 144 VLANs & 190 decoys (and not limited to).	Would it be possible to expand on this point as it implies over 2,000 endpoints per VLAN and more than 1,500 endpoints per decoy, which may not be realistic for effective segmentation or deception coverage. We request that the Bank revise the requirement to reflect actual numbers.	Rejected	The requirement specified in the RFP represents the minimum scalability benchmark expected from the proposed hardware to ensure future readiness and enterprise-wide coverage. The figures provided (3 lakh endpoints, 144 VLANs, and 190 decoys) are indicative upper limits and do not imply a fixed ratio of endpoints per

Sr. No.	RFP page No.	RFP Clause No.	Existing Clause	Query / Suggestions	Accepted (Y/N)	Clarification
16	91	18	OEM Training to the Bank's team on deployment, administering, monitoring, supervising, report generation and usage management of the solution should be provided yearly to minimum 10 officials. Ii. The details of the training are to be provided by the Bidder and shall be subject to evaluation by the Bank to ensure that all the	Is the training required on-premise, in-person and instructor led? Or would remote training be acceptable? The RFP clause says 'minimum 10 participants' for the training. What would be an expected number of attendees for the training?	Explained	The training is expected to be on-premise/off-premise but in-person. Remote training modules may be considered only as supplementary, subject to the Bank's approval. As per the RFP, the minimum number of participants shall be 10, while the maximum number of attendees will be decided at the sole discretion of the Bank depending on operational
17	72	56	Remediate the exposed credentials at endpoints to decrease attack surface available for an attacker in the enterprise	Kindly clarify if surfacing the attack surface on endpoints (such as cached credentials/vulnerabilities) is the goal	Explained	The intent of the clause is to ensure that the solution is capable of identifying and remediating exposed credentials or similar artifacts at endpoints, thereby reducing the overall attack surface. While surfacing such exposures (e.g., cached credentials, vulnerabilities, misconfigurations) is an essential capability, the solution must
18	72	59	Solution should be able to identify malware present in network file share drives and web objects (For Eg: JPEG, doc, docx, exe, gif, hip, htm, pdf, png, ppsx, ppt, pptx, qt, rm, rtf, swf, tiff, url, vbs, vcf, xls, xlsx. etc. and any other new formats having vulnerabilities carry potential malware)	We believe this is outside the scope of any deception solution. Kindly confirm if SBI is looking for something like a NAS Scanning Solution.We request you to kindly remove this point	Rejected	The requirement has been included to ensure comprehensive detection capabilities as part of the deception platform's integration with the Bank's broader security ecosystem. While the primary function of the deception solution is not NAS scanning, the solution is expected to be capable of identifying and alerting on malware embedded within network file share drives and web objects, either natively
19	60	5	Bidder should have experience of minimum five years in providing the Deception Technology Software Solution/services.Copy of the order and / or Certificate of completion of the work. The Bidder	**Bidder/OEM** should have experience of minimum **three years** in providing the Deception Technology Software Solution/services.Copy of the order and / or Certificate of completion of the work. The Bidder should also furnish user	Rejected	The clause will be revised as follows: Bidder/OEM should have experience of minimum three years in providing the Deception Technology Software Solution/services.Copy of the order and / or Certificate of completion of the

Sr. No.	RFP page No.	RFP Clause No.	Existing Clause	Query / Suggestions	Accepted (Y/N)	Clarification
20	61	6	The Bidder (including its OEM, if any) should either be Class-I or Class-II local supplier as defined under this RFP.Certificate of local content to be submitted as per	The **Bidder/OEM** (including its OEM, if any) should either be Class-I or Class-II local supplier as defined under this RFP.Certificate of local content to be submitted as per Appendix-G.	Accepted	The clause will be revised as follows: The Bidder/OEM (including its OEM, if any) should either be Class-I or Class-II local supplier as defined under this RFP.Certificate of local content to be
21	61	7	Client references and contact details (email/ landline/ mobile) of customers for whom the Bidder	Client references and contact details (email/ landline/ mobile) of customers for whom the **Bidder/OEM** has executed	Rejected	Only Indian client references will be considered. Global project executions shall not be accepted for meeting this
22			(Start and End Date of the Project to be mentioned) in the past (At least 2 client references are required).Bidder should specifically confirm on their letter head in this	(Start and End Date of the Project to be mentioned) in the past (At least 2 client references are required).Bidder should specifically confirm on their letter head in this regard as per Appendix-N	Rejected	No suggestions provided.
23	61	8	The bidder must possess certification such as ISO 9001, ISO 27001 or similar standards.	The **bidder/OEM** must possess certification such as **ISO 9001/ISO 27001** or similar standards.	Accepted	The clause will be revised as follows: The **bidder/OEM** must possess certification such as **ISO 9001/ISO**
24	61	9	The Service Provider/Vendor/OEM solution having a Gartner Peer Insights Rating of not less than 4.5 will be preferred.Copy of the Valid	Kindly remove this clause	Rejected	In the clause mentioned it is, "preferred" and not the actual criteria for the eligibily.
25	61	12	The bidder, if participating as Channel Partner of any OEM, then OEM should have a support center and **level 3 escalation (highest) located in India.** For OEMs, directly participating, the conditions mentioned above	The bidder, if participating as Channel Partner of any OEM, then OEM should have a support center in India. For OEMs, directly participating, the conditions mentioned above for support center remain applicable.	Rejected	The requirement for the OEM to have a support center and Level-3 (highest) escalation facility located in India is mandatory. Remote or global escalation support will not be accepted. The clause shall remain unchanged.
26	92	1	Payment Terms-Hardware (Hardware Appliance / Server / Other Items etc.)50 % of the cost of the hardware will be paid against proof of delivery of equipment	Hardware Payment-100% against delivery	Rejected	The request for modification of payment terms is not acceptable. Payment terms shall remain as defined in the RFP, i.e., 50% of the cost of the hardware will be paid against proof of delivery of equipment, and the balance

Sr. No.	RFP page No.	RFP Clause No.	Existing Clause	Query / Suggestions	Accepted (Y/N)	Clarification
27	92	2	Payment terms:Software (End Points, Decoys, OS & DB Licenses etc.)-50 % of the cost of the software will be paid against proof of delivery of licenses/software.	Software Payment- 100% against license delivery	Rejected	The request for modification of payment terms is not acceptable. Payment terms shall remain as defined in the RFP, i.e., 50% of the cost of the software will be paid against proof of delivery of licenses/software, and the
29	63	2	The Solution should support the following 4 stages of attack: Before the Attack: Pre- emption (Attack Surface Reduction) The Deception Solution should have the ability to monitor an organization’s attack surface.We kindly request clarification and elaboration on the term "Attack Surface Reduction" During the Attack: Detection (Deceptions, Decoys, Emulations) The Deception Solution should have the ability to easily create and deploy authentic deceptions across all endpoints. After the Attack: Response (Intelligence and Forensics) The Deception Solution should collect the precise forensic intelligence and context needed to understand and act on an incident.	Please clarify: We kindly request clarification and elaboration on the term "Attack Surface Reduction"	Explained	The term “Attack Surface Reduction” refers to the ability of the proposed Deception Solution to identify, minimize, and remediate potential exposures at endpoints and across the enterprise network that could be leveraged by an attacker. This includes, but is not limited to, discovery and management of exposed credentials, unused open ports, misconfigurations, vulnerabilities, and other exploitable artifacts. The intent is to proactively reduce avenues of compromise before an attack occurs, thereby strengthening the Bank’s overall security posture.

Sr. No.	RFP page No.	RFP Clause No.	Existing Clause	Query / Suggestions	Accepted (Y/N)	Clarification
30	64	4	The proposed enterprise deception should not look any different from the SBI network and its related infrastructure. This requirement applies to all decoys, baits, and breadcrumbs. This further entails that the dynamic deception must keep up with the changes happening in the SBI network and implementation of same should be automated and/or manual.	Server sizing for the Deception Solution depends on the number and types of decoys to be created, as different decoy types (e.g., Windows Server 2016, Windows 11, Linux) require different infrastructure and resource allocations. In order to provide accurate sizing and a suitable solution architecture, we kindly request you to share the expected types of decoys to be created on the Deception Solution—such as Windows Server, Linux, etc.	Rejected	The requirement for the deception solution to closely mimic the Bank's network and infrastructure. The details of the Bank's internal network, infrastructure, decoy types, operating systems, or configurations are considered sensitive and shall not be shared at this stage. The bidder is expected to propose sizing, resource allocation, and architecture based on the requirements specified in the RFP and its appendices. The responsibility
31	64	5	The proposed Enterprise deception solutions should scale up cost-effectively to deploy thousands of decoys, while also providing the ability to engage and respond to attacks. It is must that the proposed Solution should provide both near real time scalability and ability to engage and respond to attacks.	As mentioned in the Scope of Work, the total number of decoys is stated to be 190. However, this appears to be contradictory to another clause within the Scope of Work. We kindly request clarification on the exact number of decoys to be deployed, along with their distribution across the infrastructure. This information is essential for accurate planning and solution sizing.	Rejected	As per the Annexure-E, Scope of work, page no. 91, clause no. 13: Limited trial/pilot requirement, initial decoy requirement of 50 is mentioned. As per Annexure-F, page no.94, piont no. 2, the figures provided (3 lakh endpoints, 144 VLANs, and 190 decoys) are indicative upper limits and do not imply a fixed ratio of endpoints per VLAN or per decoy.The requirement specified in the RFP represents the minimum scalability benchmark expected from the proposed hardware and/or software solution having sufficient capacity which could be
32	65	6	The Service Provider/Vendor/OEM must provide all the required hardware, software and system licenses which can support implementation of VMs with multiple operating systems (viz. Windows, Linux, HP-UX, Unix (different flavours of Unix), AIX, and not limited to) server can be	Please clarify: The licenses required to build and deploy the Deception Solution infrastructure (such as platform, console, and related components) will be provided by the Service Provider/Vendor/OEM. However, since the decoys are expected to mimic the SBI network and its related infrastructure, any licenses required for	Rejected	The bidder/Service Provider/OEM shall be fully responsible for procuring and providing all necessary hardware, software, and system licenses required for the implementation of the solution, including licenses for decoy environments, operating systems, and associated tools. The Bank will not provide any licenses or software

Sr. No.	RFP page No.	RFP Clause No.	Existing Clause	Query / Suggestions	Accepted (Y/N)	Clarification
33	66	11	The solution should be able to create decoys for Security solutions (and not limited to) like Anti-Virus, Firewall, IPS/IDS, email gateway security, SIEM etc.	This is OEM specific clause. Hence request to revise this clause as follows: The solution should be able to create decoys for Security solutions (and not limited to) like Anti-Virus, Firewall, IPS/IDS, etc.	Rejected	The requirement to create decoys for security solutions such as Anti-Virus, Firewall, IPS/IDS, email gateway security, SIEM, etc., is not OEM-specific but intended to ensure comprehensive deception coverage across critical security layers. The clause applies to all
34	66	15	Ability to create deception of any web or mobile application to cover attacks on Mobile endpoints connected to Datacentre Servers.	Please clarify: Web or mobile applications will be deploy on Linux or Windows server OR it will be deploy on any other OS.	Rejected	The requirement for creating deceptions of web or mobile applications applies irrespective of the underlying operating system. These applications may be deployed on Linux, Windows, or any other operating systems as per the Bank's architecture and deployment requirements. The
35	67	20	The solution should be able to carry out a session replay of the attack carried out on the decoy for further analysis. The details available in session replay shall be mentioned in Remarks.	The current clause appears to be OEM-specific. Additionally, please note that script-based attacks typically do not display output on the screen, as they are executed in the background. In view of this, we kindly request that the clause be revised to include a packet capture capability, which can log and capture all activities carried out by the attacker. This will ensure comprehensive visibility into the attack behavior, regardless of whether it produces on-screen output. Hence request to revise this clause as follows:	Rejected	As per the Appendix-C, Technical & Functional specification, Page no. 71, point no. 50: "Solution must allow visual dissection of the PCAP traffic and preserve all network traffic to and from the decoys while having the ability to export PCAPs based on a time filter". Packet capture for analysis help is already covered in the point. The requirement to carry out a session replay of attacks on the decoy is essential to ensure thorough post-attack analysis and forensics. This capability is not OEM-specific but is

Sr. No.	RFP page No.	RFP Clause No.	Existing Clause	Query / Suggestions	Accepted (Y/N)	Clarification
36	67	22	The endpoint deception agent should be able to select users/computers on the basis of the following selection criteria (and not limited to): - Process list - Browser history - Installed programs – important files Interesting files - Recent commands - Active TCP connections – OU etc.	The mentioned clause appears to be part of an EDR (Endpoint Detection and Response) solution. Deploying multiple agents on the same endpoint may adversely impact system performance and user experience. In light of this, we kindly request the removal of this clause. Instead, we propose allowing an alternative approach—such as uploading tokens or breadcrumbs to the endpoint—for	Rejected	The functional requirements outlined in the clause are critical to the effectiveness of the deception solution and are not intended to replicate EDR solution or other security products but to enhance deception coverage. While the Bank is mindful of endpoint performance and user experience, any alternative approach proposed must demonstrably meet the same objectives without compromise.
37	70	43	Detections sent to the Sandbox should be visible in console with their results.	We kindly request you to share the required sizing details necessary to design and size the Sandbox Solution alongside the Deception Solution	Rejected	The requirement that detections sent to the Sandbox be visible in the console along with their results is essential to ensure real-time visibility and effective analysis. The sizing details necessary for the Sandbox solution are considered sensitive and will not be shared at this stage. Bidders are expected to independently determine the sizing and
38	71	54	Decoy web applications should be tamper-proof so that it can't get defaced while under attack	The mentioned clause appears to be related to a Web Application Firewall (WAF) solution and may not be applicable to the Deception Solution. Additionally, we would like to highlight that using tamper-proof mechanisms on decoys may limit the ability to effectively track lateral movement by attackers. In deception environments, it is advisable to allow controlled interaction with decoys to monitor attacker behavior and	Rejected	The requirement for decoy web applications to be tamper-proof is critical to ensure that attackers cannot easily deface or compromise decoys, which would undermine their purpose. This clause is not intended to replicate a Web Application Firewall (WAF) but to maintain the integrity and realism of the deception environment. Controlled interactions with decoys for monitoring attacker behavior can still be supported

Sr. No.	RFP page No.	RFP Clause No.	Existing Clause	Query / Suggestions	Accepted (Y/N)	Clarification
39	72	58	Solution should support all flavors of Virtual Servers like Hyper-V, VMware ESX, ESXi, NSX firewall and future variants and containers.	This is OEM specific clause. Hence request to revise this clause as follows: Solution should support all flavors of Virtual Servers like Hyper-V/ VMware ESX/ ESXi/ NSX firewall / future variants and containers.	Rejected	The clause is not OEM-specific but intended to ensure broad compatibility with existing and future virtualization platforms. The solution is expected to support a wide range of virtual server environments such as Hyper-V, VMware ESX, ESXi, NSX firewall, and
41	73	64	The solution should integrate the results with SIEM / SOC. All TTP's should be converted to actionable action for SIEM analysis in SOC.	Solution can integrate with SIEM/SOC solution. All TTP's should converted to actionable action for SIEM is feature of SIEM. Hence request to revise this clause as follow: The solution should integrate the results with SIEM / SOC	Rejected	While SIEM solutions perform correlation and alerting functions, the deception solution is required to process and enrich detected TTPs into actionable intelligence before forwarding them for SIEM analysis. This ensures that the SOC receives structured, context-rich alerts that can be acted upon effectively and in a
42	74	75	The solution must have the ability to reconstruct raw attack data into plain English attack analysis. It must also provide attacker / APT group attribution, mitigation recommendations, MITRE mapping within the user interface for the analyst.	This is OEM specific clause. Hence request to revise this clause as follows: The solution must have the ability to reconstruct raw attack data into plain English attack analysis. It must also provide mitigation recommendations, MITRE mapping within the user interface for the analyst.	Rejected	Attacker/APT group attribution is a critical component of advanced attack analysis and is essential for providing actionable context to the SOC. It is not OEM-specific but an expected capability that enhances the analyst's ability to understand the nature of the threat, anticipate attacker behavior, and implement appropriate mitigation strategies. Removing this requirement
43	93	7	Comprehensive warranty for Products for 03 years. Warranty period will start from the date of acceptance of solution by the Bank. Yearly in arrears and within one month after submission of invoices.	Comprehensive warranty for Products for 03 years. Warranty period will start from the date of acceptance of solution by the Bank. Yearly in advance and within one month after submission of invoices.	Rejected	Warranty payments will be made yearly in arrears to ensure that the Bank disburses payments after verifying satisfactory service delivery. Yearly advance payments are not acceptable as they expose the Bank to undue financial risk and reduce its ability to ensure compliance with warranty

Sr. No.	RFP page No.	RFP Clause No.	Existing Clause	Query / Suggestions	Accepted (Y/N)	Clarification
60	3	1. Schedule of Events - Point 6	Last date and time for Bid submission - Up to 15:00 hrs. on 30.09.2025	We request an extension till 15:00 hrs. on 14.10.2025	Rejected	The last date and time for bid submission, i.e., 15:00 hrs on 30.09.2025, shall remain unchanged. This deadline has been fixed to ensure adherence to the Bank's project schedules and evaluation timelines. Extensions are not permissible as a general rule, as they may affect the fairness and timely execution of the procurement process. However, the Bank reserves the right, at its sole
62	81	Appendix-E - Scope of Work and Payment Schedule - Point 3	Solution should support integration with the Bank's current security and operations management systems like SOC, PIMS, DLP, AD, ITAM, Centralised Key Management System, NAC, AV, Email, EDR, SOAR, TIP and NTP etc (and not limited to).	Kindly confirm kind of use case expected as part of integration with mentioned solutions.	Explained	The integration requirements specified in the clause are intended to ensure that the proposed solution can seamlessly interoperate with the Bank's existing security and operations management systems. The clause is designed to provide flexibility and does not prescribe specific use cases at this stage. Detailed use cases and workflows will be finalized in consultation with the selected bidder during the implementation phase, ensuring alignment with the Bank's
64	93	Appendix-F - Indicative Price Bid	This cost should not be more than X% of the total cost	We request that there be no line-itemwise cap of pricing	Rejected	The RFP clause specifies that the total cost of the specified component should not exceed X% of the overall project cost. It does not impose any restrictions or caps on individual line items. The

Sr. No.	RFP page No.	RFP Clause No.	Existing Clause	Query / Suggestions	Accepted (Y/N)	Clarification
65	95	Appendix-F - Indicative Price Bid - Point 5	Onsite support 16x7 basis, if required, apart from deployment phase.	Request to clarify if onsite support resources to be factored apart from the 2 L2 resources	Rejected	The RFP clause on onsite support 16x7, if required, is meant to be covered within the scope of the existing resources, including the two L2 resources specified for deployment and standard operational and support activities after deployment. No additional onsite resources beyond the specified L2 resources are envisaged. Therefore, separate resource allocation for onsite support is not required at this
66	66	13	Solution should automatically detect and alert scanning attacks and Layer 2 attacks (and not limited to) viz. ARP flood etc.	We request the bank to amend this clause as below. The solution should automatically detect and alert scanning attacks such as IP scan, etc.	Rejected	The original clause is intended to ensure that the solution detects a comprehensive range of threats, including scanning attacks and Layer 2 attacks such as ARP floods. Limiting the scope to only scanning attacks (e.g., IP scans) would reduce the expected
67	69	38	The solution should be able to create spear-phishing decoys to detect targeted spear phishing attempts.	This is not a primary use case of Deception solution. The spear phishing awareness are primarily part of the regular email awareness campaign in the banking vertical. Email Security and Secure Web Gateway (SWG) solutions are used to prevent the phishing attacks. Hence, we request bank to remove this clause.	Rejected	While spear-phishing awareness campaigns and preventive tools like Email Security and Secure Web Gateway (SWG) are important components of an overall security strategy, the purpose of this clause is to enhance detection capabilities through deception technology. Spear-phishing decoys provide an additional layer of
68	72	56	Remediate the exposed credentials at endpoints to decrease attack surface available for an attacker in the enterprise	This is not a primary use case of Deception solution. This is a use case of ITDR solution. Hence, we request bank to remove this clause.	Rejected	While ITDR solutions handle credential remediation, the purpose of this clause is to ensure that the deception solution contributes to reducing the attack surface by detecting misuse of exposed credentials. This enhances the overall security posture by providing real-time detection of attacks leveraging

Sr. No.	RFP page No.	RFP Clause No.	Existing Clause	Query / Suggestions	Accepted (Y/N)	Clarification
70	72	60	The endpoints with Windows OS, deception should be able to detect attempts to access Answer file within the OS for agent-based solution.	We request the bank to amend this clause as below. The endpoints with Windows OS, the deception should be able to detect attempts to access answer file within the OS by creating fake decoy answer files.	Rejected	The clause is intended to ensure that the solution can detect attempts to access the Answer file on endpoints. The method of detection, including whether to use decoy answer files, is left to the bidder's implementation.
71	73	67	Solution should support download of all endpoint deceptive object information in industry standard formats (and not limited to) like JSON,PDF and CSV file etc.	We request the bank to amend this clause as below. The solution should support download of all endpoint deceptive object information in industry standard formats (and not limited to) like JSON and CSV file etc.	Rejected	The clause specifies support for download in industry-standard formats, including JSON, PDF, and CSV, to ensure compatibility with reporting and audit requirements but also mentions "and not limited to," giving flexibility for
72	73	70	Reports should contain charts and be customizable	We request the bank to amend this clause as below. The solutions should provide multiple dashboards natively and should be capable to send all the logs to bank's existing SIEM for SOC team to have a correlated reporting.	Rejected	The original clause is specifically focused on report generation, requiring charts and customization to support data visualization. The request to amend the clause to include multiple dashboards and SIEM integration relates to basic and broader