PRE BID QUERIES RAISED BY PROSPECTIVE BIDDERS WITH BANK'S RESPONSE FOR EOI- NO:SBI/GITC/IT-ATM/2024/2025/49

SL No	EOI Page No	EOI Clause No	Existing Clause	Query / Suggestion	Bank's Response
1	7	Eligibility and Technical Criteria	i. Bid is open to all Bidders who meet the eligibility and technical criteria/scope of work as given in Appendix-B & Appendix-C of this EOI. The Bidder has to submit the documents substantiating eligibility criteria as mentioned in this EOI document. (a) If any Bidder submits Bid on behalf of Principal/OEM, the same Bidder shall not submit a Bid on behalf of another Principal/OEM under the EOI. Bid submitted with options of multiple OEMs shall also be considered Bid submitted on behalf of multiple OEMs. (b) Either the Bidder on behalf of Principal/OEM or Principal/OEM itself is allowed to Bid, however both cannot Bid simultaneously.	Requesting Bank to provide clarifications on the following inputs : a) If multiple bidders bid through the same OEM, then there is a high probability that this bid gets restricted to only one OEM thereby restricting the fair bidding process. Request bank to provide the option of one OEM with one bidder only	as per EOI
2	25	Appendix - B / 3	Copy of the audited financial statement for required financial years. (Certificate from statutory auditor for preceding/current year may be submitted.)	Since our company is not a listed company, we can share this only under a NDA. We request the bank to sign the NDA, so that confidential documents can be shared.	As per EOI.
3	25	Appendix - B / 4	The Bidder should be profitable organization on the basis of profit before tax (PBT) for at least 02 (two) out of last 03 (three) financial years mentioned in para 2 above.	Since this is a niche technology area, we request the Bank to modify this to either 1) " The Bidder should be profitable organization on the basis of profit before tax (PBT) for at least 01 (one) out of last 03 (three) financial years" **OR** 2) "The Bidder should have a positive gross margin for at least 02 (two) out of last 03 (three) financial years"	As per EOI
4	25	Appendix B - Bidder's Eligibility Criteria Point 4	The Bidder should be profitable organization on the basis of profit before tax (PBT) for at least 02 (two) out of last 03 (three) financial years mentioned in para 2 above.	We request Bank to consider relaxing this criteria to: The Bidder should be profitable organization on the basis of profit before tax (PBT) for at least 01 (one) out of last 03 (three) financial years mentioned in para 2 above. This request was considered by Bank in past RFPs for Payment Gateway (SBI/GITC/ePay&PG/2022-23/888) and FRM (SBI/GITC/INB/2022-2023/896)	as per EOI.
5	26	Appendix - B / 5	Bidder must have deployed the proposed solution in at least 3 BFSI clients during the last 5 years and operational to detect the user behavior and device malware related frauds with highest degree of accuracy.	India payment fraud dynamics scale and pace of change is unique globally. SBI being largest bank of India, we are of view that the solution should have been deployed and tested in Indian BFSI Clients. Hence we suggest, the clause to be considered for modification as - "Bidder must have deployed the proposed solution in at least 3 BFSI clients in India during the last 5 years....."	As per EOI.
6	26	Bidder's Eligibility Criteria	Proposed solution must be public cloud based and it must be cloud agnostic. The proposed solution must follow all the compliance of Bank's cloud policy requirements from time to time for the entire contract period	Requesting Bank to provide clarifications on the following inputs : a) Please share the details of the Bank's cloud policy/compliance requirements. b) Please share the reasons to prefer public cloud instead of private. If the reason is capital cost, then hybrid cloud/cloud bursting is an alternative option c) Additionally basis experience, it is suggested that Private clouds are most preferred solutions for the Banking security related solutions. d) Private cloud provides more flexibility (customization according to the Banking business needs and regulations), higher level of controls and data privacy. Also have robust disaster recovery plans and supports legacy applications (please note not all legacy applications) e) Compliance with Sarbanes Oxley, PCI etc., will be much easier in Private cloud.	Please Refer Corrigendum No 1, SL No 7.

SL No	EOI Page No	EOI Clause No	Existing Clause	Query / Suggestion	Bank's Response
7	26	Bidder's Eligibility Criteria	Bidder must have deployed the proposed solution in at least 3 BFSI clients during the last 5 years and operational to detect the user behaviour and device malware related frauds with highest degree of accuracy	Given that behavioral biometrics is a relatively new technology and has so far been adopted primarily by BFSI customers, it would be advantageous to reduce the required client references from three to one. This change would provide an opportunity for make-in-India products to gain traction in the market.. The current clause supports only specific vendor and should be modified as suggested below : "Bidder must have deployed/deploying the proposed solution in at least one BFSI clients in India during the last 5 years and operational to detect the user behaviour and device malware related frauds with highest degree of accuracy"	Please Refer Corrigendum No 1, SL No 8.
8	26	Bidder's Eligibility Criteria S.No. 5	Bidder must have deployed the proposed solution in at least 3 BFSI clients during the last 5 years and operational to detect the user behavior and device malware related frauds with highest degree of accuracy.	**Suggestions - Bidder / OEM** must have deployed the proposed solution in at least 3 BFSI clients during the last 5 years and operational to detect the user behavior and device malware related frauds with highest degree of accuracy.	Please Refer Corrigendum No 1, SL No. 6.
9	26	Bidder's Eligibility Criteria S.No. 5	Proposed solution must be public cloud based and it must be cloud agnostic. The proposed solution must follow all the compliance of Bank's cloud policy requirements from time to time for the entire contract period.	Request the SBI team to share the Cloud policy requirements to ensure compliance.	Relevant portion of Bank's cloud policy will be shared with qualified bidder of RFP in pursuant to this EOI, if any
10	26	5	Bidder must have deployed the proposed solution in at least 3 BFSI clients during the last 5 years and operational to detect the user behavior and device malware related frauds with highest degree of accuracy.	As per the Master Direction of the RBI, behavioral biometrics should be part of the Fraud Risk Management (FRM) system. Given that this is a new-age solution, and it is integratl part of our fraud risk management solution, we request the bank to consider our experience in providing fraud risk management solutions for detecting fraud. We propose the following revised criteria: "The bidder must have deployed the proposed solution or a similar solution for fraud detection in at least three BFSI clients within the last five years. The solution must be operational and capable of detecting user behavior and device malware-related frauds with the highest degree of accuracy."	as per EOI
11	26	8	The Bidder should not have any Service Level Agreement pending to be signed with the Bank for more than 6 months from the date of issue of purchase order.	As per our understanding, here bank to refering to Service Level Agreement pending with State Bank of India Only	Yes.
12	26	Appendix B - Bidder's Eligibility Criteria Point 5	Bidder must have deployed the proposed solution in at least 3 BFSI clients during the last 5 years and operational to detect the user behavior and device malware related frauds with highest degree of accuracy.	Can the listed support documents be provided of present clients of the partner?	No. Bidder on its own capacity should present the document.

SL No	EOI Page No	EOI Clause No	Existing Clause	Query / Suggestion	Bank's Response
13	27	Bidder's Eligibility Criteria	Client reference should state peak tps (transactions per second) handled by the Bidder's solution and it should at least 500 tps and also certify that the bidder is handling more than 2,50,00,000 transactions per month for last 6 months (The period of 6 months should fall anytime in 2023/2024)	Requesting Bank to provide clarifications on the following inputs : a) Please define the details of the peak tps like When and how long the peak occurs or expected. b) What is the expected normal tps? c) What is the expected growth of normal/peak tps in next 3-5 years? d) Please share the details of upstream and downstream IT architecture, Network speed and Latency of the dependent systems	a.) TPS is transaction per second and peak TPS may be considered as peak value touched (maximum value) at any point of time. b.), c.) and d.) As per EOI
14	27	Bidder's Eligibility Criteria	Client references and contact details (email/ landline/ mobile) of customers for whom the Bidder has implemented Behavioral Biometric with risk scoring/data points in India or elsewhere in any country in the past (Start and End Date of the Project to be mentioned). At least 3 client references are required with feedback related prevention and detection rate of fraud with formula and detection rate increase after the implementation of Behavioral Biometric solution. Client reference should state peak tps (transactions per second) handled by the Bidder's solution and it should at least 500 tps and also certify that the bidder is handling more than 2,50,00,000 transactions per month for last 6 months (The period of 6 months should fall anytime in 2023/2024	Given that behavioral biometrics is a relatively new technology and has so far been adopted primarily by BFSI customers, it would be advantageous to reduce the required client references from three to one. This change would provide an opportunity for make-in-India products to gain traction in the market. The current clause supports only specific vendor and should be modified as suggested below : "Client references and contact details (email/ landline/ mobile) of customers for whom the Bidder has implemented Behavioral Biometric with risk scoring/data points in India (Start and End Date of the Project to be mentioned). At least 1 client references are required"	Please Refer Corrigendum No 1, SL No 9.
15	27	10	Client references and contact details (email/ landline/ mobile) of customers for whom the Bidder has implemented Behavioral Biometric with risk scoring/data points in India or elsewhere in any country in the past (Start and End Date of the Project to be mentioned). At least 3 client references are required with feedback related prevention and detection rate of fraud with formula and detection rate increase after the implementation of Behavioral Biometric solution.	As per the Master Direction of the RBI, behavioral biometrics should be part of the Fraud Risk Management (FRM) system. Given that this is a new-age solution, and integral part of our fraud risk management solution, we request the bank to consider our experience in providing fraud risk management solutions for detecting fraud. We proposed to revised this criteria to - "Client references and contact details (email/ landline/ mobile) of customers for whom the Bidder has implemented Behavioral Biometric or Enterprise Fraud Risk Management Solution with risk scoring/data points in India or elsewhere in any country in the past (Start and End Date of the Project to be mentioned). At least 3 client references are required with feedback related prevention and detection rate of fraud with formula and detection rate increase after the implementation of Behavioral Biometric solution."	as per EOI
16	27	10	Client reference should state peak tps (transactions per second) handled by the Bidder's solution and it should at least 500 tps and alsocertify that the bidder is handling more than 2,50,00,000 transactions per month for last 6 months (The period of 6 months should fall anytime in 2023/2024).	We request bank to remove this criteria as TPS load handing majorly depends on the hardware provided by the bank. Our solution is vertical and horizontally scalable, so there will be no challenge in handling mentioned transctions	as per EOI

SL No	EOI Page No	EOI Clause No	Existing Clause	Query / Suggestion	Bank's Response
17	27	Appendix B - Bidder's Eligibility Criteria Point 10	Client references and contact details (email/ landline/ mobile) of customers for whom the Bidder has implemented Behavioral Biometric with risk scoring/data points in India or elsewhere in any country in the past (Start and End Date of the Project to be mentioned). At least 3 client references are required with feedback related prevention and detection rate of fraud with formula and detection rate increase after the implementation of Behavioral Biometric solution. Client reference should state peak tps (transactions per second) handled by the Bidder's solution and it should at least 500 tps and also certify that the bidder is handling more than 2,50,00,000 transactions per month for last 6 months (The period of 6 months should fall anytime in 2023/2024).	Can the listed support documents be provided of present clients of the partner?	No. Bidder on its own capacity should present the document.
18	28	Appendix-B / 13	Maximum API response time of the Proposed Solution of the bidder must be within 150 milli seconds	As per Appendix-C, Point number #30, the maximum API response time is mentioned as 500 ms. Hence this needs to be appropriately corrected and aligned to Appendix-C to 500 ms.Request bank to make the change here.	Please Refer Corrigendum No 1, SL No 1.
19	30	Technical & Functional Specification / B1. Mandatory Functionalities / 3	Proposed solution to configure Bank specific Policies/Rules with validity period	Request Bank to elaborate more on this requirement with example of validity period	Proposed solution to configure Bank specific Policies/Rules with validity period i.e rule/policy with a expiry date/time. The rule to be effective for the given timeframe only.
20	30	Technical & Functional Specification / B1. Mandatory Functionalities / 2	Proposed solution to Revert User Risk Score/ Profile associated with any implemented Policy/ Policies.	Request bank to acknowledge that it means - "That the proposed solution should respond with a risk score for the session/activity for the implemented policy/policies"	Yes.
21	30	Appendix-C	The proposed Solution to support Real time decision making.	Our assumation is solution will provide the realtime score, however decision will be done by the bank intergation appliation. Please confirm our understanding	Yes.
22	30	Appendix-C	Proposed solution to Revert User Risk Score/ Profile associated with any implemented Policy/ Policies.	Can you please explain the policy/policies	Policy means a course of action implemented by an organisation by way of rules/criteria to generate risk score
23	31	Appendix-C	Proposed solution to Integrate and work in sync with Bank's 'Fraud Risk Management Solutions (PRM)'	Can you please share the name of vendor and intergation detail of bank FRM solution ? Can we install our own FRM solution ?	It will be shared with qualified bidder of RFP in pursuant to this EOI, if any. FRM solution is not expected.
24	31	Appendix-C	Proposed solution to support Digital Banking usage pattern detection in Mobile Applications	Can you please elobrate digital banking usage patter detection ?	As per EOI. Digital banking usage patterns means "User's behaviours while using Bank's Mobile App/Digital banking app and profiling the same"
25	31	Appendix-C	Proposed solution to have Artificial Intelligence (AI)/ Machine Learning (ML) capabilities	Can bank provide the access of custimer profile for AI/ML use case ?	No. Proposed solution should have capability to generate AI/ML related use cases based on various parameters solution gathers.
26	31	Appendix-C	Proposed solution to capture Geolocation details (Continent, Country, State/ County, City, location, and ZIP/PIN Code) of the User	This feature requried required user consent to capture the location of mobile user. Please confirm our understanding that this feature work only for the consentted	Yes.

SL No	EOI Page No	EOI Clause No	Existing Clause	Query / Suggestion	Bank's Response
27	33	Technical & Functional Specification / B1. Mandatory Functionalities / 23	Having Repository of 'Virtual Private Network (VPN) and proxy IPs' and proposed solution to update the Repository in real-time.	We understand that the bank has floated this EOI for a "Behavioural Biometric Solution". The requirement mentioned in this point is related to an "IP intelligence solution" and should ideally be addressed by an existing / new solution and should be focused for solving that problem. An AI/ML based solution typically responds with risk indicators like Risky IP, Remote Access Tool etc and data points like Proxy Level, Proxy Type, TimeZone Mismatch, TOR etc, which ultimately helps the bank to identify a risky session/user. Therefore there is no need to create/maintain a large & continually growing IP repository in the system which will eventually becomes a big overhead to manage. Blindly relying on an IP repository would wrongly influence the risk score (IP Poisoning). **We request the bank to amend/remove this clause.**	"IP intelligence solution" is also for part of the proposed solution. As per EOI.
28	33	Technical & Functional Specification / B1. Mandatory Functionalities / 24	Having Repository of 'TOR (The OnionRouting) IPs' and proposed solution toupdate the Repository in real-time.	We understand that the bank has floated this EOI for a "Behavioural Biometric Solution". The requirement mentioned in this point is related to an "IP intelligence solution" and should ideally be addressed by an existing / new solution and should be focused for solving that problem. An AI/ML based solution typically responds with risk indicators like Risky IP, Remote Access Tool etc and data points like Proxy Level, Proxy Type, TimeZone Mismatch, TOR etc, which ultimately helps the bank to identify a risky session/user. Therefore there is no need to create/maintain a large & continually growing IP repository in the system which will eventually becomes a big overhead to manage. Blindly relying on an IP repository would wrongly influence the risk score (IP Poisoning). **We request the bank to amend/remove this clause.**	Proposed solution should able to identify TOR IPs as well. As per EOI.
29	34	Technical & Functional Specification / B1. Mandatory Functionalities / 25	Having Repository of 'Malicious IPs' and proposed solution to update the Repository in real-time.	We understand that the bank has floated this EOI for a "Behavioural Biometric Solution". The requirement mentioned in this point is related to an "IP intelligence solution" and should ideally be addressed by an existing / new solution and should be focused for solving that problem. An AI/ML based solution typically responds with risk indicators like Risky IP, Remote Access Tool etc and data points like Proxy Level, Proxy Type, TimeZone Mismatch, TOR etc, which ultimately helps the bank to identify a risky session/user. Therefore there is no need to create/maintain a large & continually growing IP repository in the system which will eventually becomes a big overhead to manage. Blindly relying on an IP repository would wrongly influence the risk score (IP Poisoning). **We request the bank to amend/remove this clause.**	Proposed solution should able to identify Malicious IPs as well. As per EOI.

SL No	EOI Page No	EOI Clause No	Existing Clause	Query / Suggestion	Bank's Response
30	34	Technical & Functional Specification / B1. Mandatory Functionalities / 26	Having Repository of 'Blacklisted IPs' and proposed solution to update the Repository in real-time.	We understand that the bank has floated this EOI for a "Behavioural Biometric Solution". The requirement mentioned in this point is related to an "IP intelligence solution" and should ideally be addressed by an existing / new solution and should be focused for solving that problem. An AI/ML based solution typically responds with risk indicators like Risky IP, Remote Access Tool etc and data points like Proxy Level, Proxy Type, TimeZone Mismatch, TOR etc, which ultimately helps the bank to identify a risky session/user. Therefore there is no need to create/maintain a large & continually growing IP repository in the system which will eventually becomes a big overhead to manage. Blindly relying on an IP repository would wrongly influence the risk score (IP Poisoning). **We request the bank to amend/remove this clause.**	Proposed solution should able to identify Blacklisted IPs as well. As per EOI.
31	34	Technical & Functional Specification / B1. Mandatory Functionalities / 27	Graphical User Interface (GUI) and Application Programming Interface (API) available to access Indicators of Compromise IP Repository as mentioned in Scope of work	We understand that the bank has floated this EOI for a "Behavioural Biometric Solution". The requirement mentioned in this point is related to an "IP intelligence solution" and should ideally be addressed by an existing / new solution and should be focused for solving that problem. If the Bank does not create any such repositories (As requested in Appendix-C, points 23, 24, 25, & 26) then there would be no need for a GUI / API / File Dump needed to access these 'IP Repositories" **We request the bank to amend/remove this clause.**	"IP intelligence solution" is also for part of the proposed solution. As per EOI.
32	34	Technical & Functional Specification / B1. Mandatory Functionalities / 30	The proposed solution average response time to Bank's application to be within 150 milli seconds and shall not exceed 500 milli seconds..	Since bank has requested a solution on public cloud, it will very difficult to adhere to an average response time of 150 ms(API response). We would request the bank to only keep a maximum API response of 500 ms which is also easily demonstratable.	Please Refer Corrigendum No 1, SL No 2.
33	35	Technical & Functional Specification / B2. Preferred Functionalities / 2	Proposed solution to Integrate with Bank's Customer Relationship Management (CRM) solutions	Since Bank has already highlighted the proposed solution should integrate with the Bank's FRM Solution (PRM), what capability/functionality will be achieved by integrating directly with Bank's CRM. We request the bank to amend/remove this clause.	As per EOI. This is a preferred functionality requirement.
34	35	Technical & Functional Specification / B2. Preferred Functionalities / 4	Proposed solution to support Ring Deployment (Gradual Release to target groups).	Please explain what "gradual releases to target groups" the bank is looking at? Typically banks roll-out the solution to all users of one digital channel at a time. However if the bank decides to roll-out the solution to only one target segment at a time, this will have to be managed at the bank's level.	Bank may opt to roll out the solution in phases or channel wise. Proposed solution should be ready for roll out as per Bank 's requirement.
35	35	Technical & Functional Specification / B2. Preferred Functionalities / 5	Proposed solution to detect "Live" user usage patterns.	Please elaborate what the bank means by "Live user usage patterns". Is the bank implying here that the proposed solution to detect human vs. non-human behaviour?	The statement is elaborated as under: The proposed solution to detect usage pattern of digital channel user in real time while the user is logged in to the digital channel.

SL No	EOI Page No	EOI Clause No	Existing Clause	Query / Suggestion	Bank's Response
36	36	Technical & Functional Specification / B2. Preferred Functionalities / 8	Proposed solution to Custom update the Blacklist IPs/ Whitelist IPs in the Indicators of Compromise IP Repository as mentioned in scope of work	We understand that the bank has floated this EOI for a "Behavioural Biometric Solution". The requirement mentioned in this point is related to an "IP intelligence solution" and should ideally be addressed by an existing / new solution and should be focused for solving that problem. An AI/ML based solution typically responds with risk indicators like Risky IP, Remote Access Tool etc and data points like Proxy Level, Proxy Type, TimeZone Mismatch, TOR etc, which ultimately helps the bank to identify a risky session/user. Therefore there is no need to create/maintain a large & continually growing IP repository in the system which will eventually becomes a big overhead to manage. Blindly relying on an IP repository would wrongly influence the risk score (IP Poisoning). **We request the bank to amend/remove this clause.**	As per EOI
37	36	B3: Service Set-up in India requirement	Already established service set-up in India	**Suggestions -** At the time of award a Service Center should be set in India with resources	as per EOI
38	38	Scope of Work / 1.i	Implement solution to fingerprint Customers based on Behavioral Biometrics parameters, IP Intelligence statistics, device binding etc and conduct Risk Assessment based on the same. The indicative list of parameters to be captured are mentioned in Appendix-H	Please explain what the bank means by "IP intelligence statistics"	IP intelligence statitistics means users's risk score based on detection of TOR IP, Malicious IP, Proxy IP, blacklisted IP, IP reputation etc.
39	38	Scope of Work / 1.ii	Implement Risk & Rule Engine based on customer's usage behavioral parameters and other parameters captured from any Bank's application (INB/YONO/YONO-Lite/Bhim-UPI/AePS/Kiosk/YONO 2.0 etc.) and Transaction acquiring infrastructures (like ATM/POS/eCOM/wearables).	Behavioural Biometric Solution does not work on non-digital channels like AePS, ATM, POS, Wearables etc. as it is technically not possible to collect the end-users behaviour from these listed channels. Hence, we request Bank to remove this requirement for integration with non-digital channels.	As per EOI. This is part of broad (not exhaustive) scope of work not a mandatory eligibility creteria.
40	38	Scope of Work / 1.iv	Support implementation of Adaptive Authentication in Bank's Services/Applications.	Request bank to acknowledge that it means - "The Bank will leverage the existing Authentication Solution to trigger the right Authentication Technique and only Behavioural Insights (Score, Threat Indicator, Risk Factors, data points) are expected from bidder's proposed Solution.	Yes. Behaviour insight along with Risk score and other threat indiacator data points are required to be received from proposed solution in real time API Call for step up/adaptive authentication.
41	38	1. Description of Work	ii. Implement Risk & Rule Engine based on customer's usage behavioral parameters and other parameters captured from any Bank's application (INB/YONO/YONO-Lite/Bhim-UPI/AePS/Kiosk/YONO 2.0 etc.) and Transaction acquiring infrastructures (like ATM/POS/eCOM/wearables).	Can Bank clarify how will they provide customer usage behavioral parameters and other parameters to be captured from Transaction acquiring infrastructures (like ATM/POS/eCOM/wearables)?	As per EOI. It has been kept for future perspective for description of work.
42	39	Scope of Work / 1 (a) Description of work: Genral / 1	The proposed solution should provide emergency failure alternatives for both self-non-availability & dependent non-availability.	Request Bank to elaborate more this requirement with examples - What are self non-availability & dependent non-availability in this case?	The proposed solution should provide emergency failure alternatives for both self-non-availability & dependent non-availability. i.e High availability measures must be in place in solution architecture for any component/sub-component non-availability.
43	39	Scope of Work / 1 (a) Description of work: Genral / 3	Wherever functionalities are not replicable/restricted in non-Production environments, it is Bidders' responsibility to provide simulation to mimic the production functionality which also includes Test data creation.	Request Bank to change this to - "Wherever there is a dependency on Bank's system, Bank would provide the necessary support for test data creation as the solution would be embedded with Banking applications".	As per EOI.

SL No	EOI Page No	EOI Clause No	Existing Clause	Query / Suggestion	Bank's Response
44	39	Scope of Work / 1 (a) Description of work: Genral / 5	Bidder should ensure implementation & management of DevOps process for the proposed solution based on tools recommended by the Bank with no additional cost for its Support, etc.,	Since the proposed Solution is offered as SaaS and hosted on a Public Cloud, the vendor solution typically uses its own tools to manage Devops and will ensure that it meets the security standards of the bank to deliver the agreed SLA. Hence, request bank to remove this requirement on Devops tools to be recommended by the bank.	As per EOI.
45	39	1 (a) Description of Work: General	5. Bidder should ensure implementation & management of DevOps process for the proposed solution based on tools recommended by the Bank with no additional cost for its Support, etc.,	Group-IB already has its own DevOps tools and setup used to support our global customer deployment. We request Bank to remove this clause.	as per EOI
46	40	Scope of Work / 1 (a) Description of work: Genral / 10	Bidder is responsible for customization of sdk and JavaScript to make it compatible with the Bank's Application without any cost to the Bank during the contract period.	Request Bank to share the existing technology stack of the channels listed in Appendix-C	As per EOI.
47	41	Scope of Work / 1 (b) Description of Work: For Behavior Biometrics Solution-Risk engine and device Binding/fingerprinting / c	Apart from reporting, user classification/ Profile information should be stored by the proposed solution in the way and retention period deemed necessary by the Bank.	We suggest the bank periodically extracts the data from the bidder's solution and store it within Bank's existing Data Warehousing Solution from where it can be retained for the necessary period. We request bank to amend/delete this clause.	As per EOI.
48	41	1 (b) Description of Work: For Behavior Biometrics Solution-Risk engine and device Binding/fingerprinting	a. Proposed solution should support both Real-time decisions making, and Event based triggers.	Group-IB solution supports near Real time decision making using Synchronus API integration and also event based triggers, Request Bank to confirm if they also have the same understanding about this capability.	Yes
49	41	1 (b) Description of Work: For Behavior Biometrics Solution-Risk engine and device Binding/fingerprinting	d. Policies/Rules could be applicable either at the Application level or at the Enterprise level.	Group-IB supports Policies/Rules applied at the Application level. Request Bank to remove the application of Rules/Policies at the Enterprise level.	as per EOI.

SL No	EOI Page No	EOI Clause No	Existing Clause	Query / Suggestion	Bank's Response
50	42	Scope of Work / 1 (b) Description of Work: For Behavior Biometrics Solution-Risk engine and device Binding/fingerprinting / h	Device state Parameters (Like Malware (including in memory) Presence, Screen shared, RAT(Remote access tool), Jail Broken, Rooted, etc.,)	Request Bank to elaborate more on "including in memory" with an example.	in-memory malware/ Fileless malware is malicious code that works directly within a computer's memory instead of storing on the hard drive.
51	42	Scope of Work / 1 (b) Description of Work: For Behavior Biometrics Solution-Risk engine and device Binding/fingerprinting / i	Parameters used to define Policies/ Rules should be customizable as per Bank's needs. These Parameters if not readily configurable/available as part of the proposed solution, the same should be captured from the Customer and/or Bank's Applications (RINB/CINB/YONO/YONO-Lite/AePS, Kiosk Banking/FASTag, Bhim-UPI etc.) Including Transaction Acquiring infrastructures (like ATM/POS/eCOM/wearables) and made available for Bank's decision making at no additional cost to the Bank.	Behavioural Biometric Solution does not work on non-digital channels like AePS, ATM, POS, Wearables etc. as it is technically not possible to collect the end-users behaviour from these listed channels. Hence, we request Bank to remove this requirement for integration with non-digital channels.	As per EOI.
52	42	1 (b) Description of Work: For Behavior Biometrics Solution-Risk engine and device Binding/fingerprinting	i. Parameters used to define Policies/ Rules should be customizable as per Bank's needs. These Parameters if not readily configurable/available as part of the proposed solution, the same should be captured from the Customer and/or Bank's Applications (RINB/CINB/YONO/YONO-Lite/AePS, Kiosk Banking/FASTag, Bhim-UPI etc.) Including Transaction Acquiring infrastructures (like **ATM/POS/eCOM/wearables)** and made available for Bank's decision making at no additional cost to the Bank.	Request the bank to clarify if Behaviour Biometrics need to be captured on non digital devices (e.g. ATM or POS) and if yes then how will they provide this data? We require a web platform or mobile application to add .js or SDK to deploy solution.	As per EOI. It has been kept for future perspective for description of work.
53	43	Scope of Work / 1 (b) Description of Work: For Behavior Biometrics Solution-Risk engine and device Binding/fingerprinting / j	Proposed Solution should have the ability to Blacklist and Whitelist: various parameter individually or combination e.g. Users, IPs, Devices etc. Further such blacklisting and whitelisting can also be based on parameters such as Geolocations (Countries), Network Characteristics (Connection Type, Network Reputation, and Traffic Patterns), Transaction Types based on risk level and frequency etc.	Request bank to elaborate more on the Network Characteristics mentioned (Connection Type, Network Reputation, & Traffic Patterns) with examples	As per EOI.
54	43	Scope of Work / 1 (b) Description of Work: For Behavior Biometrics Solution-Risk engine and device Binding/fingerprinting / k	Proposed solution should have the ability to integrate with Bank's Customer Relationship Management (CRM) solution & optimize the Risk Engine/ Models/ Decision making engine automatically.	Since Bank has already highlighted the proposed solution should integrate with the Bank's FRM Solution (PRM), what capability/functionality will be achieved by integrating directly with Bank's CRM. We request the bank to amend/remove this clause.	As per EOI.

SL No	EOI Page No	EOI Clause No	Existing Clause	Query / Suggestion	Bank's Response
55	43	Scope of Work / 1 (b) Description of Work: For Behavior Biometrics Solution- Risk engine and device Binding/fingerprinting / I	Integration with CRM would be through APIs and GUI for handling the cases/ Incident to be provided as part of Integrated Operations Portal.	Since Bank is expecting the proposed solution to integrate with Bank's EFRM Solution(PRM), then it would be more efficient for the fraud analyst to use a single window to manage the cases which is PRM. Using this approach, the fraud analyst would have a single view of the case (i.e. behavioural risk score & insights and transactional details from PRM) instead of shuttling between two consoles. Hence we request the bank to amend/remove this clause.	As per EOI.
56	44	Scope of Work / 1 (b) Description of Work: For Behavior Biometrics Solution- Risk engine and device Binding/fingerprinting / Note iii	Details where Accuracy/ Confidence parameters are involved, the same should be captured by the proposed solution and stored [Ex: Geo Coordinates (Latitude & Longitude)]	We feel that the accuracy/confidence parameters around the network parameters are not relevant to this EOI, as the EOI is focused on Fraud Prevention Solution using Behavioural Biometrics. Also, the accuracy/confidence parameters of the network parameters have no or very low impact on the ability to detect fraud. Hence we request bank to amend / remove this clause accordingly.	As per EOI.
57	44	Scope of Work / 1 (C) Description of Work: For Adaptive Authentication	Adaptive Authentication is the process of Authenticating a customer based on a Perceived Risk level. Adaptive Authentication is also referred to as Risk based Authentication. Proposed Solution should facilitate Adaptive Authentication/ Risk based	Request Bank to acknowledge our understanding - We understand, Bank will leverage the existing Authentication Solution to trigger the right Authentication Technique and only Behavioural Insights (Score, Threat Indicator, Risk Factors, data points) are expected from vendor's proposed Solution.	Yes. Behaviour insight along with Risk score and other threat indiacator data points are required to be receivedf rom proposed solution in real time API Call for step up/adaptive authentication.
58	44	Scope of Work / 1 (D) Description of Work: For Indicators of Compromise IP Repository / i	Proposed solution should have Indicators of Compromise 'IP Repository' with following details. a) Virtual Private Network (VPN) IPs b) TOR (The Onion Routing) IPs c) Proxy IPs d) Malicious IPs e) Blacklisted Ips	We understand that the bank has floated this EOI for a "Behavioural Biometric Solution". The requirement mentioned in this point is related to an "IP intelligence solution" and should ideally be addressed by an existing / new solution and should be focused for solving that problem. An AI/ML based solution typically responds with risk indicators like Risky IP, Remote Access Tool etc and data points like Proxy Level, Proxy Type, TimeZone Mismatch, TOR etc, which ultimately helps the bank to identify a risky session/user. Therefore there is no need to create/maintain a large & continually growing IP repository in the system which will eventually becomes a big overhead to manage. Blindly relying on an IP repository would wrongly influence the risk score (IP Poisoning). **We request the bank to amend/remove this clause.**	As per EOI.

SL No	EOI Page No	EOI Clause No	Existing Clause	Query / Suggestion	Bank's Response
59	45	Scope of Work / 1 (D) Description of Work: For Indicators of Compromise IP Repository / ii	Indicators of Compromise IP Repository' containing above information should be updated in real time basis.	We understand that the bank has floated this EOI for a "Behavioural Biometric Solution". The requirement mentioned in this point is related to an "IP intelligence solution" and should ideally be addressed by an existing / new solution and should be focused for solving that problem. An AI/ML based solution typically responds with risk indicators like Risky IP, Remote Access Tool etc and data points like Proxy Level, Proxy Type, TimeZone Mismatch, TOR etc, which ultimately helps the bank to identify a risky session/user. Therefore there is no need to create/maintain a large & continually growing IP repository in the system which will eventually becomes a big overhead to manage. Blindly relying on an IP repository would wrongly influence the risk score (IP Poisoning). **We request the bank to amend/remove this clause.**	As per EOI.
60	45	Scope of Work / 1 (D) Description of Work: For Indicators of Compromise IP Repository / iii	API/file-dump accessible 'Indicators of Compromise' information should be made available to all Bank services and Applications independently. There should be no limit on the number of queries, applications, etc., which can query this information and Bank won't bear any additional cost for the same.	We understand that the bank has floated this EOI for a "Behavioural Biometric Solution". The requirement mentioned in this point is related to an "IP intelligence solution" and should ideally be addressed by an existing / new solution and should be focused for solving that problem. An AI/ML based solution typically responds with risk indicators like Risky IP, Remote Access Tool etc and data points like Proxy Level, Proxy Type, TimeZone Mismatch, TOR etc, which ultimately helps the bank to identify a risky session/user. Therefore there is no need to create/maintain a large & continually growing IP repository in the system which will eventually becomes a big overhead to manage. Blindly relying on an IP repository would wrongly influence the risk score (IP Poisoning). **We request the bank to amend/remove this clause.**	As per EOI.
61	46	Scope of Work / 1 (E) Description of Work: For Integrated Operations Portal / xiv	Event Management: Including but not limited to Alerts Configuration and Escalation matrix Configuration.	Please elaborate in detail on what is 'escalation matrix configuration' in event management?	The propose solution should have event management capabilities along with capability to generate Alerts in case of breach of any criteria/condition. Futher if alert is pending for defined time period, it must be escalated as per configured escalation matrix in the solution defined by the Bank.
62	47	Scope of Work / 1 (E) Description of Work: For Integrated Operations Portal / xix	'Ring Deployment implementation for all features/services/functionalities through Integrated Operations Portal	Request Bank to elaborate in detail with an example of 'Ring Development for features/services/functionalities'?	Ring deployment is a progressive method of software deployment that reduces risk and enhances system availability.

SL No	EOI Page No	EOI Clause No	Existing Clause	Query / Suggestion	Bank's Response
63	47	(E) Description of Work:	Dashboards and Reports: i. Bidder should be able to provide Dashboards and reports as per the Bank's needs. ii. Dashboards should be able to populate even 'Live Data.' iii. Solution should be able to generate reports in real time as well as scheduled.	Requesting Bank to provide clarifications on the following inputs : a) Please share the current details of the Bank's Data Warehouse architecture. This will help us to optimize the data flow to your downstream systems b) Do you expect the data flow to downstream system on intraday basis or EOD activity? If it's intraday, please share the frequency details	a.) Bidder should be able to provide Dashboards and reports based on data and profiles information collected by the proposed solution. b.)No
64	48	Scope of Work /1 (F) Description of Work: For Parameters to be Captured/ Identified	Fingerprinted data should as far as possible be maintained at the User's Device.	Behavioural Biometric Solution does not store any user's data with user's device. The profiles are maintained at the Application level. Hence we request bank to remove/amend the clause accordingly.	As per EOI.
65	48	Scope of Work /1 (F) Description of Work: For Parameters to be Captured/ Identified	Data management policies of the Bank should be followed.	Request bank to share the data management policies at a high-level.	Relevant portion of data management policy will be shared with qualified bidder of RFP in pursuant to this EOI, if any.
66	48	Scope of Work / 1 (F) Description of Work: For Parameters to be Captured/ Identified / xiv	Biometric Authentication Attempts/Ratio	Request Bank to elaborate in detail with an example of 'Biometric Authentication Attempts/Ratio. If the Bank is using physical biometric to authenticate an user (Face ID on iOS). It cannot be detected by behavioural biometric solution and hence we request bank to remove this clause.	As per EOI.
67	48	Scope of Work / 1 (F) Description of Work: For Parameters to be Captured/ Identified / xv	App Usage Patterns and App Permissions	Request Bank to elaborate in detail with an example of 'App Usage Pattern'	As per EOI.
68	48	Scope of Work / 1 (F) Description of Work: For Parameters to be Captured/ Identified / xvii	Authentication Methods Frequented	Request Bank to elaborate in detail with an example of 'Authentication Methods Frequented'	It means frequently used authentication method by the user
69	48	Scope of Work / 1 (F) Description of Work: For Parameters to be Captured/ Identified / xix	Payments related checks like a. Volume velocity b. Hotlisted cards c. Suspicious bank accounts	Request Bank to elaborate in detail with an example of 'Payment related checks'	It means payment related rules for velocity checks, blacklisted cards/bank accounts/merchants etc.
70	48	Scope of Work / 1 (F) Description of Work: For Parameters to be Captured/ Identified / xx	Privilege escalation attempts.	Request Bank to elaborate in detail with an example of 'Privilege escalation attempts'	Privilege escalation means gaining illicit access of elevated rights, permissions, entitlements, or privileges beyond what is assigned for an identity, account, user, or machine.

SL No	EOI Page No	EOI Clause No	Existing Clause	Query / Suggestion	Bank's Response
71	48	Scope of Work / 1 (F) Description of Work: For Parameters to be Captured/ Identified / xxi	Transmission of sensitive information in readable form	Request Bank to elaborate in detail on what is expected here with an example	Please Refer Corrigendum No 1, SL No 3.
72	48	Scope of Work / 1 (F) Description of Work: For Parameters to be Captured/ Identified / xxii	User enumeration attempts.	Request Bank to elaborate in detail with an example of 'User enumeration attempts'	Enumeration is the process of systematically probing a target for information by the attacker/hacker.
73	48	Scope of Work / 1 (F) Description of Work: For Parameters to be Captured/ Identified / xxiii	Parameter manipulation attempts	Request Bank to elaborate in detail with an example of 'Parameter manipulation attempts'	Parameter tampering is a form of web attack that involves manipulating or interfering with the application business logic that is exchanged between client and server to alter application data, such as user credentials, permissions, and price information.
74	48	Scope of Work / 1 (F) Description of Work: For Parameters to be Captured/ Identified / xxiv	Passwords figuring in data breaches	Request Bank to elaborate in detail with an example of 'Passwords figuring in data breaches'	Please Refer Corrigendum No 1, SL No 4.
75	48	1 (F) Description of Work: For Parameters to be Captured/ Identified	xxi. Transmission of sensitive information in readable form	Can the bank expand the type of 'sensitive information' that should be captured in readable form?	Please Refer Corrigendum No 1, SL No 3.
76	49	Scope of Work / 1 (F) Description of Work: For Parameters to be Captured/ Identified / xxx	The proposed solution shall support the Bank's Web/mobile applications to obtain the customer consent to capture the behavioral biometric data parameters. Only after the consent of the customer, shall the solution capture & process users' behavioral biometric data.	The consent from the customer is implicit and its technically not feasible to turn on or turn-off the JS/SDK for a specific user. Hence we request bank to remove the clause.	As per EOI.
77	49	Scope of Work / 1 (F) Description of Work: For Parameters to be Captured/ Identified / xxxi	If due to Denial of permissions by Customers, certain Data are unable to be captured then the same must be recorded and customer preference should be stored.	The consent from the customer is implicit and its technically not feasible to turn on or turn-off the JS/SDK for a specific user. Hence we request bank to remove the clause.	As per EOI.
78	49	Scope of Work / 1 (F) Description of Work: For Parameters to be Captured/ Identified / xxxii	Customer consents have to be captured without fail, cases of non-capture of customer consent on account of any technical reason(s) will have to be addressed and resolved within a fixed minimum period.	The consent from the customer is implicit and its technically not feasible to turn on or turn-off the JS/SDK for a specific user. Hence we request bank to remove the clause.	As per EOI.

SL No	EOI Page No	EOI Clause No	Existing Clause	Query / Suggestion	Bank's Response
79	50	Scope of Work / 1 (G) Description of Work: For Profiling	Friction Percentage per Customer [(Number of Challenges/ Number of Logins Attempted) *100]	We believe, the friction percentage described here is more related to an authentication platform. Any behavioural biometric solution is like an add-on fraud risk solution which integrates with Bank's EFRM Solution and the metrics for a Fraud Prevention Solution are different like Alert Rate, Detection Rate, GTF ratio; hence this metric shall not be applicable and we request Bank to remove this clause.	As per EOI.
80	50	Scope of Work / 1 (G) Description of Work: For Profiling	When the number of Customer Interactions (Ex: Login Attempts) is greater than or equal to 5, then the overall 'Customer Risk Profiling' and 'Individual Parameters (Captured by the proposed solution)' should have an accuracy greater than 99%. Any deviation would attract Penalty.	Please elaborate on this point.	As per EOI.
81	51	Scope of Work / 1 (H) Description of Work: For Infrastructure / C	Recovery Time Objective (RTO) & Recovery Point Objective (RPO) of the proposed solution should be as per Performance metrics defined by the Bank.	Request bank to share the expected performance metrics on RPO & RTO	It will be shared with qualified bidder of RFP in pursuant to this EOI, if any.
82	51	1 (H) Description of Work: For Infrastructure	d) All Information on assets, incidents, changes, Vulnerabilities etc., should be tracked by the Bidder and reported to the Bank.	Since the infrastructure is provided in Public Cloud request Bank to provide the reason for tracking and sharing the changes on assets? Also request Bank to advice on the frequency of sharing such reports - Monthly/quaterly.	as per EOI.
83	52	Scope of Work / 2 / Integration requirements	Proposed solution should facilitate capturing of usage patterns associated with Bank's Acquiring Infrastructure like ATM/ POS/ eCOM/ Wearables etc.	Behavioural Biometric Solution does not work on non-digital channels like AePS, ATM, POS, Wearables etc. as it is technically not possible to collect the end-users behaviour from these listed channels. Hence, we request Bank to remove this requirement for integration with non-digital channels.	As per EOI. Requirement is Technically possible to read the behaviour of customer who visit ATMs based on ATM ID/POS etc carries through the transaction, Frequent withdrawal of amount etc., can be used for profiling the customer. Basis alerts can be generated any deviation occurs.
84	52	Scope of Work / 2 / Integration requirements	On boarding of the customer	As per point #14 of Appendix -B (page #28/66) and technical specification in Appendix-C; the bank requires a solution for Account Take Over & Social Engineering Scams and not for Account On-boarding fraud detection. Can the bank please clarify on this. If this EOI is for Account Take Over & Social Engineering Scams, then we request bank to remove the Account on-boarding requirement from this section.	As per EOI. Proposed solution should have the capability and covers account on-boarding frauds also.
85	52	Integration requirements	Proposed solution should facilitate capturing of usage patterns associated with Bank's Acquiring Infrastructure like ATM/ POS/ eCOM/ Wearables etc.	Request Bank to advice on how they will provide such user patterns? What format and what collection method - APIs?	It has been kept for future perspective for integration requirements.
86	53	Scope of Work / 2 / Integration requirements /b.	The Proposed Solution should be Architected in a way to maintain Single Risk Profile for Customers across the Bank (Which would involve Data Synchronization, API calls, Integration with Enterprise Fraud Risk Management System and passing of proposed solution's captured behavioral & other data to FRM through Channel application). However, At its discretion, Bank may choose the integration approach and choose to deploy common profile across Bank's Applications or implement Bank's application specific profiles.	Request Bank to elaborate more on what is common profile and application specific profile in this "*At its discretion, Bank may choose the integration approach and choose to deploy common profile across Bank's Applications or implement Bank's application specific profiles*" with an example	As per EOI. Application specific profile is one profile per application i.e. two different profiles may exists for Internet Banking and UPI for one customer. Common prifle is one profile per customer across various channel application.

SL No	EOI Page No	EOI Clause No	Existing Clause	Query / Suggestion	Bank's Response
87	53	Integration requirements	Proposed Solution should support working in complementary with the existing Fraud Risk Management solution i.e., Proposed Solution should be able to work as both Upstream and Downstream systems with Bank's Enterprise Fraud Risk Management Solution along with Bank's other web, mobile and payment/acquiring Infra/Applications.	Can the bank share the Fraud and Risk Management Platforms used across applications as mentioned in page 52 (Corporate Banking, Retail Banking, YONO, BHIM SBI Pay)	It will be shared with qualified bidder of RFP in pursuant to this EOI, if any.
88	54	Integration requirements	Integration of Risk Engine with existing Bank's systems - d. Integration with PRM would be in combination of Messaging formats and Integration methods mentioned below, Messaging Format: JSON, XML, cdif etc., Integration Methods: KAFKA, TCP/ IP, Message Queue, APIs etc	Request Bank to advice if they are fine some additional methods for integraiton methods such as RabbitMQ which support JSON APIs as well.	as per EOI
89	54	Integration requirements	e. Proposed solution should support Data exchange with Bank's systems in a scheduled way, in Batches, in Real time; any Utility required for Data exchange should be part of proposed solution. Bank if desired, may use tools like Oracle Golden Gate for Data exchange.	Group-IB solution supports data exchange in real time using APIs. Request Bank to advice on the need of scheduled or batch shairng of data or request them to make it optional.	as per EOI
90	55	Scope of Work / 2 / Integration requirements / c)	Any security advisory issued by the Bank, Regulator or Government Agencies which may involve vulnerability(eg. Log4j) in or risk arising on account of proposed solution need to be complied within the time limit as required by the Bank, and any deviation from such compliance will not be acceptable.	We believe, this requirement is related and applicable to a solution hosted on an on-prem setup. Since Bank has indicated the proposed solution should be on a public cloud, this clause may not be applicable. Hence we request bank to remove this clause.	As per EOI.
91	55	Scope of Work / 3 / Performance and Scalability Requirements / d)	For any functionality (Risk Scoring, threat analysis, processing captured patterns/data etc.), solution's response time to the Bank's Application should not exceed 150 ms on an-average.	As per Appendix-C, Point number #30, the maximum API response time should be 500 ms. We request the bank to make the change here accordingly.	Please Refer Corrigendum No 1, SL No 5.
92	55	Scope of Work / 3 / Performance and Scalability Requirements /g)	Capacity planning for the proposed solution is to be ensured by the Bidder on an ongoing basis and Utilization parameters like Memory, CPU, Storage should be kept below 60% during the Contract period. Related capacity utilization reports must be submitted to the Bank regularly and on- demand basis.	We believe, this requirement is related and applicable to a solution hosted on an on-prem setup. Since Bank has indicated the proposed solution should be on a public cloud, this clause may not be applicable. Hence we request bank to remove this clause.	As per EOI.
93	57	Scope of Work / 3 / Performance and Scalability Requirements	The amount of time taken from the point when Bank's system/application initiates request to the proposed solution, till the final response is received from the proposed solution againt the request, back to the Bank's System/application is referred to as 'response time' of the proposed solution. Within the proposed solution, when intended functionality is having dependency with multiple/other systems, computational time taken by the other dependent systems would be considered as part of the 'response time' of the proposed solution.	The response time for the API call depends on a number of factors beyond the control of behavioural biometric solution e.g.: network latency etc. It would be more appropriate to calculate the response time as the time taken from the time the behavioural biometric solution receives a request and correspondingly responds. We request Bank to change the definition of "Response time" to "The amount of time taken from the point when the Behavioural Biometrics Solution receives a request , till the time a response is sent."	As per EOI.
94	61	Appendix - F	Value of Work Order (In Lakh) (only single work order)	This is a confidential information protected under NDA with our clients and cannot be disclosed. PO with redacted information can be shared instead. Please advise if this is OK with the bank.	As per EOI.

SL No	EOI Page No	EOI Clause No	Existing Clause	Query / Suggestion	Bank's Response
95	62	Appendix - G	Certificate of Local Content	We understand that this certificate is not applicable for 'Non-Local Supplier'. Please confirm.	As per EOI.
96	-	-	Hardware requirement	For HW sizing/price recommendations. Please provide following details. The hardware and infrastrcuture requirements will help in arriving at TCO. Total Users of the AML system: Concurrent Users: Total Customers: Total Accounts: Total Transactions per day or per month(across all areas monitored under AML compliance):	It will be shared with qualified bidder of RFP in pursuant to this EOI, if any.
97	-	-	-	Kindly confirm that bank will provide the hardware and database required	No
98	38 to 59			As part of this EOI response, Is the bidder expected to respond with comments to each of the points listed under Scope of Work from Pages #38 to #57?	Not required for Scope of Work.
99	page 36	Appendix-C	Proposed solution to Visualize ‘User access Geolocation’ in Maps with interactive Drill down options	please correct our assumation to use the API from the bank system for geoloaction map . Map view, we generally recommended google API and bank has to provide the relvant MAP view access for this requirement . Please confirm	Assumption is not correct. Bank will not provide any API. Proposed solution should have its own and capture geolocation & Map view.
100		Bidder’s Eligibility Criteria	Suggestion	We request the bank to modify the eligibility criteria to include behavioral biometric solutions from Made-in-India OEMs. This adjustment aligns with government and MEITY policies promoting "Made in India" solutions.	as per EOI and appropriately covered in EOI for Make-in-India clause.
101		General		Is sub-contracting permitted in this EOI bid?	No.