Annexure II

	Reply to Prebid queries for RFP Reference Bid No – GEM/2024/B/4927595 Date: 13th May 2024 (Request for Proposal for Selection of service provider for Breach and Attack Simulation).						
S.No	**Page No**	**Point/Section**	**Category**	**Clarification point as stated in the tender document**	**Comment/ Suggestion/ Deviation**	**Banks Reply**	**Further details**
1	63	2.13	Scope of work	The proposed BAS solution should be able to conduct the simulation on DC, DR and other infrastructure of the bank.	Please help us with exact number of zones and all the infrastructures bank wish to have BAS solution conduct simulation	No Change	Kindly refer RFP for scope of work.

2	71	13.1.5	Scope of Work (Technical Requirements)	The proposed solution should have the ability to create new attacks by integrating samples collected or sourced from other platforms without OEM intervention.	New attack patterns, tools and behaviours should be constantly tracked by the BAS solution vendor and update them in the BAS solution. Instead of having that dependency on creating new attack by integrating samples. Hence we request you to please change it to below: The proposed solution should have the ability to create new attacks by integrating samples collected or sourced from other platforms without OEM intervention. The proposed solution OEM's should have native and in-house Cyber Threat Intelligence feeding BAS solution ascertained by a 3rd party Research firm (e.g. Forrester or Gartner). OEM should also have native and inhouse Incident Respose feeding BAS solution.	No Change	As per RFP Document.
3	72	13.1.16	scope of work	The proposed solution should have the ability to add and run, any zero day global critical attack in a threat library in maximum time of 24 hrs from the reported time of exploit. Further, response action should be available to remediate the threats in Realtime	Timelines are not fixed for any critical attacks. Timelines to add into the library cannot be fixed within 24hours. We request you to please change it to below so that bank can get real world threat actor behavior, payload detils etc. : The proposed BAS solution should have a native and in-house Incident Response (IR) feeding BAS solution ascertained by a 3rd party Research firm (e.g. Forrester or Gartner)	No Change	As per RFP Document.

4	**76**	13.1.61	Scope of Work	Bidder should be able to check any outbound flows of data / critical information, outlined by bank, during simulation. Such simulation should cover exfiltration methods such as SFTP, removable media, on various cloud services like Gdrive etc	The key to any simulation is to test data exfilteration independeint of any software applications. Hence we request you to please change it to below: Bidder should be able to check any outbound flows of data / critical information, outlined by bank, during simulation. Such simulation should cover exfiltration methods independent of any software applications.	No Change	As per RFP Document.
5	77	13.1.70	Scope of Work	Service provider should measure the time to detect and respond the attack simulation.	Responding to an attack is beyond a BAS soution and hapens outside of the BAS tool hence there will not be ways to measure time to detect and respond. We request you to remove this specification.	No Change	As per RFP Document.
6	77	13.1.71	Scope of Work	Bidder should be able to perform attack simulation by exploiting missing patches and highlight issues pertaining to the same.	Simulation of attack is not an alternative to patch management but its a way to to test if the absense of a patch can be exploited. Hence we request you to please change it to below: Bidder should be able to perform attack simulation by exploiting the known CVE's and highlight issues pertaining to the same.	No Change	As per RFP Document.
7	33	Point no C.6	Eligibility Criteria	The proposed solution must be compliant to all the extant government and regulatory guidelines in India, which includes guidelines issued by RBI and CERT-In.	We request to please clarify and eleborate the exact guidelins for regulators.	No Change	As per RFP Document.

8	33	Point no C 6	Eligibility Criteria	The proposed solution must be compliant to all the extant government and regulatory guidelines in India, which includes guidelines issued by RBI and CERT-In.	We request to please clarify and eleborate the exact guidelins for regulators.	No Change	As per RFP Document.
9	33	Point D.1	Eligibility Criteria	The proposed BAS solution should have been implemented by the bidder / OSD / authorized channel partner of OSD in at least two Commercial Banks / Financial Institutions / Govt. Organizations in India in the last 5 years.	BAS Solutions are still in being adopted by PSU's and government entities. But few larger enterprises are already matured. Hence we request you to please change it to below: The proposed BAS solution should have been implemented by the bidder / OSD / authorized channel partner of OSD in at least two Commercial Banks/ Large Enterprises / Financial Institutions / Govt. Organizations in India in the last 5 years.	No Change	As per RFP Document.
10	35	Technical Bid evaluation point no 1	Eligibility Criteria	The number of Breach attack simulation (BAS) services proposed to the Bank and rendered by the bidder to the commercial banks/ Financial Institutions / Govt. Organizations in India in last 5 years (as on RFP date)# . Only solution proposed by the bidder to the Bank shall be counted.	Large system integrators build their capabilities on the platform or technology space and not on particular product. Hence we request to change it to below: The number of Breach attack simulation (BAS) services proposed to the Bank and rendered by the bidder to the commercial banks/ Financial Institutions / Govt. Organizations in India in last 5 years (as on RFP date)# . Any BAS solution proposed by the bidder to the references provided.	No Change	As per RFP Document.

11	NA	NA	scope	The proposed BAS solution should have native and in-house Cyber Threat Intelligence feeding BAS solution ascertained by a 3rd party Research firm (e.g. Forrester or Gartner)	BOB should not be dependent on any thrid party or any other threat intel feeds for BAS solution. Althought it should have capability to integrate but should ask for OEM's capability to have native and inhouse threat intel feeds feeding BAS solution that too those shold be ascertained by 3rd Party research firms like gartner and forrester to get the assurance of the presense and quality of feeds to test in BOB environment.	NOT APPLICABLE	NOT PART OF THE RFP
12	NA	NA	scope	The proposed BAS solution should have a native and in-house Incident Response (IR) feeding BAS solution ascertained by a 3rd party Research firm (e.g. Forrester or Gartner)	Its not only about threat intel feeds, its also about the threats which are detected by the OEM's IR consultants on the ground those feeding the BAS tool to feed the real world behaviour of a threat actor which can be then simulated in BOB environment which might not be published yet should be available with BOB for testing their environment.	NOT APPLICABLE	NOT PART OF THE RFP
13	NA	NA	scope	The proposed solution should have a native and in-house world class Red Team Practice feeding BAS.	BAS is about testing testing the efficacy of your security environment by simulating real-world cyber attacks. Real world attacks come from IR, Red Teams who see and simulate such attacks. Hence we request you to have this specification so that BOB can get the new insights to test the environment.	NOT APPLICABLE	NOT PART OF THE RFP
14	NA	NA	scope	The proposed BAS solution should demonstrate evidence of production of adversary behaviors based on Advanced Persistent Threat (APT) intrusion sets before public disclosures	This is really important to know the threat actor before public disclosures as any one can become a victim of such behaviors hence we request BOB to add this in to the specification.	NOT APPLICABLE	NOT PART OF THE RFP

15	NA	NA	scope	The proposed BAS solution should demonstrate ability to pivot from embedded and native Threat Intelligence database to BAS dashboard	This is a very basic requirement to navigate easily from embedded Threat Intel database and BAS.	NOT APPLICABLE	NOT PART OF THE RFP
16	NA	NA	scope	The proposed BAS solution should demonstrate execution of real adversary destructive and wiper payloads based on unique malware from in-house IR engagements	In house IR engagements of the OEM gives the real attacker behavior, patterns, tools used, unique maleare being used, payloads being used etc. This might not be available in any data base publically. Any one can fall victim of this as no one has visibility of payload except the IR consultants who see this every day. Hence we request you to add this specification to BOB's benefit.	NOT APPLICABLE	NOT PART OF THE RFP
17	NA	NA	scope	The proposed BAS solution should demonstrate ability to execute non-neutered and non-altered adversary payloads from active adversary engagement in a safe manner	This is reallyl important for BOB to run malicious software or code (payloads) created by attackers (adversaries) in their original, unmodified form. This is done in a controlled environment for analysis and testing purposes. Indicates that the payload is being executed exactly as it was created by the adversary, without any modifications or disarmament. We request you to please add this specification.	NOT APPLICABLE	NOT PART OF THE RFP
18	NA	NA	scope	The proposed BAS solution should possess native and in-house vulnerability (including zero days) reverse engineering Team for BAS / security validation tool	NIL	NOT APPLICABLE	NOT PART OF THE RFP

19	Page no. 12	Point 8	Payment Terms a. Software Licenses Cost	50% of the license cost on delivery of Software Licenses plus applicable taxes at actuals. The required documents to be provided are original invoice, Delivery challans / license copy and OEM letter for licenses mapping to Bank of Baroda. The relevant documents should be duly stamped and signed by bidder representative and Bank officials. • 30% of the license cost after successful installation of the software and payable against implementation sign-off in the form of implementation report duly stamped and signed by the bidder representative and Bank officials. • 20% of the license cost after Go-Live closure signoff from Bank. Go-Live Closure Sign Off report should be duly stamped and signed by bidder representative and Bank officials	As bank will be holding the implementation cost payment till Go-Live request bank to amend the clause as "**80%** of the license cost on delivery of Software Licenses plus applicable taxes at actuals. The required documents to be provided are original invoice, Delivery challans / license copy and OEM letter for licenses mapping to Bank of Baroda. The relevant documents should be duly stamped and signed by bidder representative and Bank officials. • **15%** of the license cost after successful installation of the software and payable against implementation sign-off in the form of implementation report duly stamped and signed by the bidder representative and Bank officials. • **5%** of the license cost after Go-Live closure signoff from Bank. Go-Live Closure Sign Off report should be duly stamped and signed by bidder representative and Bank officials"	No Change	As per RFP Document.

20	Page no. 12	Point 8	Payment Terms: b. Implementation & Integration Cost (OTC)	• 70% of the implementation & integration cost post Phase-I Implementation sign off from Bank. Phase-I Implementation sign-off will be provided upon complete installation, configuration and implementation of the proposed Breach and attack simulation (BAS) solution with all components in the Bank. Sign Off in the form of Implementation Sign-off report should be signed by duly stamped and signed by Banks identified Project Manager & vendor representative. • 30% of the implementation & integration cost post final Go-Live Closure Sign off from Bank. Go-Live Closure Sign-off will be provided upon completion / closure of the project and handover to Bank team.	As Bank will be holding the Software payment also request Bank to amend the clause as "**• 90%** of the implementation & integration cost post Phase-I Implementation sign off from Bank. Phase-I Implementation sign-off will be provided upon complete installation, configuration and implementation of the proposed Breach and attack simulation (BAS) solution with all components in the Bank. Sign Off in the form of Implementation Sign-off report should be signed by duly stamped and signed by Banks identified Project Manager & vendor representative. • **10%** of the implementation & integration cost post final Go-Live Closure Sign off from Bank. Go-Live Closure Sign-off will be provided upon completion / closure of the project and handover to Bank team.	No change	As per RFP Document.
21	Page no. 13	1.4	Payment Terms: C. Annual Subscription License Cost / Annual Technical Support (ATS) Cost	The Annual Subscription License Cost / Annual Technical Support (ATS) Cost invoices will be raised by Service Provider on half yearly basis after completion of each half year. The invoices will be payable against receipt of satisfactory report of previous half year from the Bank's Project / Operations Manager and relevant supportive documents including services report.'	Request bank to amend the clause as " Annual Subscription License Cost / Annual Technical Support (ATS) Cost invoices will be raised by Service Provider on yearly in advance.	No change	As per RFP Document.

22	Page no. 71	1.4	13.1 Mandatory Technical Requirements: Point 1	The proposed solution should be deployable on-premises or India based cloud, All infrastructure cost related to cloud shall be borne by the bidder.	Request bank to clarify If solution is On-Premises Bank will provide required infrastructure, Hardware, VMs, Database and software to host the solution.	No change	As mentioned in the RFP Infrastructure i.e Virtual Machine for the on prem deployment of the solution will be provided by the bank.
23	Page no.33	1.4.1	Section D1 Experience and support	The proposed BAS solution should have been implemented by the bidder / OSD / authorized channel partner of OSD in at least two Commercial Banks / Financial Institutions / Govt. Organizations in India in the last 5 years	Will you consider the enterprise implementations.	No change	As per the RFP Document
24	Page no. 34	1.4.1	Section D3 Experience and support	The bidder should have minimum 5 number of employees on their permanent payroll with CISSP / OSCP / CCSP / CISM certifications from ISACA / (ISC)2 / EC-Council/ Offensive Security.	Will you consider OEM certification	No Change	As per RFP Document.

25	Page no.63	1.5	Annexure 12 (2.9 & 2.14)	2.9 The bidder has to setup the proposed solution infrastructure at Bank's DC (Mumbai) or DR (Hyderabad) locations as per the requirement of the bank. All necessary software and network components to host the proposed solution at Bank's premises and Cloud should be supplied, configured, and implemented by the bidder. 2.14 The bidders should ensure DR set up of the proposed services to ensure continuity of services in case of failure of primary setup.	Section 2.9 says that DC or DR for the proposed solution whereas in 2.14 says that DR should be considered. Please clarify	No change	The DC site is in Mumbai and DR site is in hyderabad. As mentioned in the point no 2.14 The bidder should ensure DR setup of the proposed service to ensure continuity of services in case of failure of primary setup that is DC site.

26	12	Annexure 02 - Evaluation Terms	D - Experience and Support Infrastructure	The proposed BAS solution should have been implemented by the bidder / OSD / authorized channel partner of OSD in at least two Commercial Banks / Financial Institutions / Govt. Organizations in India in the last 5 years.	We would request you amend the clause as per below The proposed BAS solution should have been implemented by the bidder / OSD / authorized channel partner of OSD in at least two Commercial Banks / Financial Institutions / Govt. Organizations in India in the last 5 years / **International Known Orgnization**	No Change	As per RFP Document.
27	14	Annexure 02 - Evaluation Terms	D - Experience and Support Infrastructure	The bidder should have experience in offering Breach and attack simulation (BAS) solution in India.	We would request you to amend clause as per below The bidder**r/OSD / OEM** should have experience in offering Breach and attack simulation (BAS) solution in India.	No change	As per RFP Document.
28	17	Annexure 02 - Evaluation Terms	D - Experience and Support Infrastructure	The bidder should have minimum 5 number of employees on their permanent payroll with CISSP / OSCP / CCSP / CISM certifications from ISACA / (ISC)2 / EC-Council/ Offensive Security.	We would request you to amend clause as per below The bidder / OEM / OSD should have minimum 5 number of employees on their permanent payroll with CISSP / OSCP / CCSP / CISM certifications from ISACA / (ISC)2 / EC-Council/ Offensive Security.	No Change	As per RFP Document.

29	63	Annexure 02 - Evaluation Terms	B. Technical Bid Evaluation	The number of Breach attack simulation (BAS) services proposed to the Bank and rendered by OEM / OSD directly or through their channel partners to the commercial banks/ Financial Institutions / Govt. Organizations in India in last 5 years (as on RFP date)# .	We would request you amend the clause as per below The number of Breach attack simulation (BAS) services proposed to the Bank and rendered by OEM / OSD directly or through their channel partners to the commercial banks/ Financial Institutions / Govt. Organizations in India in last 5 years / International Known Organization (as on RFP date)# .	No change	As per RFP Document.
30	Pt. 8 at Pg. 2	Annexure 02 - Evaluation Terms	B. Technical Bid Evaluation	The number of Breach attack simulation (BAS) services proposed to the Bank and rendered by the bidder to the commercial banks/ Financial Institutions / Govt. Organizations in India in last 5 years (as on RFP date)# . Only solution proposed by the bidder to the Bank shall be counted.	We would request you to kindly amend the clause as per below. The number of Breach attack simulation (BAS) services proposed to the Bank and rendered by the bidder/OEM to the commercial banks/ Financial Institutions / Govt. Organizations in India in last 5 years / **International Known Orgnization** (as on RFP date)# . ~~Only solution proposed by the bidder to the Bank shall be counted.~~	No Change	As per RFP Document.

31	12		8. Payment Terms	a.Software Licenses Cost • 50% of the license cost on delivery of Software Licenses plus applicable taxes at actuals. The required documents to be provided are original invoice, Delivery challans / license copy and OEM letter for licenses mapping to Bank of Baroda. The relevant documents should be duly stamped and signed by bidder representative and Bank officials. • 30% of the license cost after successful installation of the software and payable against implementation sign-off in the form of implementation report duly stamped and signed by the bidder representative and Bank officials. • 20% of the license cost after Go-Live closure signoff from Bank. Go-Live Closure Sign Off report should be duly stamped and signed by bidder representative and Bank officials	We request Bank to amend the clause as:- a.Software Licenses Cost • **80%** of the license cost on delivery of Software Licenses plus applicable taxes at actuals. The required documents to be provided are original invoice, Delivery challans / license copy and OEM letter for licenses mapping to Bank of Baroda. The relevant documents should be duly stamped and signed by bidder representative and Bank officials. • **10%** of the license cost after successful installation of the software and payable against implementation sign-off in the form of implementation report duly stamped and signed by the bidder representative and Bank officials. • **10%** of the license cost after Go-Live closure signoff from Bank. Go-Live Closure Sign Off report should be duly stamped and signed by bidder representative and Bank officials	No Change	As per RFP Document.

32	13		C. Annual Subscription License Cost / Annual Technical Support (ATS) Cost	The Annual Subscription License Cost / Annual Technical Support (ATS) Cost invoices will be raised by Service Provider on half yearly basis after completion of each half year. The invoices will be payable against receipt of satisfactory report of previous half year from the Bank's Project / Operations Manager and relevant supportive documents including services report.	Since OEM payment terms are upfront, we request bank to kindly amend the clause as:- The Annual Subscription License Cost / Annual Technical Support (ATS) Cost invoices will be raised by Service Provider on **yearly basis at the start of each year**. The invoices will be payable against receipt of satisfactory report of previous year from the Bank's Project / Operations Manager and relevant supportive documents including services report.	No change	As per RFP Document.
33	34		Experience and Support Infrastructure	The bidder should have minimum 5 number of employees on their permanent payroll with CISSP / OSCP / CCSP / CISM certifications from ISACA / (ISC)2 / EC-Council/ Offensive Security.	We request bank to amend the clause as :- The bidder should have minimum **3** number of employees on their permanent payroll with CISSP / OSCP / CCSP / CISM certifications from ISACA / (ISC)2 / EC-Council/ Offensive Security.	No change	As per RFP Document
34	35		Technical Bid Evaluation	The number of Breach attack simulation (BAS) services proposed to the Bank and rendered by the bidder to the commercial banks/ Financial Institutions / Govt. Organizations in India in last 5 years (as on RFP date)# . Only solution proposed by the bidder to the Bank shall be counted. For each client experience - 5marks Maximum Marks - 15	Since BAS is compartively new technology, hence we request Bank to amend the clasuse as:- The number of Breach attack simulation (BAS) services proposed to the Bank and rendered by the bidder to the commercial banks/ Financial Institutions / Govt. Organizations in India in last 5 years (as on RFP date)# . Only solution proposed by the bidder to the Bank shall be counted. **For each client experience - 15marks** Maximum Marks - 15	No change	As per RFP Document.

35	34		Eligibility Criteria	The bidder should have minimum 5 number of employees on their permanent payroll with CISSP / OSCP / CCSP / CISM certifications from ISACA / (ISC)2 / EC-Council/ Offensive Security. Copy of valid certificate/s to be provided as a proof for each employee. An undertaking letter should be provided by the bidder on their letter head confirming that the employees are on their payroll.	Kind request to keep minimum 3 numbers of the employee instead of 5 Numbers of employee	No change	As per RFP Document.
36	30		Eligibility Criteria	The bidder must be in the business of supply, implementation, and maintenance of providing Cyber Security Services / Security Operations Centre in India at least for the last 2 years (as on RFP date).	We can provide Provide & Email order but as some customers still deployment is going on.	No Change	As per RFP Document.
37	35		Technical Bid Evaluation	The number of Breach attack simulation (BAS) services proposed to the Bank and rendered by the bidder to the commercial banks/ Financial Institutions / Govt. Organizations in India in last 5 years (as on RFP date)# . Only solution proposed by the bidder to the Bank shall be counted.	Kind request to keep one order for bidder & two numbers	No change	As per RFP Document.

38	72	15	Technical Requirement	The proposed solution should be able to add new attacks identified by Computer Emergency Response Team (CERT-In) within a maximum of 24 Hrs. Further, response action should be available to remediate the threats in Real Time.	24-hour SLA is too stringent for all type of CERT-IN attack advisories, namely informational, low severity etc. Hence please change this clause for 24-hour SLA for globally critical attacks. **The proposed solution should be able to add new globally critical attacks within a maximum of 24 Hrs. Further, response action should be available to remediate the threats in Real Time.**	No Change	As per RFP Document.
39	73	18	Technical Requirement	The proposed solution should have the capability to integrate with the SIEM, SOAR solution of the bank to identify issues related to the performance and hygiene of detection rules and obtain insights to help optimize threat detection and response capabilities	Picus can provide all the mitigation content over API to SIEM & SOAR. However the responsibility of writing playbooks using the content provided over API rests with the SOAR administration team as they are the custodians of the playbooks. Hence please amend this clause from 'integrate' to 'provide all mitigation content over API'. **The proposed solution should have the capability to provide all mitigation content over API with the SIEM, SOAR solution of the bank to identify issues related to the performance and hygiene of detection rules and obtain insights to help optimize threat detection and response capabilities**	No Change	As per RFP Document.

40	73	25	Technical Requirement	The proposed solution should cover multiple exfiltration techniques including but not limited to HTTP, HTTPS, FTP, SFTP, open ports etc.	Data Exfiltration attacks are generally 'inside-out'. Hence it is not a valid use case. Moreover, this appears to be a vendor-specific clause and limits participation. **The proposed solution should cover multiple exfiltration techniques including but not limited to HTTP, HTTPS, TCP, SMTP, etc.**	No Change	As per RFP Document.
41	74	28	Technical Requirement	The proposed solution should be able to move laterally to achieve a defined object and should cover methods including but not limited to brute force, password spraying, pass the hash , pass the token, LDAP password stealing, kerb roasting, third party credentials harvesting, LLMNR/NBT-NS Poisoning and Relay etc.	Picus supports numerous techniques in its extensive library. Specifically LLMNR/NBT-NS Poisoning and Relay are considered dangerous for production environments. Hence requesting to remove these specific techniques. All others are OK. **The proposed solution should be able to move laterally to achieve a defined object and should cover methods including but not limited to brute force, password spraying, pass the hash , pass the token, LDAP password stealing, kerb roasting, third party credentials harvesting, etc.**	No Change	As per RFP Document.

42	76	61	Technical Requirement	Bidder should be able to check any outbound flows of data / critical information, outlined by bank, during simulation. Such simulation should cover exfiltration methods such as SFTP, removable media, on various cloud services like Gdrive etc.	Removable media is a physical activity, not a BAS usecase. SFTP port is generally not used from inside to outside communication. It is not a valid adversary behavior and generally this port is blocked in firewalls (best practice). G-Drive works on https (port 443) and adversaries use many other drives that work on 443 port as this is generally allowed through the firewall. In order to expand the coverage of this vector, please change from G-drive to https. **Bidder should be able to check any outbound flows of data / critical information, outlined by bank, during simulation.**	No Change	As per RFP Document.
43	77	70	Technical Requirement	Service providers should measure the time to detect and respond to the attack simulation.	Detect is OK, Respond is not possible via BAS. (Maybe this is in the bidders' manual Incident Response scope). Please remove if this expected from BAS tool. **Service providers should measure the time to detect the attack simulation.**	No Change	As per RFP Document.
44	77	71	Technical Requirement	Bidder should be able to perform attack simulation by exploiting missing patches and highlight issues pertaining to the same.	BAS looks at vulnerabilities and exploitability as per latest adversary behavior and techniques. BAS looks at vulnerabilities and exploitability as per latest adversary behavior and techniques. **Hence requesting to change 'missing patches' to 'latest adversary behavior and techniques'Bidder should be able to perform attack simulation by exploiting latest adversary behavior and techniques and highlight issues pertaining to the same.**	No Change	As per RFP Document.

45	77	72	Technical Requirement	Bidder should provide data/ information on the bank's vulnerabilities (inherent, obsolete versions, unpatched and other types), misconfigurations, less secure configurations or unconfirmed setups, internal applications, services, URLs, ports, network components, systems, databases, and any other bank's infrastructure exposed in public domain and other forums	BAS technology does not focus on IT Assets, Vulnerabilities or Applications, albeit only on Threats and Security Controls. This use case is dedicated External Attack Surface Management which is a separate product category. This limits vendor participation. Please remove	No Change	As per RFP Document.
46		1 of 17	Eligibility Criteri Section A General point no 2	Documentry proof of successful implementation / reference letter from clients	Request bank to also accept email confirmation sign-off .	No Change	As per RFP Document.
47		5 of 17	Eligibility Criteri Section D point no 2	The bidder should have minimum 5 number of employees on their permanent payroll with CISSP / OSCP / CCSP / CISM certifications from ISACA / (ISC)2 / EC-Council/ Offensive Security	Request bank to also include CEH and CISA certifications as well	No Change	As per RFP Document.
48		66 of 137	Secrtion 3 Delivery	Delivery of the license has to happen in 8 weeks and Installationwith 9 weeks from the date of the PO	Kindly request bank to extend the delivery time line to 10 -12 week and installatioj oof the solituion to 16 -18 weeks	No Change	As per RFP Document.

49	72	12	Techinical Requirement	Any PII data, user credentials collected during simulation activity, if required, should be stored in encrypted / masked form only.	type of PII storage information	No Change	As per RFP Document.
50	73	19	Techinical Requirement	The proposed solution should support integration and communicate with other solutions based on an “Application Programming Interface” (API), for the purposes such as Customized reports, Customized dashboards, Integration with third party solutions like SOAR, SIEM, EDR, XDR etc.	SOAR Integration information not found	No Change	As per RFP Document.
51	33	1	Eligiblity Criteria	The proposed BAS solution should have been implemented by the bidder / OSD / authorized channel partner of OSD in at least two Commercial Banks / Financial Institutions / Govt. Organizations in India in the last 5 years.	Request for relaxation for this clause	No Change	As per RFP Document.
52			Eligiblity Criteria	Not Mentioned	Does "Limited Company" also include a Pvt Ltd Company?	No change	Yes, it includes Pvt Ltd Company.
53			Eligiblity Criteria	Not Mentioned	Can we include the Provisional Financials for 2023-2024 in the last three years' data to be shared?	No Change	As per RFP Document.
54			Eligiblity Criteria	Not Mentioned	For the Profitability Clause, can we consider the financial years 2021-2022, 2022-2023, and 2023-2024?	No Change	As per RFP Document.