Bank's Clarification to the Pre-Bid Queries

Request for Proposal for Selection of Service Provider for External Attack Surface Management (EASM) and Digital Risk Monitoring (DRM) Services (GeM Bid No. - GEM/2023/B/3530910 dated 13-Jun-2023)

Sr.	Page #	Point / Section #	Clarification point as stated in the tender document	Comment/ Suggestion	Bank's Clarification to Pre-bid queries
1	56-65	26	The bidder should store historical information about the bank to provide cybersecurity maturity over time.	Suggest the Bank to make this a Mandatory to understand the trajectory of Attack vectors that can potentially be used by a Threat actor to conduct an attack (storing historical information about the bank's cybersecurity incidents, breaches, and vulnerabilities provides a valuable resource for threat analysis, incident response, compliance, risk assessment, and staff training. It enables the bank to learn from the past, strengthen its security measures, and continuously improve its cybersecurity maturity over time.)	No Change.
2	56-65	33	The proposed platform / console to the Bank should provide option to tag / categorize the assets identified during external assets scan.	Suggest Bank to make this Mandatory as Categorisation will help to fine tune actionable threats, thereby reducing the alert fatigue, and providing Bank / SOC team, with Actionable Threat Intelligence	No Change.
3	56-65	38	The bidder should evaluate and analyze asset attributes to determine if an asset is risky, vulnerable or behaving in an anomalous manner and report to the Bank through automated mechanism.	Suggest Bank to make this Mandatory as Having the exposure of all the assets gives visibility into most vulnerable assets which has continuous mention in several forums and could likely be exploited as the initial attack vector.	No Change.
4	56-65	43	The bidder should support application security scanning of web and mobile applications to identify OWASP top 10 vulnerabilities.	Request Bank to make this a Mandatory requirement as Scanning for OWASP Top 10 vulnerabilities in web and mobile applications is crucial to identify and fix security risks, comply with regulatory standards, and maintain a robust overall security posture. It helps prevent attacks, manages risk, and	No Change.

Sr.	Page #	Point / Section #	Clarification point as stated in the tender document	Comment/ Suggestion	Bank's Clarification to Pre-bid queries
				proves cost-effective by addressing issues during the development phase rather than post-launch. Ultimately, this practice safeguards your organization's reputation and customer trust.	
5	56-65	75	The bidder must continuously discover and map all assets within Bank's environment, including servers, workstations, mobile devices, supply chain and cloud assets using high fidelity discovery of the BOB's digital footprint, which includes BOBs internet-facing assets, internet hosts, services, websites, certificates, IPv4, IPv6, Autonomous System Number (ASN), DNS, Cloud, etc.	Request Bank to make this Mandatory, as this helps bank in discovering assets that are functional beyond their specific purpose and which could be exploited as the initial attack vector.	No Change.
6	56-65	76	Apart from the IT assets, the vendors software dependencies and plugins must be fingerprinted and risk related to the same must be highlighted by the bidder.	Request Bank to make this a mandatory requirement as Ensuring a vendor's software dependencies and plugins are fingerprinted and risks highlighted is not just a good practice, it's essential. This process uncovers hidden vulnerabilities that could otherwise be exploited, threatening the entire system's integrity. Without it, you're essentially navigating blindfolded in a risk-infested landscape, jeopardizing data, reputation, and trust.	No Change.
7	56-65	77	The bidder must also cover threats associated with fake apps, data / credential leaks in code repositories, Fake Customer care numbers that pose a risk to the bank.	Request Bank to make this a Mandatory requirement as Monitoring Brand related threats is utmost important, considering the number of scans happening these days through fake contact centre number which is the source of new scams.	No Change.
8	39	B. Technical Bid Evaluation	The OEM/OSD has own Security Operations Centre (SOC) / Security Monitoring Setup and the same is ISO 27001 / SOC 2 / SOC 3 certified. For Own SOC	We request the bank to remove the evaluation parameter for own SOC and SOC in India as it is better suited for the bidder and not the OEM	Please read – 1. "For Own SOC" as "For Own SOC / Security Monitoring Setup" and 2. "SOC in India" as

Sr.	Page #	Point / Section #	Clarification point as stated in the tender document	Comment/ Suggestion	Bank's Clarification to Pre-bid queries
			SOC in India ISO 27001 / SOC 2 / SOC 3 certification Maximum Marks		"SOC / Security Monitoring Setup in India". No Change.
9	58	20	The bidder should identify new global threats like Malicious IP Addresses, Domain, URL, Filename, File hash, Email address, Known C&C (Command and Control) hosts and provide report to the Bank in an automated manner.	This is proprietary to a particular vendor. Request BoB to kindly remove this clause	The bidder is expected to identify new global threats as mentioned in the clause and should provide report to the Bank. No Change.
10	58	22	The bidder should be able to provide the historical data of the threat actor, threat activity, threat objects (historical data of the IPs, URLs, etc. used by the malicious entity) to the Bank.	This is proprietary to a particular vendor. Request BoB to kindly remove this clause	The clause as per RFP is as follows: "The bidder should be able to provide historical data of the threat actor, threat activity, threat objects (historical data of the IPs, URLs, etc.) with respect to the Bank, post commencement of services. If feasible, information pertaining to other organizations may also be provided." No Change.
11	61	46	The proposed platform / console provided to the Bank should provide the facility for searching the categorization of the historical data of the threat actor, threat activity, threat objects (historical data of the IPs, URLs, etc. used by the malicious entity) linked on a single view.	Request the BOB to elaborate the use case here.	Bank should have access to the EASM and DRM platform / console with search mechanism on various parameters like malicious IP, URL, etc. and provide a unified view of the same.
12	63	58	The bidder should be capable of blocking of the phishing sites in web browsers including but not limited to Google Chrome, Mozilla Firefox, Microsoft Edge and Internet Explorer.	This is proprietary to a particular vendor. Request BoB to kindly remove this clause	The phishing sites should be blocked in major web browsers as per Bank's requirement. No Change.
13		26	The number of External Attack Surface Management (EASM) and Digital Risk Monitoring (DRM) services proposed to the	Request to provide relaxation and change to OEM with 5 years experience rendered to Financial Institute	No Change.

Sr.	Page #	Point / Section #	Clarification point as stated in the tender document	Comment/ Suggestion	Bank's Clarification to Pre-bid queries
			Bank and rendered by the bidder to the commercial banks/ Financial Institutions / Govt. Organizations in India in last 3 years (as on RFP date)# . Only solution proposed by the bidder to the Bank shall be counted.		
14	27	Technical, Experience and Support Point 2	The bidder should have successfully provided External Attack Surface Management (EASM) and Digital Risk Monitoring (DRM) services in minimum 2 commercial banks/ Financial Institutions / Govt. Organizations in India in last 3 years (as on RFP date)	We request Bank to modify this clause as: The bidder should have successfully provided External Attack Surface Management (EASM) and Digital Risk Monitoring (DRM) services in minimum 2 commercial banks/ Financial Institutions / Govt. Organizations in India in last 5 years (as on RFP date)	No Change.
15	28	B. Technical Bid Evaluation	The number of External Attack Surface Management (EASM) and Digital Risk Monitoring (DRM) services proposed to the Bank and rendered by the bidder to the commercial banks/ Financial Institutions / Govt. Organizations in India in last 3 years (as on RFP date)# . Only solution proposed by the bidder to the Bank shall be counted.	We request bank to modify this clause as: The number of External Attack Surface Management (EASM) and Digital Risk Monitoring (DRM) services proposed to the Bank and rendered by the bidder to the commercial banks/ Financial Institutions / Govt. Organizations in India in last 3 years (as on RFP date)	No Change.
16	26	C. Technical, Experience and Support	The bidder should have atleast -2- years of experience in offering External Attack Surface Management (EASM) and Digital Risk Monitoring (DRM) services in India. OR Below clause is applicable for bidders who fall under the category of Micro & Small Enterprise (MSEs) or Start-ups (Necessary valid documentary proof certifying the bidder as an MSE or a Start-up needs to be submitted by the bidder) The bidder should have atleast 18 months of	We request you allow OEM should have experience in implemented the EASM and DRM solution in last 2 years. As all the services will be provided by OEM.	No Change.

Sr.	Page #	Point / Section #	Clarification point as stated in the tender document	Comment/ Suggestion	Bank's Clarification to Pre-bid queries
			experience in offering External Attack Surface Management (EASM) and Digital Risk Monitoring (DRM) services in India.		
17	27	C. Technical, Experience and Support	The bidder should have successfully provided External Attack Surface Management (EASM) and Digital Risk Monitoring (DRM) services in minimum 2 commercial banks/ Financial Institutions / Govt. Organizations in India in last 3 years (as on RFP date)	We request you allow OEM should have successfully provided EASM and DRM services to minimum 2 commercial Banks/ Financial Institutions/ Govt. Organisations in India in last 3 Years.	No Change.
18	28	B. Technical Bid Evaluation	Number of employees on the permanent payroll of the bidder with CISA / CISSP / CEH / CCSP / CISM certifications from ISACA / (ISC)2 / EC-Council.	Request you to consider OEM and Bidder Certification as the services will be provided by them.	No Change.
19	29	B. Technical Bid Evaluation	The OEM/OSD has own Security Operations Centre (SOC) / Security Monitoring Setup and the same is ISO 27001 / SOC 2 / SOC 3 certified.	Request to change it OEM should have SOC/ Security Monitoring Setup and same is ISO 27001/ SOC2/SOC3 Certified.	No Change.
20	55	5	The bidder should log all user activity which should be available for view, review and auditing purpose.	Request you to please remove this clause/ Keep it as Good to have.	No Change.
21	57	29	The bidder should provide data/information on security flaws/inherent vulnerabilities identified about the Bank's web and mobile applications exposed to the Internet	Request you to please provide clarification on mobile apps; is the Bank referring to the web servers of the mobile apps. **Kindly keep this clause Good to have.**	Mobile applications include applications as well as the associated public facing infrastructure of the apps like web servers. No Change.
22	58	36	The bidder should continuously scan of Bank's public facing websites and mobile applications for any potential threats or vulnerabilities, without any operational or performance impact to the Bank's applications.	Request you to please provide clarification on mobile apps; is the Bank referring to the web servers of the mobile apps or mobile web server? **Kindly keep this clause Good to have.**	Mobile applications include applications as well as the associated public facing infrastructure of the apps like web servers. No Change.
23	58	37	The bidder should provide recommendations to safeguard Bank's public facing assets	Request you to please provide clarification on mobile apps; is the Bank referring to the	Mobile applications include applications as well as the

Sr.	Page #	Point / Section #	Clarification point as stated in the tender document	Comment/ Suggestion	Bank's Clarification to Pre-bid queries
			including but not limited to web applications and mobile applications against threats / risks identified.	web servers of the mobile apps or mobile web server? **Kindly keep this clause Good to have.**	associated public facing infrastructure of the apps like web servers. No Change.
24	58	40	The bidder should detect for possible defacement of public facing websites and mobile applications on continuous basis to protect the brand, credibility and reputation of the bank.	This is feature of WAF. Request you to please keep this as Good to have.	No Change.
25	59	50	The bidder should provide 24x7x365 detection, monitoring and unlimited takedowns service for phishing websites, rogue apps, brand abuse and brand infringement targeting the Bank.	need clarification on no. of current Takedowns performed by the bank. Request to remove the Unlimited clause and provide the nos of expected takedowns.	No Change.
26	63	72	The bidder should comply with the extant guidelines issued by the government agencies, regulator or Bank with respect to Brand Monitoring Services. It should make any necessary changes in the services accordingly and provide updated services without any additional cost.	Kindly remove below clause. It should make any necessary changes in the services accordingly and provide updated services without any additional cost.	No Change.
27	63	73	The bidder should provide unlimited takedowns including but not limited to phishing sites, brand abuse, fake social media accounts/pages/groups and rogue apps during the contract period.	Kindly remove unlimited takedowns. Please help to provide tentative numbers.	No Change.
28	63	76	Apart from the IT assets, the vendors software dependencies and plugins must be fingerprinted and risk related to the same must be highlighted by the bidder.	Please provide more clarity.	The software dependencies and plugins in the Bank's web and mobile applications should be fingerprinted during scan and risk related to the same should be highlighted by the bidder.

----------X----------X----------