

Date: February 20, 2025

CORRIGENDUM No. 1: RESPONSE TO PRE-BID MEETING QUERIES FOR GeM TENDER ON CYBER SECURITY MANAGED SERVICE PROVIDER (REF.NO: GEM/2025/B/5907817).

Please refer to the GeM tender reference no. GEM/2025/B/5907817 for CYBER SECURITY MANAGED SERVICE PROVIDER. The Pre-Bid meeting was conducted on February 17, 2025, at 11.30 AM. The bidders are advised to consider the following amendments/Corrigendum before submission of their bids against this tender.

The details are as follows:

Sr No	Pre-Bid Query	Existing Clause	Revised Clause / Clarification
1	<p>Requested following modification for the eligibility criteria Point No.6:</p> <ol style="list-style-type: none"> 1. Include Information Security along with Cyber Security services. 2. Instead of the past three Financial Years [FYs], consider the past Five FYs. 3. Include Insurance Sector along with the BFSI sector. 4. Consider a reduction in minimum of 6 resources contract. 5. For some work orders or purchase orders, the resource count is not mentioned. In such cases, consider the Project Value. 	<p>Eligibility Criteria: Point No. 6</p> <p>The bidder must have provided Cyber Security Managed Services (CSMSP) to at least three public sector Bank/Scheduled commercial Bank/Small Finance Bank in India/All India Financial Institutes (AIFIs) in India for the past three Financial Years. (FY 2023-24, FY 2022-23, FY 2021- 22) of minimum 6 resource contract.</p>	<p>Eligibility Criteria: Point No. 6</p> <p><u>Revised Clause:</u></p> <p>The bidder must have provided Cyber Security /Information Security Managed Services (CSMSP) to at least three public sector Bank/Scheduled commercial Bank/Small Finance Bank in India /All India Financial Institutes (AIFIs) / Insurance sector in India for the past five Financial Years.(FY 2023-24, FY 2022-23, FY 2021- 22, FY 2020-21, FY 2019-20) of minimum 5 resource contract.</p> <p>The Cyber/Information Security contract must have a minimum</p>

			value of INR 1.75 crore per year for resource contracts, if the purchase order document lacks information about the quantity or number of resources being ordered. Multiple orders from the same company will be considered as single count for evaluation purpose.
2	<p>Eligibility Criteria: Point No. 1</p> <p>Requested to include LLP organisations for participation in Eligibility Criteria Point No. 1</p>	<p>Eligibility Criteria: Point No. 1</p> <p>The bidder should be registered as a Limited company (Private or Public) in India as per Company Act 1956 / 2013 since last 5 years as on 31.12.2024</p>	<p>Eligibility Criteria: Point No. 1</p> <p><u>Revised Clause:</u></p> <p>The bidder should be registered as a Limited company (Private or Public) in India as per Company Act 1956 / 2013 or an LLP since last 5 years as on 31.12.2024</p>
3	<p>Scope of Work Point 2.6</p> <p>It is requested to include a B.Com qualification along with other academic qualifications and reduce the total required experience to 2–3 years.</p>	<p>Scope of Work Point 2.6</p> <p>Resource Type - L1 Number of Resources - 3 Educational Qualification - B.Sc. (IT, CS) OR Bachelor of Engineering (IT,CS) OR Master Of Computer Application(MCA)</p> <p>Professional Qualification - CEH And OSCP/CISA/CISM/CISSP/ ISO 27001-2013 Years of Experience - 3 to 5 years</p>	<p>Scope of Work Point 2.6</p> <p><u>Revised Clause:</u></p> <p>Resource Type - L1 Number of Resources - 3 Educational Qualification – B.Com /B.Sc. (IT, CS) OR Bachelor of Engineering (IT,CS) OR Master Of Computer Application(MCA)</p> <p>Professional Qualification - CEH And OSCP/CISA/CISM/CISSP/ ISO 27001-2013 Years of Experience - 3 to 5 years</p>

4	<p>Scope of Work Point 2.6</p> <p>It is requested to consider ISO 27001:2013 certification as an OR condition instead of an AND condition and to reduce the required experience level to 3–5 years.</p>	<p>Scope of Work Point 2.6</p> <p>Resource Type - L2 Number of Resources - 2 Educational Qualification - Bachelor of Engineering (IT,CS) OR Master Of Computer Application(MCA) Professional Qualification - OSCP /CISA /CISM /CISSP /CRISC and ISO 27001-2013 Years of Experience - 6 to 10 years</p>	<p>Scope of Work Point 2.6</p> <p><u>Revised Clause:</u></p> <p>Resource Type - L2 Number of Resources - 2 Educational Qualification - Bachelor of Engineering (IT,CS) OR Master Of Computer Application(MCA) Professional Qualification - OSCP /CISA /CISM /CISSP /CRISC and ISO 27001-2013 Years of Experience - 6 to 10 years</p> <p>Note: If a resource holds a CISSP certification, the ISO 27001:2013 requirement can be waived.</p>
5	<p>Eligibility Criteria: Point No. 3</p> <p>It is requested to include “CEH “ certification.</p>	<p>Eligibility Criteria: Point No. 3</p> <p>The Bidder should have a pool of full time minimum 100 professionals with any of the international accreditation like CISA/CISSP/OSCP/CISM/LPT/ISO 27001 LA/LI employed with them since last 2 years deployed in Information security /Cybersecurity domain. The profile of the resources who are stationed in India shall be considered for the count.</p>	<p>Eligibility Criteria: Point No. 3</p> <p><u>Revised Clause:</u></p> <p>The Bidder should have a pool of full time minimum 100 professionals with any of the international accreditation like CEH /CISA /CISSP /OSCP/CISM/LPT/ISO 27001 LA/LI employed with them since last 2 years deployed in Information security /Cybersecurity domain. The profile of the resources who are stationed in India shall be considered for the count.</p>

6	<p>Technical Evaluation Criteria :</p> <p>Point No. 5</p> <p>Please clarify whether the presentation is required as part of the bid submission on the 27th of this month, or if an alternative date will be provided for the same after eligibility evaluation</p>	<p>Technical Evaluation Criteria :</p> <p>Point No. 5</p> <p>Capability Presentation with resources aligned for this engagement. Following parameters will be assessed.</p> <ol style="list-style-type: none"> 1. Company profile and domain experience 2. Proposed resource experience and qualification details 3. Bidders experience in cyber security services especially BFSI sector. 4. Client feedback /reference letter. 	<p>Technical Evaluation Criteria :</p> <p>Point No. 5</p> <p><u>Clarification:</u></p> <p>The capability presentation should be uploaded in PDF format. The Bank will invite eligible bidders for the presentation.</p>
7	<p>Payment Terms and Conditions: Point No 4.2</p> <p>Please explain the methodology to be used for calculating the billing amount.</p>	<p>Payment Terms and Conditions: Point No 4.2</p> <p>The resource payment will be made on monthly basis within 10 working days after submission of correct Invoice along with Monthly Review Report and attendance details .</p>	<p>Payment Terms and Conditions: Point No 4.2</p> <p><u>Clarification:</u></p> <p>Total Billing Amount per resource type = Monthly resource rate quoted [Inclusive GST] X Number of resources - Any deductions as per RFP terms and conditions.</p>

8	<p>Period of engagement & Leaves: Point 2.5</p> <p>We understand that additional payments will be made as part of the monthly billing for any such requirements. Kindly confirm our understanding</p>	<p>Period of engagement & Leaves: Point 2.5</p> <p>In Case of emergency, resource may have to work on Saturdays and holidays.</p>	<p>Period of engagement & Leaves: Point 2.5</p> <p><u>Clarification:</u></p> <p>No additional payments will be made for working on Saturdays/holidays in case of emergency.</p> <p>The Bank may consider compensatory leave on case-to-case basis.</p>
9	<p>Activities to be performed by the Resources: Point No. 2.7 - 30</p> <p>Please explain the scope of activities to be performed.</p>	<p>Activities to be performed by the Resources: Point No. 2.7 - 30</p> <p>30. Implementation and monitoring of ISO 27001-2022 controls in the Bank.</p>	<p>Activities to be performed by the Resources: Point No. 2.7 - 30</p> <p><u>Clarification:</u></p> <p>The Bank is ISO 27001:2013 certified for the scope of Data Centre, DR, HR and Administration departments. The Bank will appoint a vendor for the implementation and assessment of ISO 27001:2022 certification.</p> <p>The service provider shall review and monitor the implementation status of ISO 27001:2022 controls</p>

			and report any gaps to the Bank's Information Security (IS) team as an ongoing activity.
10	<p>Eligibility Criteria: Point No. 8</p> <p>It is requested to consider Minimum 5 engagement of the organization in the BFSI sector in India or Abroad in context of Cyber Security / Information Security managed service Provider since last Five Financial Years.</p>	<p>Eligibility Criteria: Point No. 8</p> <p>Minimum 5 engagement of the organization in the BFSI sector in India or Abroad in context of Cyber Security Managed Service Provider (CSMSP) since last three Financial Years. (FY 2023-24, FY 2022-23, FY 2021-22)</p>	<p>Eligibility Criteria: Point No. 8</p> <p><u>Revised Clause:</u></p> <p>Minimum 5 engagement of the organization in the BFSI sector in India or Abroad in context of Cyber Security / Information Security Managed Service Provider (CSMSP) since last five Financial Years. (FY 2023-24, FY 2022-23, FY 2021-22, FY 2021-20, FY 2019-20)</p>
11	<p>Payment Terms and Conditions 4.2:</p> <p>It is requested to reduce the penalty amount.</p>	<p>Payment Terms and Conditions 4.2:</p> <p><u>Condition 1: Leaves beyond 12 days per Year per Resource Type.</u> CSMSP must ensure onsite resource availability as per the tender requirements. Any leave exceeding 12 days per year per resource type and less than 4 resource at a time will incur a penalty of ₹ 5,000 per day per resource apart from monthly billing. If the resource is required to take continuous leaves for a period exceeding four days, including bank holidays and public holidays, the CSMSP must provide a substitute/backup resource at Exim Bank.</p>	<p>Payment Terms and Conditions 4.2:</p> <p><u>Revised Clause:</u></p> <p><u>Condition 1: Leaves beyond 12 days per Year per Resource Type.</u> CSMSP must ensure onsite resource availability as per the tender requirements. Any leave exceeding 12 days per year per resource type and less than 4 resource at a time will incur a penalty of ₹ 2,000 per day per resource apart from monthly billing. If the resource is required to take continuous leaves for a period exceeding four days, including bank holidays and public holidays, the CSMSP must provide a</p>

			substitute/backup resource at Exim Bank.
12	Payment Terms and Conditions 4.2: It is requested to reduce the penalty amount.	Payment Terms and Conditions 4.2: Condition 4: <u>Replacement of resource:</u> If any resource is found unsuitable or underperforming during the deployment period, CSMSp must provide a replacement within 7 working days from the date of intimation. Any delay in replacing the resource will incur a penalty of ₹10,000 per day until the new resource is deployed.	Payment Terms and Conditions 4.2: <u>Revised Clause:</u> Condition 4: <u>Replacement of resource:</u> If any resource is found unsuitable or underperforming during the deployment period, CSMSp must provide a replacement within 7 working days from the date of intimation. Any delay in replacing the resource will incur a penalty of ₹5,000 per day until the new resource is deployed.
13	General Question	Which all are the tools to be provided by the Bank for the proposed scope of work.	Bank will provide following tools : <u>Clarification:</u> Nessus Tenable , Burp Suite , NMAP TITUS Data Classification Force Point DLP , Solar Winds, Windows SCCM , Manage Engine , Traplo , PAM – Arcon, SOPHOS XDR , ATP for Email etc.
14	Technical Evaluation Criteria 3.3 : Point No : 3	Technical Evaluation Criteria 3.3 Point No. 3 The Bidder should have a pool of full time minimum 100 professionals with any of the international accreditation like CISA/CISSP/OSCP/CISM/LPT/ ISO 27001 LA/LI employed with them since	Technical Evaluation Criteria 3.3 Point No. 3 <u>Revised Clause:</u> The Bidder should have a pool of full time minimum 100 professionals with any of the international accreditation like CEH /CISA /CISSP

		the last 2 years deployed in Information security /Cybersecurity domain.	/OSCP/CISM/LPT/ISO 27001 LA/LI employed with them since last 2 years deployed in Information security /Cybersecurity domain. The profile of the resources who are stationed in India shall be considered for the count.
15	Technical Evaluation Criteria 3.3 : Point No : 4	<p>Technical Evaluation Criteria 3.3 : Point No : 4</p> <p>The bidder must have provided Cyber Security Managed Services (CSMSP) to at least three public sector Bank/Scheduled commercial Bank/Small Finance Bank in India/All India Financial Institutes (AIFIs) in India for the past three Financial Years. (FY 2023-24, FY 2022-23, FY 2021- 22) of minimum 6 resource contract.</p>	<p>Eligibility Criteria: Point No. 4</p> <p><u>Revised Clause:</u></p> <p>The bidder must have provided Cyber Security /Information Security Managed Services (CSMSP) to at least three public sector Bank/Scheduled commercial Bank/Small Finance Bank in India /All India Financial Institutes (AIFIs) / Insurance sector in India for the past five Financial Years.(FY 2023-24, FY 2022-23, FY 2021- 22, FY 2020-21, FY 2019-20) of minimum 5 resource contract.</p> <p>The Cyber/Information Security contract must have a minimum value of INR 1.75 crore per year for resource contracts, if the purchase order document lacks information about the quantity or number of resources being ordered. Multiple orders from the same company will</p>

			be considered as single count for evaluation purpose.
16	Compliance to RBI Master Directions.	Bidder must adhere to RBI's Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices (RBI/2023-24/107 DoS.CO.CSITEG/SEC.7/31.01.015/2023-24 dated November 7, 2023) and Master Direction on Outsourcing of Information Technology Services (RBI/2023-24/102 DoS.CO.CSITEG/SEC.1/31.01.015/2023-24 dated April 10, 2023).	

All other terms and conditions of the tender document will remain unchanged. The tender document is available on our website <https://www.eximbankindia.in/tenders-and-notices>

Sd/-
Madheshwaran G