Corrigendum No. 2

Engagement of Managed Security Service Provider RFP for Engaging ISD Empaneled ISSP for Red Teaming Activity (Closed RFP)

RFP No- SBI/GITC/ISD/2025-26/CS/04 (RFP –1459)

Pre-Bid Queries and Responses

Vendor Name	Sl. No	RFP Page No	RFP Clause No.	Existing Clause	Query/Suggestions	SBI Response
AQM Technologies Private Limited	1	56	Appendix-E	A few of the attack vectors are listed below, but not limited to, to be considered for conducting testing at least 8 physical locations: •Public IP addresses •Domains/ Web Applications •Mobile Applications •ATM •Kiosks / Cheque Deposit Kiosk (CDKs) •Branch/ Administrative offices/ LHOs (i.e., Sample of urban and rural bank premises within India) •Wireless networks •Operational Technology (IoTs etc.)\	Please specify the numbers against each Line items mentioned in the scope of work- eg; How many Public IP addresses to cover? Number of Domains/Web Apps, Mobile Apps, ATM, Kiosks, No. of Branches, Number of Wireless networks etc.	Please adhere to the published guidelines of the RFP
AQM Technologies Private Limited	2	56	Appendix-E	A few of the attack vectors are listed below, but not limited to, to be considered for conducting testing at least **8 physical locations**	Please share the list of locations covered in the scope	Please adhere to the published guidelines of the RFP
AQM Technologies Private Limited	3	56	Appendix-E	The Red teaming activities should at least cover the given indicative scenarios, however more scenarios can be considered during the engagement.	Please specify the type of Red-Teaming to be done. Will it be black-box testing or Grey-box testing?	As it is Red Teaming activity, Bank will not provide any credentials for this exercise.

AQM Technologies Private Limited	4	56	Appendix-E	Scope of work	Please specify whether Bank will provide us pre-configured laptops for compromising Active Directory (AD) and tampering with EDR/Antivirus solution.	Please adhere to the published guidelines of the RFP
AQM Technologies Private Limited	5	56	Appendix-E	Scope of work	Please specify whether Bank will provide us isolated setup for conducting a simulated ransomware tests without disrupting business operations.	Please adhere to the published guidelines of the RFP
AQM Technologies Private Limited	6	56	Appendix-E	A few of the attack vectors are listed below, but not limited to, to be considered for conducting testing at least 8 physical locations	Please confirm targeted devices (CCTV, Bio Metric, Printers, etc.) to be covered in Red Teaming as only few attack vectors are given in RFP section- Scope of Work.	Please adhere to the published guidelines of the RFP
AQM Technologies Private Limited	7	56	Appendix-E	Scope of work	Please confirm if Phishing and Social Engineering to be covered in this scope. If yes, please specify number of employees to target	No, Phishing and Social Engineering is not the part of the scope.
AQM Technologies Private Limited	8	47	Appendix-C	Technical Evaluation The Bidder should have obtained at least cumulative purchase order value of 01 Crore in last 02 years (01.04.2023 to 31.03.2025) in the field of Red Teaming activity.	Please let us know if VAPT or Security Testing experience can be considered here. If not, request you to append this clause as: The Bidder should have obtained at least cumulative purchase order value of 25 Lakhs in last 02 years (01.04.2023 to 31.03.2025) in the field of Red Teaming activity.	VAPT or Security Testing experience will not be considered as Red Teaming activity & clause remains same as per RFP.
AQM Technologies Private Limited	9	47	Appendix-C	The Bidder should have conducted at least 05 Red Team Exercise in BFSI sector in India in last 02 years (01.04.2023 to 31.03.2025).	Please let us know if VAPT or Security Testing experience can be considered here.	VAPT or Security Testing experience will not be considered as Red Teaming activity.

SecurEyes Techno Services Pvt Ltd	10	47	Sl.No.4 Appendix-C	The Bidder should have conducted at least 05 Red Team Exercise in BFSI sector in India in last 02 years (01.04.2023 to 31.03.2025).	1.Extension of period from last 2 years to 5 years. 2. Inclusion of foreign Banks	The Bidder should have conducted at least 05 Red Team Exercise in BFSI sector in India in last 03 years (01.04.2022 to 31.03.2025).
SecurEyes Techno Services Pvt Ltd	11	47	Sl.No.5 Appendix-C	The Bidder should have obtained at least cumulative purchase order value of 01 Crore in last 02 years (01.04.2023 to 31.03.2025) in the field of Red Teaming activity.	1. Inclusion of foreign Banks 2. To reduce 1 Cr cap for given period	Please adhere to the published guidelines of the RFP
DTTILLP	12	56	Scope of work	A few of the attack vectors are listed below, but not limited to, to be considered for conducting testing at least 8 physical locations	Kindly confirm what physical locations is SBI referring to	Please adhere to the published guidelines of the RFP
DTTILLP	13	56	Scope of work	Operational Technologies	Please share the share the list of IoT devices used in SBI	Please adhere to the published guidelines of
DTTILLP	14	56	Scope of work	Explore the feasibility if the source code of the bank products could be changed during their red team activities without bringing the application down	Kindly clarify if expectation is to modify the source code of the products/applications in the production or non-production environment? Please provide more clarity on this point regarding the exact expectations	Please adhere to the published guidelines of the RFP
DTTILLP	15	56	Scope of work	Explore the feasibility whether the servers of critical applications could also be shut down by their red team activities without bringing it down	Kindly confirm if servers of critical applications are shut down during Red Team activity, the application will surely go down. Please provide more clarity on this point regarding the exact expectations	Please adhere to the published guidelines of the RFP

DTTILLP	16	56	Scope and Deliverables	Service Provider should cover 08 physical locations within India" and "Service Provider must cover the given scenarios for each location	Please provide more clarity on these points	Please adhere to the published guidelines of the RFP
DTTILLP	17	2	Schedule of Events	Last date and time for Bid submission Up to 12.00 P.M. on 28.04.2025	We kindly request a one-week extension to obtain the necessary internal approvals for bid submission	Last date and time for Bid submission Up to 12.00 P.M. on 07.05.2025
KPMG	18	2	Schedule of Events	Last date and time for Bid submission : Up to 12.00 P.M. on 28.04.2025	Please extend the Bid submission date by 3 to 4 days	Last date and time for Bid submission Up to 12.00 P.M. on 07.05.2025
KPMG	19	95	Annexure A	A few of the attack vectors are listed below, but not limited to, to be considered for conducting testing at least 8 physical locations:	Please share the list of locations where activity needs to be performed. Also, do we have any specific activity to be performed or all 7 themes has to be carried out on this locations as well?	Please adhere to the published guidelines of the RFP
KPMG	20	95	Annexure A	Explore the feasibility whether the servers of critical applications could also be shut down by their red team activities without bringing it down	We are assuming list of critical application will be provided by the bank.	Please adhere to the published guidelines of the RFP
KPMG	21	95	Annexure A	Unauthorized Data Exfiltration from Banks environment	We understand bank will provide a laptop with basic user privilege and from there we are supposed to exfiltrate the data.	Please adhere to the published guidelines of the RFP
KPMG	22	95	Annexure A	Explore the feasibility whether the servers of critical applications could also be shut down by their red team activities without bringing it down	We are assuming list of critical application will be provided by the bank.	Please adhere to the published guidelines of the RFP

Ernst & Young LLP	23	47	Technical – Evaluation Parameter point - 3	The Bidder should have at least 20 professionals having Offensive Security Certified Professional (OSCP) from offensive-security/ Certified Ethical Hacker (CEH) from EC-Council/ Licensed Penetration Tester (LPT) from EC-Council / GPEN: GIAC Penetration Tester from SANS/ GWAPT: GIAC Web Application Penetration Tester from SANS as full-time employee.	Request you to modify the clause to include Certified Red Team Professional (CRTP) as one of the accepted certifications. **Modified clause:-** " The Bidder should have at least 20 professionals having Offensive Security Certified Professional (OSCP) from offensive-security/ Certified Ethical Hacker (CEH) from EC-Council/ Licensed Penetration Tester (LPT) from EC-Council / GPEN: GIAC Penetration Tester from SANS/ GWAPT: GIAC Web Application Penetration Tester from SANS/ Certified Red Team Professional (CRTP) as full-time employee."	The Bidder should have at least 20 professionals having Offensive Security Certified Professional (OSCP) from offensive-security/ Certified Ethical Hacker (CEH) from EC-Council/ Licensed Penetration Tester (LPT) from EC-Council / GPEN: GIAC Penetration Tester from SANS/ GWAPT: GIAC Web Application Penetration Tester from SANS/ Certified Red Team Professional (CRTP) as full-time employee.
Ernst & Young LLP	24	47	Technical – Evaluation Parameter point - 4	The Bidder should have conducted at least 05 Red Team Exercise in BFSI sector in India in last 02 years (01.04.2023 to 31.03.2025).	Request you to modify the clause for demonstrating the experience in last 3 years rather than 2 years **Modified clause:-** "The Bidder should have conducted at least 05 Red Team Exercise in BFSI sector in India in last 03 years (01.04.2022 to 31.03.2025). "	The Bidder should have conducted at least 05 Red Team Exercise in BFSI sector in India in last 03 years (01.04.2022 to 31.03.2025).
Ernst & Young LLP	25	47	Technical – Evaluation Parameter point - 6	The Bidder should have performed Penetration Testing/ Ethical Hacking/ Red Team Testing activities covering the scope (AD, Internal Infrastructure, Headless	Request you to modify the clause for demonstrating the experience in last 3 years rather than 2 years	Please adhere to the published guidelines of the RFP

				devices and Internet facing Digital assets) in at least 03 Indian Public/ Private Scheduled Commercial Banks in last 02 years.	Kindly modify the clause "*The Bidder should have performed Penetration Testing/ Ethical Hacking/ Red Team Testing activities covering the scope (AD, Internal Infrastructure, Headless devices and Internet facing Digital assets) in at least 03 Indian Public/ Private Scheduled Commercial Banks in last* ***03 years*** ."	
Ernst & Young LLP	26	54	Appendix C6	Assignments handled of minimum 03 distinct clients under Red Teaming Exercise in Indian Public/ Private Scheduled Commercial Banks during the last 02 years(FY 2023-2024 and 2024-2025).	As per the technical evaluation criteria, it is stated that the Bidder should have conducted Penetration Testing / Ethical Hacking / Red Team Testing activities covering the specified scope (Active Directory, Internal Infrastructure, Headless Devices, and Internet-facing Digital Assets) for at least three (03) Indian Public or Private Scheduled Commercial Banks in the last two (02) years. However, Appendix 6 mentions that a minimum of three (03) distinct Red Teaming assignments must have been handled for Indian Public or Private Scheduled Commercial Banks during the last two years (FY 2023–2024 and 2024–2025). We request clarification on whether the requirement is: 1. 3 engagements in total (including any of Penetration Testing / Ethical Hacking / Red Teaming), or	Please adhere to the published guidelines of the RFP

					2. Specifically, 3 distinct Red Teaming assignments in the mentioned timeframe. Request you to modify the clause for demonstrating the experience in last 3 years rather than 2 years	
Ernst & Young LLP	27	56	Appendix E-Deliverables/ scope of work	A few of the attack vectors are listed below, but not limited to, to be considered for conducting testing at least 8 physical locations: • Public IP addresses • Domains/ Web Applications • Mobile Applications • ATM • Kiosks / Cheque Deposit Kiosk (CDKs) • Branch/ Administrative offices/ LHOs (i.e., Sample of urban and rural bank premises within India) • Wireless networks • Operational Technology (IoTs etc.)\ The Red teaming activities should at least cover the given indicative scenarios, however more scenarios can be considered	1. Kindly provide the list of the 8 locations that need to be covered. Additionally, please specify the scenarios mentioned in the scope that should be addressed for each location. 2. Could you please provide the count for the following elements to be covered as part of the scope: ATMs, Kiosks/Cheque Deposit Kiosks, Branch/Administrative Offices/LHOs, Wireless Networks, and IoT devices.	Please adhere to the published guidelines of the RFP

				during the engagement.		
Ernst & Young LLP	28	NA	NA	NA	Is revalidation expected as part of the process. If so, could you specify how many rounds of revalidation are anticipated	Please adhere to the published guidelines of the RFP
		56	Appendix E-Deliverables/ scope of work	Operational Technology (IoTs etc.)	kindly clarify what kind of IoT assets to ve covered as part of the scope.	Please adhere to the published guidelines of the RFP
Ernst & Young LLP	29	56	Appendix E-Deliverables/ scope of work	o Compromising Active Directory (AD) and tampering with EDR/Antivirus solution o Explore the feasibility if the source code of the bank products could be changed during their red team activities without bringing the application down o Exposing the vulnerabilities by lateral movement in Bank's internal network	For the mentioned scenarios, should the Red Team exercise be conducted with an external Red Team when internal network access is achieved through external penetration testing, or will the internal Red Team exercise be conducted under the assumption of a "breach scenario" If the internal Red Team exercise is to be conducted, will the bank provide the necessary systems and infrastructure for testing	Please adhere to the published guidelines of the RFP
Ernst & Young LLP	30	NA	NA	NA	If selected as successfull bidder, request you to kindly include the following clause in scope of work section:-	Please adhere to the published guidelines of the RFP

					"The provisions of this Section apply to Testing Services. Testing Services include scanning, penetration, intrusion testing or related analysis of the Client's information systems or enterprise whether by using intrusive or passive techniques and software tools. The Client hereby consents to EY performing the Testing Services and shall obtain all necessary consents of third party service providers of the Client to such Testing Services. If the Testing Services will be performed with respect to any information systems, applications or components that are hosted by any third party such as an internet service provider or application service provider then the consent shall be in the form separately provided by EY to the Client at the latter's request.	

					The Client understands that Testing Services may result in disruptions of and/or damage to the Client's or third party's information systems and the information and data contained therein, including but not limited to denial of access to a legitimate system user, automatic shut-down of information systems caused by intrusion detection software or hardware, or failure of the information system. The Client is solely responsible for understanding the testing steps that will be performed as part of the Testing Services and for arranging alternative means of operation should such disruptions or failures occur and for all damage caused by the Testing Services. EY shall have no responsibility or liability for, and the Client and its affiliates shall have no recourse, and shall bring no claim, against EY or any EY Entity, or against any subcontractors, members, shareholders, directors, officers, managers, partners or employees of any of EY or any other EY Entity, with respect to any liability or damages as a result of such Testing Services, including with respect to any third party claim against the Client related to or arising out of the Testing Services. *The Client shall indemnify and hold harmless the Indemnitees from and against*	

					all claims and causes of action, pending or threatened, of any kind (whether based in contract, tort or otherwise) by third parties related to or arising out of the Testing Services provided hereunder, and *liabilities, losses, damages, costs and expenses (including, without limitation, reasonable outside attorneys' fees and the allocable costs of in-house) suffered or incurred by any of the Indemnitees related to or arising out of any such claims or causes of action. The Client's subsidiaries and affiliates are deemed a third party as that term is used in this Section"*	
Ernst & Young LLP	31	NA	NA	NA	If selected as successfull bidder, request you to kindly include the following clause in SOW: *"EY may terminate this Agreement, or any particular Services, immediately upon written notice to Client if EY reasonably determines that it can no longer provide the Services in accordance with applicable law or professional obligations. ."*	Please adhere to the published guidelines of the RFP
Ernst & Young LLP	32	NA	NA	NA	If selected as successfull bidder, request you to kindly include the following clause in SOW:	Please adhere to the published guidelines of the RFP

					"Client acknowledges that the U.S. Securities and Exchange Commission regulations indicate that, where auditor independence is required, certain confidentiality restrictions related to tax structure may render the auditor to be deemed to be non-independent or may require specific tax disclosures. Accordingly, if and only to the extent that U.S. Securities and Exchange Commission auditor independence regulations apply to the relationship between Client or any of Client's associated entities and any EY Firm, with respect to the tax treatment or tax structure of any transaction to which the Services relate, Client represents, to the best of its knowledge, as of the date of this Agreement, that neither Client nor any of its affiliates has agreed, either orally or in writing, with any other advisor to restrict Client's ability to disclose to anyone such tax treatment or tax structure. Client agrees that the impact of any such agreement is its responsibility"	