Addendum to Annexure 13 of RFP is provided below.

All other Terms & Conditions are same as per our RFP no. BCC:CISO:111:111:448 dated 22-Nov-2019 for Selection of Service Provider For Conducting Compromise Assessment.

Annexure 13 – Technical Specifications

This annexure lists the Mandatory Technical requirements from the Bank to fulfill its objective. Compliance of the technical requirements shall mean complete compliance and not partial compliance.

S. No.	Description	Compliance (Yes/No)	Remarks
Personnel Expertise			
1	The personnel engaged in the activity must have atleast 5 years hands on experience in identifying compromises and responding to breaches along with malware and/or IOC analysis.		
2	The personnel engaged in this activity must have at least one or more of cyber security related valid certifications such as OSCE, OSCP, GCFA, GCFE, CISSP, CISA, CEH, etc.		
Technology and Tools			
3	The bidder/OEM must provide the technology deployed for searching the systems for Compromise Assessment. Any agents / clients / software distribution tool including applicable licenses should be provided by the bidder.		
4	The bidder/OEM must have threat intelligence which must be utilized for the purpose of the compromise assessment.		
5	The bidder/OEM must provide technology to deploy and monitor network traffic in order to identify signs of attacker activity, Backdoor command and control connections and traffic towards malicious IP addresses and malicious domains.		
6	The bidder/OEM must provide standard tools and scripts for analysis of systems and they must be compatible with existing technologies and architecture of Bank's network.		
Methodology			
7	The bidder/OEM must have the capability to analyze and provide details on all stages of attack: Initial reconnaissance, compromise, establish foothold, escalate privileges, internal		

S. No.	Description	Compliance (Yes/No)	Remarks
	reconnaissance and final attack.		
8	The bidder/OEM must be able to utilize a mix of automated and manual techniques to identify indicators of compromise and submission of exhaustive reports to the Bank. Bidder must also have the ability to perform malware analysis and reverse engineering of malware samples		
9	The bidder/OEM must be able to search for various artifacts of malicious threat vectors including but not limited to persistence mechanisms, lateral movement mechanisms, registry keys update, malicious process, etc.		
10	The bidder/OEM must be able to conduct log data analysis activities if necessary		
11	The bidder/OEM should be able to provide response options / recommendations to the findings in compromise assessment		
12	The bidder/OEM must be able to develop a long-term strategy / remediation roadmap to address systemic weaknesses identified during the assessment.		
13	The bidder/OEM must be able to develop plan of incident response, from the initial detection to the final resolution of the incident.		
14	The bidder/OEM must have the capability to detect non-malware attacker activity, behavioral based attacks, insider threat including misuse of privileged credentials.		
Analysis and Reporting			
15	The bidder/OEM must be able to provide comprehensive details of assessment with recommendations in the form of reports		
16	The bidder/OEM must be able to Provide Executive reports for high-level managers and non-technical stakeholders based on the details of the assessment as per Bank's requirement.		
17	The bidder/OEM must be able to provide system wise report along with certification to move the system to BOB network.		
Licenses			
18	The bidder/OEM must have appropriate licenses, as applicable, for proposed tools and technology for compromise assessment.		