S. No.	RFP Page No	RFP Section No.	Content of Section (Details from RFP document)	Query/ Suggestion/ Clarification required	IFTAS Response
1	5	2.2 Important Dates	Last date for submission of Technical and Commercial Bid (Softcopy) 21st April 2022 before 5 PM	Timeline to submit the bid is very stringent. Due to multiple levels of approval, request you to provide 7-10 additional working days to submit the bidding document.	As per RFP
2	5	2.2 Important Dates	Last date for submission of Technical and Commercial Bid (Softcopy) - 21st April 2022 before 5 PM	Request you to kindly provide an extension to submit RFP Response by 29th April'22	As per RFP
3	7	3.2 Definition	x. "Contract Period" means the period of 5 years from the date of completion of audit, validation & certification by all the OEMs for their respective products, constituting the solutions. Start date for the contract period will be the date on which certifications from all OEMs are submitted by the bidder.	What is the total contract duration of this project? Do we need to provide commercials for 1 year or for 5 years? What is the total project duartion like what will be the expected audit start date and end date?	This is not applicable for the engagement. The audit requirement is a one time activity.
4	8	3.2 Definition	Xi. Support & Comprehensive Annual Maintenance Contract (AMC) is a post acceptance support of the solution/project for the Contracted Period. Under AMC, the Bidder shall provide comprehensive support and services for all the hardware components of the proposed solution at all the project locations of IFTAS.	RFP is for Comprehensive Cybersecurity Assessment , but as mentioned in the definition 'bidder shall provide comprehensive support and services for all hardware and components'. This is not clear to us why is AMC for hardware and components is responsibility of the bidder as we understand the project scope is limited to one time security assessment / process review Kindly elaborate more on this point with respect to the scope of work.	This is not applicable for the engagement
5	9	3.3 Instruction to bidders	ix. Annexure - IX: Performance Bank Guarantee	Kindly specify if bank guarantee has to be submitted only by the successful bidder.	Bank gaurantee is Only for successful bidder.
6	11	5. Scope of work	Kindly specify if IFTAS would allow the bidder to work remotely.	Kindly specify if IFTAS would allow the bidder to work remotely.	Its onsite engagement
7	11	5. Scope of work	KPMG will not perform any re-configuration audit or re-assement audit for the gaps identified.	KPMG will not perform any re-configuration audit or re-assement audit for the gaps identified.	"Content of section" is not mentioned.
8	11	5. Scope of work	Scope of work	Kindly specify if the scope of work is including the cloud infrastructure as well. If Yes, kindly specify cloud infra details.	Captive Private / Community Cloud known as IBCC
9	11	5. Scope of work 2 IT Managemen t and Processes	Review and evaluate the IT Governance, Policy, Procedures as per the ISO 27001 / NIST standards, which include: IT Asset Management Security Incident Management Change Management SLA Management Project Management Patch Management Health and Performance Monitoring Vendor Management IT Outsourcing process IT Procurement process	Kindly specify if this only process review or tool review is also expected from the auditor. If yes, kindly specify the exact name and number of the tools used Kindly specify below the number and type against each IT Asset Management - Number of asset Security Incident Management - Does this include only the security incidents or general incidents as well Project Management - Types of projects Vendor Management - List and category of vendors	Process review along with records verification as per sampling technique

10	11	5. Scope of work 3.2	Assess IFTAS' current cyber security measures/controls with industry best practices, business objectives and regulatory requirements. Which should include study of cyber security components such as Anti-malware protection, Email Security, vulnerability management, patching	Kindly specify this review needs to performed basis which RBI guidelines. Also kindly share the exact circular numbers	As per RFP
11	11	5. Scope of work 3.3	The auditor shall review security controls implemented for endpoints (Desktop, Laptop & Servers) as per best industry practices.	Kindly specify this review needs to performed basis which RBI guidelines. Also kindly share the exact circular numbers	As per RFP
12	11	5 Scope of W	General	Frequency of Audit (Monthly, Annual, Quarterly, etc) What is the employee count? How many numbers of departments are present? How many applications are there in scope? How many critical processes in scope for BCP? Kindly provide total number of endpoints, Server, Network and other IT Infrastructure. Kindly confirm whether the project will be delivered in onsite or offsite mode?	1. One time engagement 2. approx. 300 3. 8 4. As per RFP 5. As per RFP 6. Around 1000, exact detail will be shared with successful bidder 7.Onsite
13	11	5 Scope of work	Scope of Work	Kindly share the device count and OS versions for the devices for which configuration review to be done.	1. Endpoint Windows 10 (Around 300), 2. Server OS are Windows 2012 and 2016 Open Source Linux (Around 550), including Prod, DR, UAT 3. Bidder shall use the sampling technique with 5% of production environment
14	11	5 Scope of work	Scope of Work	Please specify the solutions implemented for malware protection, email security, vulnerability management and patching.	OEM Detail will be shared with successful bidder, implemented solutions are: 1. Antispam with Anti-APT 2. Vulnerability Management 3. Patching 4. EDR
15	11	5 Scope of work - IS Policy	Review and evaluate the Information Security Policy as per the ISO 27001 / NIST standards with respect to Confidentiality, Integrity & Availability.	Request you to kindly elaborate whether the bidder has to evaluate the information security policy from an implementation effectiveness perspective.	No, Bidder has to review the Information Security Policy document to validate that advance Cyber Security Control are addressed
16	11	5 Scope of work - IT Managemen t	Review and evaluate the IT Governance, Policy, Procedures as per the ISO 27001 / NIST standards	Request you to kindly elaborate whether the bidder has to evaluate the IT Governance, Policy, Procedures from an implementation effectiveness perspective.	Yes
17	11	5 Scope of work - Cyber Security	Review existing Cyber Security Policies, Framework, Standards, and Processes	Request you to kindly elaborate whether the bidder has to evaluate the Cyber Security Policies, Framework, Standards, and Processes from an implementation effectiveness perspective.	Yes, the implementation and effectiveness of Cyber Security controls

18	11	5 Scope of work - Cyber Security	Assess IFTAS' current cyber security measures/controls with industry best practices, business objectives and regulatory requirements. Which should include study of cyber security components such as Anti-malware protection, Email Security, vulnerability management, patching, etc.	1. Request you to provide detailed list of in-scope cyber security components for review. The same is required for effort estimation purpose. 2. Request you to elaborate whether the bidder is required to conduct configuration review of the in-scope cyber security components. 3. Request you to elaborate whether the bidder is required to conduct effectiveness review of the in-scope cyber security components	1. Anti-malware, Email Security, Vulnerability Management, Proxy, Firewall, IPS, Proxy, PIM, WAF, DDoS, Next Generation SIEM, 2. Yes, sampling technique 3. Yes
19	11	5 Scope of work - Cyber Security	Assess the "segregation of duties" control with respect to project implementation, development, testing, administration, operation, and monitoring roles.	1. Request you to elaborate whether is bidder is expected to assess the "segregation of duties" of the cybersecurity components as stated in section scope of section (3.2). 2. Request you to clarify whether the bidder is expected to assess the "segregation of duties" of any other components apart from the cyber security components as stated above	Yes (Anti-malware, Email Security, Vulnerability Management, Proxy, Firewall, IPS, Proxy, PIM, WAF, DDoS, Next Generation SIEM,)
20	11	5 Scope of work - Cyber Security	The auditor shall review the Cyber Security processes for: ▯ Security events / alerts monitoring (SOC) ▯ Cyber Security Incident Management ▯ Threat / Vulnerability Management ▯ Impact Analysis, and Risk Assessment ▯ Baselining / Hardening control for IT assets	1. Request you to kindly elaborate whether the bidder has to evaluate the mentioned processes from an implementation effectiveness perspective. 2. Request you to clarify whether the bidder is expected to review the SOC architecture from security perspective. 3. Request you to clarify whether the bidder is expected to review the baselining/hardening documents.	1. No 2. No 3. No
21	11	5 Scope of work - Network Security	The auditor should review the configuration and policies of perimeter security controls such as Firewall, IPS, WAF, DDoS, Proxy, etc. to ensure that it meets industry security standards.	Request you to provide detailed list of in-scope perimeter security controls for review. The same is required for effort estimation purpose.	1 x Firewall/IPS Management System 1 x Internet Network Firewall/IPS 1 x Internal Network Firewall/IPS 1 x Cloud Firewall (NSX-T) 1 x DDoS 1 x WAF 2 x Anti-virus Solution 1 x EDR Solution 1 x Sandboxing 1 x Email Security 1 x Proxy Setup 1 x Vulnerability Management, 1 x PIM 1 x Next Generation SIEM
22	12	5 Scope of work - LAN / WAN / Extranet Network	The auditor should review the configuration of the routers and switches deployed in IFTAS location and datacenter to ensure that the configuration meets current policies, procedures, and controls and/or industry security standards, to include port status, encryption, routing configurations and various hardening parameters.	Request you to provide the count of routers and switches for review. The same is required for effort estimation purpose.	1 x DC Router 1 x Internet Router 2 x DC Switch 4 x INFINET Routers (DC Site) 4 x INFINET Routers (Member Bank Site) 1 x Branch Router 1 x Branch Switch

23	12	5 Scope of work - Identity & Access Management	Review membership of privilege groups configured in Windows domain	Request you to clarify if the review can be performed on a sampling basis. If yes, kindly specify a sample size (E.g. 5 privilege groups) for the review.	10 - 15 Groups
24	12	5 Scope of work - Identity & Access Management	Review policy / configuration for general user level access and privileged user access	Request you to clarify if the review can be performed on a sampling basis. If yes, kindly specify a sample size (E.g. 5 general users and 5 privilege users) for the review.	10 General user from different departments 5 privilege user
25	12	5 Scope of work - Identity & Access Management	Review of database privileges assigned to Administrator, Applications, and General Users	Request you to clarify if the review can be performed on a sampling basis. If yes, kindly specify a sample size (E.g. 5 Administrators, 5 Applications, and 5 General Users) for the review.	10~15 administrator / application accessing the database
26	12	5 Scope of work - Identity & Access Management	Review Privilege Identity / Access Management (PIM/PAM) control	Request you to elaborate whether the bidder is required to conduct configuration review of the PIM/PAM control.	Yes
27	12	5 Scope of work - Identity & Access Management	Review remote access methods for Staff, Vendor, and other 3rd parties	1. Request you to elaborate on what are the different methods for remote access currently being used at IFTAS. 2. Request you to clarify if the review can be performed on a sampling basis. If yes, kindly specify a sample size (E.g. 5 staff, 5 vendors) for the review.	1. VPN and VDI 2. 3 Staff and 3 Vendor
28	12	5 Scope of work - Windows Domain Environment	Review architecture of the Windows Domain, Trees, Forests, and trust relationship	Request you to provide the count of each of the following which are present in the IFTAS architecture: - Number of Domains - Number of Trees - Number of Forests - Number of trust relationships The same is required for effort estimation purpose	IFTAS has one primary domain, one tree and one forests where 4 DNS zone and 15 OU are configured
29	12	5 Scope of work - Windows Domain	Review Windows Domain policy	Request you to clarify if the review can be performed on a sampling basis. If yes, kindly specify a sample size for the review.	One GPU Policy
30	12	5 Scope of work - Windows Domain Environment	Review Windows Share drive access for creeping privilege	Request you to clarify if the review can be performed on a sampling basis. If yes, kindly specify a sample size (E.g. 5 share drives) for the review.	One Share folder server with 47 share folders
31	12	5 Scope of work - Application Security	Review the software development process	What is the current process for software development - Agile, DevOps, etc?	Mixed
32	12	5 Scope of work - Application Security	Review the critical applications of IFTAS which include, ITSM, Email System, SIEM, SFMS Payment applications, Captive Cloud hosting Solution, ERP, PIM	Request you to kindly elaborate on 'captive cloud hosting solution'	VMware Private cloud

33	12	5 Scope of work - Application Security	Review application change management process	1. Request you to kindly elaborate whether the bidder has to evaluate the application change management process from an implementation effectiveness perspective. 2. Request you to clarify if the review can be performed on a sampling basis. If yes, kindly specify a sample size (E.g. 5 change management requests) for the review	Review the Process 1. No 2. NA
34	12	5 Scope of work - Application Security	Application administration and monitoring process	1. Request you to kindly elaborate whether the bidder has to evaluate the Application administration and monitoring process from an implementation effectiveness perspective. 2. Request you to clarify if the review can be performed on a sampling basis. If yes, kindly specify a sample size (E.g. 5 applications) for the review.	1. Yes 2. Yes Review the critical applications of IFTAS which include, ITSM, Email System, SIEM, SFMS Payment applications, Captive Cloud hosting Solution, ERP, PIM
35	12	5 Scope of work - Application Security	User Authentication, authorization, access control and password management	Request you to clarify if the review can be performed on a sampling basis. If yes, kindly specify a sample size (E.g. 5 applications) for the review.	As per RFP Review the critical applications of IFTAS which include, ITSM, Email System, SIEM, SFMS Payment applications, Captive Cloud hosting Solution, ERP, PIM
36	12	5 Scope of work - Application Security	Segregation of duties	Request you to clarify if the review can be performed on a sampling basis. If yes, kindly specify a sample size (E.g. 5 applications) for the review.	As per RFP Review the critical applications of IFTAS which include, ITSM, Email System, SIEM, SFMS Payment applications, Captive Cloud hosting Solution, ERP, PIM
37	12	5 Scope of work - Application Security	Review the user roles as per "Need to Know" and "Least Privilege" principles	Request you to clarify if the review can be performed on a sampling basis. If yes, kindly specify a sample size (E.g. 5 applications) for the review.	As per RFP Review the critical applications of IFTAS which include, ITSM, Email System, SIEM, SFMS Payment applications, Captive Cloud hosting Solution, ERP, PIM
38	12	5 Scope of work -Data Centre Audit	1. Review Logical & Physical Access Control 2. Review Building Management Systems, Power Supply, UPS & DG 3. Review Data Centre infrastructure – network cabling, server / Communication racks, Power Distribution Units (PDU), KVM 4. Review the surveillance systems	Is the bidder expected to travel to the data centre locations of IFTAS - Mumbai & Hyderabad for the review.	Yes
39	12	5. Scope of work 3.5	The auditor shall review the Cyber Security processes for: ▯ Security events / alerts monitoring (SOC) ▯ Cyber Security Incident Management ▯ Threat / Vulnerability Management ▯ Impact Analysis, and Risk Assessment ▯ Baselining / Hardening control for IT assets	Kindly specify if this only process review or tool review is also expected from the auditor. If yes, kindly specify the exact name of the tool used along with the number of tools used for this process	Process review along with records verification as per sampling technique

40	12	5. Scope of work 4.2	The auditor should review the configuration and policies of perimeter security controls such as Firewall, IPS, WAF, DDoS, Proxy, etc. to ensure that it meets industry security standards.	Kindly specify against which guidelines and number of Firewall, IPS, WAF, DDoS, Proxy involved. Also specify if any other tool needs to be included in this	As per RFP
41	12	5. Scope of work 5.1	The auditor should review the configuration of the routers and switches deployed in IFTAS location and datacenter to ensure that the configuration meets current policies, procedures, and controls and/or industry security standards, to include port status, encryption, routing configurations and various hardening parameters	Kindly specify against which benchmarks this review needs to be performed. Example CIS etc. Also specify the exact number of IP's or the exact number of switches and routers	CIS
42	12	5. Scope of work 8.3	Review application change management process	Kindly specify if only the process needs to be reviewed or the tool as well	Review the Process
43	12	5. Scope of work 9.4	Review the surveillance systems	Kindly specify list of surveillance systems used	CCTV at 3rd Party DC Location
44	12	5. Scope of work 11	Assess the maturity level of the IFTAS in the cybersecurity space including the review of policies, procedures and implemented controls. The assessment should be performed in following the 5 function areas and associated categories. Identify Protect Detect Respond Contain Recover	Kindly specify if this activity needs to be performed against any specific framework For Example : NIST Framework (V1.1)	The Bidder has to propose the best which meet IFTAS requirement
45	12	5. Scope of work 9	Data center audit	This audit will be performed for 3 locations (Mumbai 2 and Hyderabad 1) Also confirm whether Hyderabad will be considered as DR site.	IFTAS Host the private cloud, hence Mumbai and Hyderabad are DC site and referred as Availability Zone
46	12	8.9	Application Security	Kindly specify the number of storage and database used. Also does this include the cloud infrastructure as well.	Will be shared with successful bidder
47	12	5 Scope of Work (Application Security)	Review the critical applications of IFTAS which include, ITSM, Email System, SIEM, SFMS Payment applications, Captive Cloud hosting Solution, ERP, PIM	Do we need to perform the security testing of the applications (app VAPT) mentiond (ITSM, Email System, SIEM, SFMS Payment applications, Captive Cloud hosting Solution, ERP, PIM)? If yes, kindly provide below details for estimation: Application Names: No of dynamic pages for each application: No of lines of code for each application:	No
48	12	5 Scope of work	Data Centre Audit	Data Centre audit – Please specify the expectations from the review of BMS, Power supply, UPS, DG and Data Centre infrastructure	As per RFP

49	13	5 Scope of work - Business Continuity	Review Business Continuity Plan (BCP) and Disaster Recovery (DR) plan	Request you to kindly elaborate whether the bidder has to evaluate the Application administration and monitoring process from an implementation effectiveness perspective.	No for this "Content of Section"
50	13	5 Scope of work - Business Continuity	Review Resiliency and High Availability implemented for critical applications.	Request you to clarify if the review can be performed on a sampling basis. If yes, kindly specify a sample size (E.g. 5 applications) for the review.	Yes, 10
51	13	5 Scope of work - Business Continuity	Review Resiliency and High Availability implemented for critical applications.	Request you to confirm the no of applications for which review needs to be performed	10
52	13	5 Scope of work - Business Continuity	Review BCP and DR test results	1. Kindly elaborate if the bidder is expected to conduct a DR/BCP drill. 2. Request you to clarify if the review can be performed on a sampling basis. If yes, kindly specify a sample size (E.g. 5 previously conducted BCP and DR test results) for the review.	1.No 2.Yes, 5
53	13	5 Scope of work - Business Continuity	Review Data Backup and Restoration process	1. Request you to kindly elaborate whether the bidder has to evaluate the Data Backup and Restoration process from an implementation effectiveness perspective. 2. Request you to clarify if the review can be performed on a sampling basis. If yes, kindly specify a sample size (E.g. Data Backup and Restoration process of 5 applications) for the review.	1.Yes 2.Yes, 5
54	13	5 Scope of work - Business Continuity	Data / database Synchronization process between DC / DR	1. Request you to kindly elaborate whether the bidder has to evaluate the Data / database Synchronization process from an implementation effectiveness perspective. 2. Request you to clarify if the review can be performed on a sampling basis. If yes, kindly specify a sample size (E.g. Data Backup and Restoration process of 5 databases) for the review.	1.Yes 2.Yes, 5
55	14	7. Project Milestones	3 Audit Execution Within 8-10 weeks from the date of the PO	We would request for an extension in audit execution by 4 weeks, considering the audit scope.	As per RFP
56	15	8 Eligibility Criteria	The Bidder shall have a minimum annual turnover of at least Rs. 50 Crore in each of the last three financial years (for e.g., 2018-19, 2019-20 & 2020-21). The Bidder shall have positive net worth in each of the last three financial years	Tax slab looks high. We request you to please revise the turnover ceiteria as Average Turnover will be 10 cr for the following financial years (2018-19, 2019-20 and 2020-21).	As per RFP, applicable for all bidders.
57	15	7. Project Timeline	Project timeline	The timeline of 8 to 10 weeks for Audit Execution, mentioned in the RFP looks less compared to the scope mentioned. Please extend the timeline to 12 to 14 weeks.	As per RFP

58	16	9.2 Technical Evaluation Matrix	Across the entire table	Request you to kindly provide the breakup for maximum marks against the details mentioned in the column/ (example:- For "Number of resources having certification CISSP / CISA / CISM, who will be working on IFTAS Audit requirement.", what shall be the breakup of 25 marks against the details mentioned in 3rd column of the table)	As per RFP
59	16	9.2 Technical Evaluation Matrix	Experience of a Bidder in Conducting similar Audit	What is the minimum number of similar audits the bidder must have conducted to score full marks?	Bidder shall have done the IT / Information System / Information Security audit for minimum 3 BFSI customer in Year 2021.
60	16	9.2 Technical Evaluation Matrix	Number of resources having certification CISSP / CISA / CISM, who will be working on IFTAS Audit requirement	What is the minimum number of certified resources the bidder must have conducted to score full marks?	Evaluation committee will evulate the proposal of each bidder along with resources sized to meet IFTAS requirement
61	16	9.2 Technical Evaluation Matrix	1.Capabilities in Audit / Assessment work 2. The size of auditing team 3. Independent Evaluators Report 4. Market Review and Feedback	1. Request you to confirm the submission document for "Independent Evaluators Report" which needs to added as part of our response. 2. Request you to confirm the submission document for "Market Review and Feedback" which needs to added as part of our response	Bidder to provide as part of proposal
62	16	9.2 Technical Evaluation Matrix	An eligible Bidder along with their proposed OEM/s will be invited to IFTAS to make an exclusive presentation detailing the proposed solution, implementation approach, rollout strategy etc. for the solution. The Bidder is required to present details of the proposed hardware and its related environment, configuration etc. keeping in view the requirements of the solution	Request you to kindly provide elaboration for these 2 points as we understand that current RFP is to perform audit against the scope of work. Request you to confirm the involvement of OEM/s and implementation of solution during the technical evaluation phase	Please read as " An eligible Bidder will be invited to IFTAS to make an exclusive presentation detailing the proposed solution, implementation approach, rollout strategy etc. for the solution"
63	20	Clause 18 Page 20	Audit & Inspection	Team to propose the following- Any audit shall be subject to the following: (I) the audit shall be restricted to the engagement and shall be conducted with prior reasonable notice (ii) client or its authorized representatives shall execute a Non-Disclosure Agreement before such audit which shall govern the conduct of audit and any results thereof; (iii) the auditors or the representatives of client for the audit shall not be bidder's competitors; (iv) the audit shall not be conducted more than once in a calendar year and twice in entirety; and (v) any findings during the audit, shall be shared with client and be discussed and agreed mutually client and bidder for its closure.	As per RFP
64	22	24	Cyber Security Compliance Certifi	We shall not provide any such certificate	As per RFP
65	23	Clause 27 Page 23	Arbitration	Team to propose amendment here that any dispute arising under this RFP/contract shall be referred to arbitration in accordance with the Arbitration and Conciliation Act, 1996, as amended from time to time. The sole arbitrator shall be appointed by the parties basis mutual agreement. The Arbitration shall be in English	As per RFP

66			General	Please specify any regulatory circulars or guidelines which need to be used as baseline for assessment	No
67			General	Request you to kindly include Quality Cost Based Selection (QCBS selection method) in the selection criteria of bidders	As per RFP
68	12	5 Scope of work	Conduct Network Security Architecture review as per best industry practices The auditor should review the configuration and policies of perimeter security controls such as Firewall, IPS, WAF, DDoS, Proxy, etc. to ensure that it meets industry security standards. Review the network segmentation	Please provide details and number of the assets to be considered for Security device configuration review? How many VLANs are present?	1 x Firewall/IPS Management System 1 x Internet Network Firewall/IPS 1 x Internal Network Firewall/IPS 1 x Cloud Firewall (NSX-T) 1 x DDoS 1 x WAF 2 x Anti-virus Solution 1 x EDR Solution 1 x Sandboxing 1 x Email Security 1 x Proxy Setup 1 x Vulnerability Management, 1 x PIM 1 x Next Generation SIEM
69	12	5 Scope of work	The auditor should review the configuration of the routers and switches deployed in IFTAS location and datacenter to ensure that the configuration meets current policies, procedures, and controls and/or industry security standards, to include port status, encryption, routing configurations and various hardening parameters. Review the network segmentation	Please provide details and number of the assets to be considered for network device configuration review?	1 x DC Router 1 x Internet Router 2 x DC Switch 4 x INFINET Routers (DC Site) 4 x INFINET Routers (Member Bank Site) 1 x Branch Router 1 x Branch Switch
70	12	5 Scope of work	Review the software development process		No query from the bidder
71	12	5 Scope of work	Review the critical applications of IFTAS which include, ITSM, Email System, SIEM, SFMS Payment applications, Captive Cloud hosting Solution, ERP, PIM	Do we need to conduct WASA of the applications? How many applications are present? Whatare the sizes of the Applications? For ERP, how many modules are present and what are they? Please specify the exact requirement from the SEIM review	1. No 2. As per RFP