

This is with reference to the Request for Proposal (RFP) Ref. No. IFT/GRC/260422 issued by IFTAS.

S.no	Page No.	RFP Section	RFP Clause	Query from Bidder	IFTAS Response
1	5	1.2 Objective	Generic	Do you currently have any GRC tool in place to manage current GRC activities in IFTAS?	No
2	5	1.2 Objective	Generic	What kind of existing documentation are available for existing GRC solutions?	Not applicable.
3	5	Scope of work	IFTAS intends to configure and implement Governance, Risk, and Compliance (GRC) Management solution. The Solution should have below capabilities: 1 Information Security Policy Compliance Management 2 IT Compliance Management, which include global standards ISO 27001, PCI DSS, NIST, etc. 3 IT / Cyber Security Risk Management 4 IT / Cyber Security Audit Management 5 Business Continuity Management (BCM) 6 Control Self Assessments (CSA) by using assessment questionnaires	Has IFTAS identified any tools for GRC tool? If yes please provide names of the tool/vendor.	There are no specific tools that have been identified.
4	5	Scope of work	The Solution should have below capabilities: 1 Information Security Policy Compliance Management 2 IT Compliance Management, which include global standards ISO 27001, PCI DSS, NIST, etc. 3 IT / Cyber Security Risk Management 4 IT / Cyber Security Audit Management 5 Business Continuity Management (BCM) 6 Control Self Assessments (CSA) by using assessment questionnaires	Does IFTAS have framework/policy/procured implemented/documented around following GRC Processes ? 1 Information Security Policy Compliance Management 2 IT Compliance Management, which include global standards ISO 27001, PCI DSS, NIST, etc. 3 IT / Cyber Security Risk Management 4 IT / Cyber Security Audit Management 5 Business Continuity Management (BCM) 6 Control Self Assessments (CSA) by using assessment questionnaires	We have Information security policy documented.
5	6	2.2. RFP Procedure - Important Dates	Last date for submission of Technical and Commercial Bid (Softcopy) 17th May 2022 on or before 5 PM	Request to kindly extend the Submission of Bid by 2 weeks to 31st May 2022 so as to provide enough time for the Bidder to collate the required information for the Bid	As per RFP
6	10	5 Scope of work	Services	Does your organization want the vendor to study and define/refine the process / framework for Risk Management, Policy & Compliance Management, Audit Management and Business Continuity Management as part of consulting engagement?	Yes
7	10	Technical Specifications	The Bidder shall supply, install, configure, integrate, and support all the necessary software components required for the Solution mentioned in this RFP.	Is IFTAS open to procure licenses from tool vendor directly and only Implementation will be done by bidder?	Bidder to provide complete solution as per Requirement

8	10	Technical Specifications	The solution shall be integrated with existing Windows AD environment, and SIEM solution.	Kindly confirm and provide details of the below-listed external systems to be integrated with the GRC system: Windows AD environment, SIEM solution If any other external system is required to be integrated with GRC tool please provide details of the same.	ITSM,VAPT tool etc.
9	10	Technical Specifications	The Bidder shall supply, install, configure, integrate, and support all the necessary software components required for the Solution mentioned in this RFP.	Most of the GRC systems offers Out of the Box (OOB) user cases which are designed based of leading GRC practices. Considering IFTAS would be procuring these OOB user cases, what level of customization would you require in the these pre-built workflows, reports, dashboards, roles etc.?	The tool needs to be customized to suit IFTAS practices in line with the GRC best practices.
10	10	Technical Specifications	The Bidder shall supply, install, configure, integrate, and support all the necessary software components required for the Solution mentioned in this RFP.	Does IFTAS have business requirement for following GRC use cases documented ? 1 Information Security Policy Compliance Management 2 IT Compliance Management, which include global standards ISO 27001, PCI DSS, NIST, etc. 3 IT / Cyber Security Risk Management 4 IT / Cyber Security Audit Management 5 Business Continuity Management (BCM) 6 Control Self Assessments (CSA) by using assessment questionnaires	IFTAS has documented Information Security policy
11	10		The Bidder shall supply, install, configure, integrate, and support all the necessary software components required for the Solution mentioned in this RFP.	How many different environment is expected to be deployed (Development, UAT, Production, DR etc.)	UAT,PROD & DR.
12	11	6. Project Milestones	The dates mentioned for the activities are tentative in nature. The exact dates of completion of various activities shall be firm up in discussion with the successful Bidder	Request to kindly confirm if the expected implementation / Production release timelines is approximately 11-12 weeks from issuance of PO. Request if a tentative timeline of 20-24 weeks can be considered for implementation period to be further discussed once the detailed requirements are finalised	Timelines as per RFP, To be finalised with successful bidder

13	11	7. Eligibility Criteria	Those Bidders, who satisfy all the eligibility criteria as mentioned herein below, may only respond. Documents in support of all eligibility criteria are required to be submitted along with the Technical Bid. Offers received from the Bidders who do not fulfill any of the following eligibility criteria are liable to be rejected	Request to kindly confirm if a Consortium will be considered as eligible for submitting the Bid	Participant Bidder to comply with RFP eligibility criteria and other terms of conditions.
14	11	Support and Maintenance	The dates mentioned for the activities are tentative in nature. The exact dates of completion of various activities shall be firmed up in discussion with the successful Bidder.	We understand that IFTAS is looking to complete the implementation in 4 months. From our experience we would advise on a phased approach, would IFTAS accept phasing?	Timelines as per RFP, To be finalised with successful bidder
15	11	Technical Specifications	Successful bidder shall assign project manager and associated support personnel for the onetime implementation.	Will the work be conducted remotely, on-site, or a hybrid solution including both remotely and on-site?	On-site at IFTAS premises.
16	11		Execute User Acceptance Test (UAT) for the proposed solution, i.e., minimum 2 users from each department. Acceptance shall be based on the results of the test cases. If during the test period, the proposed Solution experiences no failures and functions according to the requirements of the RFP, as determined by IFTAS, the Solution shall be considered accepted.	As part of User Acceptance Testing (UAT), will assist in conducting two rounds of UAT. Kindly confirm, would additional UAT sessions would be required?	To be discussed and agreed with successful bidder.
17	11		Bidder is required to provide OEM training (preferably onsite) to IFTAS team (for 10 persons) through authorized OEM partners for products and technology being implemented as part of this RFP.	Could IFTAS confirm types of trainings required ? Example: Platform Admin training or Functional or Both	Both
18	11		Bidder is required to provide OEM training (preferably onsite) to IFTAS team (for 10 persons) through authorized OEM partners for products and technology being implemented as part of this RFP.	Could IFTAS confirm types of trainings required ? Example: training for top IFTAS executives, training for stakeholders from departments, "train the trainer" training etc. Also, kindly confirm how many training sessions would be required for each of these training types.	Trainings for various stakeholders from verticals.
19	11		Bidder is required to provide OEM training (preferably onsite) to IFTAS team (for 10 persons) through authorized OEM partners for products and technology being implemented as part of this RFP.	What kind of training material (SOP/Videos etc.) do you expect bidder to provide as part of training?	SOP & Live Training
20	11	Project Milestones		We feel that the timelines mentioned in the RFP are too short and we would like to request for extended timelines for each activity	As per RFP

21	12	Eligibility Criteria Point 4	Bidder shall have implementation experience of minimum	Whether experience of providing Audit & Compliance Management Software will be considered ?	As per RFP
22	12	Eligibility Criteria Point 5	The proposed solution shall be in the latest Leaders Quadrant of Gartner's Magic Quadrant or any other such - equivalent or independent evaluator.	We request a relaxation in this eligibility criteria. Instead we request IFTAS to also consider solutions made by Indian MSME's that are not appearing any of such leader quadrant.	As per RFP
23	14	10. Support and Maintenance	The successful bidder shall provide 24 x 7 support during the warranty period, ensuring the accepted level of performance as specified in "Service Level Agreement"	Request to kindly provide the following clarifications for the Support period 1. Any expected number of team members for providing the support? 2. Is the support to be provided completely from Onsite or a combination of Onsite / Offsite (Remote)? 3. Is there any existing incident raising / management application that IFTAS has for raising Support requests	Support can be a combination of onsite/remote. ITSM tool is in place for raising support requests internally.
24	14		a. Product licenses should be Enterprise licenses in the name of IFTAS on subscription basis, for the entire project contract period (i.e., for 5 Years of subscription). License date will start after acceptance from IFTAS.	What is the type of Support and Maintenance is required ? Example. Function Support (Managed Service) or Technical Support or Both	Both
25	17	12 Payment Terms and Conditions	1 Onetime installation, implementation, training, and documentation charges 100% payment After successful installation and training and submission of documents. 2 Subscription Cost Quarterly Subscription cost will be paid quarterly in arrears	1. We request that the payment terms be reconsidered as mentioned below as the entire Application License cost would be required to be paid initially to the OEM for proceeding with implementation of the software a. 100 % License Cost to be paid initially at the start of the project / prior to proceeding with installation and implementation and significant costs need to be borne by SI / Bidder b. Implementation cost to be paid as per below i. Installation of Application in Development / UAT Environment- 10% ii. Installation of Application in Production Environment - 5% iii. Sign off of Business Requirement Document (BRD) by IFTAS - 20% iv. UAT Release - 25% v. UAT sign off - 25% vi. Production Release & Training- 15%	As per RFP

26	17	Payment Terms Sr. No.1	Ontime Installation, Implementation, Training and documentation charges – 100% payable after successful implementation and training and submission of documents.	Implementing any solution is an effort for a vendor. Hence accenting a payment of 100% after go-live may create serious issues for vendors cash flow. Therefore, we would like to request for change in the payment terms as following..... 1) 40% SRS Sign-off 2) 25% UAT Delivery 3) 25% UAT Sign-off 4) 10% Go-live	As per RFP
27	20	17. Termination of Purchase Order/Contract:	IFTAS, by written notice, may terminate the contract in whole or in part, as per the under-noted reasons, at any time by giving 90 days prior notice in writing to the Bidder	Request to kindly incorporate also a clause for the termination by SI/OEM if they can no longer provide the Services in accordance with applicable law or professional obligations	As per RFP, Bidder to evaluate complete requirement and participate appropriately.
28	24	30. Confidentiality of Information	Confidentiality	Request to kindly consider a defined period of 3 years for the Confidentiality requirements post the Expiry or Termination of the Agreement rather than a perpetual requirement	As per RFP
29	30	SI No-1 Annexure- II: Technical Specifications	Desired Tool	Is there any tool preference for GRC implementation since it is going to be On-premises ?	On Premises
30	30	SI No-2 Annexure- II: Technical Specifications	Infrastructure / Environment	Who will own the license of the GRC tool being proposed for your GRC Enterprise system consolidation?	License required on Subscription basis.
31	30	Annexure- II: Technical Specifications	Specifications / Requirements	Request to kindly provide the following clarifications for the requirements 1. Are there existing Frameworks/ Polcies detailing the requirements for Legal Compliance, IT Risk, Audit/Compliance Findings etc or will the same also have to prepared along with the business requirements documentation 2. Is there an existing Risk / Control Library and Risk assessment Framework or will the same be required to be developed? 3. Point 19 - Which external data / systems are expected to be connected via API 4. Point 72 - Is a separate module / Portal / Interface expected for external Vendors and what would be the expected information provided by these Vendors? 5. Is there historical data that will be expected to be migrated?	1. Yes. 2. Yes. Requires fine tuning. 3. AD, SIEM, VAPT, ITSM, PIM, etc. 4. No. To be considered in future. 5. No.

32	30		The Solution should have pre-mapped controls for global standards and frameworks which include, ISO 27001/27002/27005/27032, CIS, COBIT, NIST, IT Act 2000/2008, GLBA, PCI DSS, SOX, ITIL v4.0. (The bidder must provide the complete list of standards supported by the solution.)	From IT Compliance Management requirement, there would be requirement of paid license content (Example: ISO 27001 etc.). It is expected that IFTAS will procure these paid licenses. Please confirm.	Bidder to provide complete solution as per Requirement
33	30		The Solution must be an on-premises and use the IFTAS virtualization platform.	Is IFTAS open to look for SaaS based GRC tools hosted within India ?	No. On-premise solution.
34	30		The Solution should have capability to integrate with various security controls such as MS Active Directory, SIEM, Vulnerability Management, PIM, ITSM tool etc.	Please provide details (Product name and version in use) of external system which IFTAS wants GRC tool to be integrate with.	To be shared with Successful bidder
35	30		The Solution should document the IT and Cybersecurity infrastructure including overview of business products/services, business processes, information assets, facilities and personnel and hierarchy of the Department.	How does IFTAS current organizational structure and business hierarchy look like? (For example: IFTAS > Subsidiaries > Divisions > Business Units>Process & Service > Assets)	To be shared with Successful bidder
36	31		The Solution should be able to demonstrate control effectiveness metrics measurements in a comparable way against thresholds decided for metrics.	What is the current framework that IFTAS has in place? Can IFTAS elaborate as to what parameters are expected?	To be shared with Successful bidder
37	32	SI No - 41 Annexure- II: Technical Specifications	Data Archival	"The solution must keep the History of last 7 years risk." - Technically as long as it is needed GRC tool can keep the historical data. It is just that with time, the size will start growing exponentially. Hence, it is necessary to review after 4 years on the need for keeping historical data. Is 7 years of historical data mandatory from IFTAS perspective?	Yes
38	32	Annexure II - Point 41	The solution must keep the History of last 7 years risk.	We request the Bank to kindly specify the size of the data. It will help us to arrive at hardware specifications required for the solution.	The bidder to provide Hardware requirement, IFTAS shall arrange the Hardware
39	33	SI No-74 Annexure- II: Technical Specifications	Services	"The Solution should provide Enterprise risk management system and Enterprise Audit Management. This is future requirements, and must be activated by using a separate module license. " The Enterprise solutions are basic modules required for managing and assessing business assets and business hierarchy, but this is this only needed as part of future scope and not for intial use. But, technically it is recommended to have this configured as part of the ongoing work. Please confirm.	Yes, bidder to consider this.
40	34	Annexure- III: Commercial Bid	License	Is the vendor expected to provide the Tool license cost as well as part of this RFP proposal?	Bidder to provide complete solution as per Requirement

41		Generic	Generic	How is Production release performed? Are there any tools being used like (TFS, RLM, Jenkins, GitHub, and so on)?	To be shared with Successful bidder
42		Generic	Generic - Sizing	What is the expected average record size ?	To be shared with Successful bidder
43		Generic	Generic	If the process/framework is currently available, what is the format of the data? Is it available in .CSV format?	Yes .CSV format
44		Generic	Generic	What are the upstream and downstream data ingestion and sharing process in your GRC Organization?	Bidder to provide complete solution as per Requirement
45		Generic	Generic	Will there be any integrations (LDAP, API, Datafeed) planned with the expected GRC System?	Yes
46		6 Project Milestones	Generic	Since the mentioned timelines are only indicative, actual high level timelines will be arrived at after understanding more on the tool to be used and modules to be implemented. Is the understanding correct?	Timelines as per RFP, To be finalised with successful bidder
47		Generic	User Base	Is it that the IFTAS GRC tool will cater to only 150 users at the max going forward? Or Is the overall number of stakeholders for all solutions will still be 150?	Yes, but the solution should be scalable.
48		Generic	Application Access	How are end-users expected to login/sign-in to the application platform? If the end-user count is less (150), such set of users can be managed locally without AD integration (if it's not necessary by compliance). Please confirm.	Should be with AD integration
49		Generic	External exposure	Will the final GRC application be external facing (have connection to internet or internet available systems)?	No
50				Which SIEM solution (also under the scope of integration with GRC solution) is being used by IFTAS currently ?	To be shared with Successful bidder
51			Reference: Annexure II-Technical Specification Q.19	What are the data sources that IFTAS is looking forward to connect with MetricStream solution to feed in external data?	AD, SIEM, ITSM, VAPT, etc.
52			Reference: Annexure II-Technical Specification Q.23	Please elaborate on the requirement with a use case especially with respect to technical baseline configuration procedures mapped to various technologies.	As per RFP
53				What are the current legacy systems currently in use by IFTAS. Is there any scope of data migration from these systems to the GRC solution?	No data migration Required.
54				Please provide the technical stack used by IFTAS for on-prem deployment.	To be shared with Successful bidder