e-RFP Ref. No.JKB/CHQ/ISD/Cyber-Governance/2026-1669
Dated: 02-03-2026

Online Request For Proposal (e-RFP)

for

Supply, Implementation and Support Services for Cyber Governance, Risk and Compliance Platform

e- RFP Ref No. JKB/CHQ/ISD/Cyber-Governance/2026-1669
Dated: 02-03-2026

Issued By
J&K Bank
Information Security Department,
3rd Floor Annexe Building,
CHQ, Srinagar
Phone No -01942713301
email id - info.security@jkbmail.com

SCHEDULE OF RFP

e- RFP Reference No.	JKB/CHQ/ISD/Cyber-Governance/2026-1669 Dated: 02-03-2026
Date of Issue of RFP	05-03-2026
e-RFP Description	Supply, Implementation and Support Services for Cyber Governance, Risk and Compliance Platform
Issuer of the e-RFP-Department	Information Security Department, Corporate Headquarters, M.A. Road Srinagar 190 001 J&K
Bank's Communication Details	Mr. Saqib Ajaz Keen (Senior Manager) M.No. 9796719988 e-mail: saqib.ajaz@jkbmail.com J&K Bank Information Security Department, Corporate Headquarters, M.A. Road, Srinagar 190 001 e-mail: info.security@jkbmail.com
e-RFP Application Fee	Rs. 5000/- (Rupees Five Thousand Only only) to be deposited through Transfer / NEFT only to below a/c : Account Name: Tender Fee/ Cost Account 16-digit Account No : 9931530300000001 IFSC Code: JAKA0HRDCHQ (0 denotes zero) Bank: The J&K Bank Ltd Branch: Corporate Headquarters MA Road Srinagar J&K - 190001
Earnest Money Deposit (EMD) (Refundable)	₹ 3,00,000/- (INR Three Lacs only) to be deposited through Transfer / NEFT only to below A/c: Account Name: Earnest Money Deposit (EMD) 16-digit Account No: 9931070690000001 IFSC Code: JAKA0HRDCHQ (0 denotes zero) Bank: The J&K Bank Ltd Branch: Corporate Headquarters MA Road Srinagar J&K - 190001 UTR Number & Date / Tran No. & Date may be uploaded on e-Tendering Portal as Proof of the EMD

	(EMD is exempted for all Start-ups as recognized by DPIIT/DIPP)
Performance Bank Guarantee	5% of Consultancy Fee
Bid Document Availability including changes/amendments, if any to be issued	RFP can be downloaded from and submitted on Bank's e-Tendering Services Provider's Portal https://jkbank.abcprocure.com from March 05, 2026, 16.00 Hrs.to March 27, 2026, 17.00 Hrs.
Pre-bid Queries submission Date and Mode	All Clarifications / Queries shall be raised online only through e-Tendering Portal https://jkbank.abcprocure.com by or before March 11, 2026, 17.00 Hrs.
Clarifications to pre-bid queries will be provided by the Bank.	All communications regarding points / queries requiring clarifications shall be given online through prescribed e-Tendering Portal on March 18, 2026
Last Date of Submission of RFP	March 27, 2026, 17.00 Hrs.
Submission of online Bids	As prescribed in Bank's online tender portal https://jkbank.abcprocure.com
Date and time of opening of technical bid	To be notified separately
Corrigendum	All the Corrigendum will be uploaded on online tender portal https://jkbank.abcprocure.com only
For e-Tender related Queries	Service Provider: M/s. E-procurement Technologies Limited (Auction Tiger) , B-705, Wall Street- II, Opp. Orient Club, Ellis Bridge, Near Gujarat College, Ahmedabad- 380006, Gujarat Help Desk: Sr. No - Name 1 - Sandhya Vekariya - 6352631968 2 - Suraj Gupta - 6352632310

	3	Ijlalaehmad Pathan - 6352631902
	4	Imran Sodagar - 9328931942

DISCLAIMER

The information contained in this RFP document or any information provided subsequently to bidder(s) whether verbally or in documentary form/email by or on behalf of the J&K Bank is provided to the bidder(s) on the terms and conditions set out in this RFP document and all other terms and conditions subject to which such information is provided. This RFP is neither an agreement nor an offer and is only an invitation by the J&K Bank to the interested parties for submission of bids. The purpose of this RFP is to provide the bidder(s) with information to assist the formulation of their proposals. While effort has been made to include all information and requirements of the Bank with respect to the solution requested, this RFP does not claim to include all the information each bidder may require. Each bidder should conduct its own investigation and analysis and should check the accuracy, reliability and completeness of the information in this RFP and wherever necessary obtain independent advices/clarifications. The Bank makes no representation or warranty and shall incur no liability under any law, statute, rules or regulations as to the accuracy, reliability or completeness of this RFP. The Bank may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP. The Bank and its officers, employees, contractors, agents, and advisers disclaim all liability from any loss or damage (whether foreseeable or not) suffered by any person acting on or refraining from acting because of any information including forecasts, statements, estimates, or projections contained in this RFP document or conduct ancillary to it whether or not the loss or damage arises in connection with any negligence, omission, default, lack of care or misrepresentation on it.

The Bank also accepts no liability of any nature whether resulting from negligence or otherwise, howsoever caused arising from reliance of any Bidder upon the statements contained in this RFP. The Bidder is expected to examine all instructions, forms, terms and specifications in this RFP. Failure to furnish all information required under this RFP or to submit a Bid not substantially responsive to this RFP in all respect will be at the Bidder's risk and may result in rejection of the Bid.

The issue of this RFP does not imply that the Bank is bound to select a Bidder or to award the contract to the Selected Bidder, as the case may be, for the Project and the Bank reserves the right to reject all or any of the Bids or Bidders without assigning any reason whatsoever before issuance of purchase order and/or its acceptance thereof by the successful Bidder as defined in Award Criteria and Award of Contract in this RFP.

The Bidder shall, by responding to the Bank with a bid/proposal, be deemed to have accepted the terms of this document in totality without any condition whatsoever and accepts the selection and evaluation process mentioned in this RFP document. The Bidder ceases to have any option to object against any of these processes at any stage subsequent to submission of its responses to this RFP. All costs and expenses incurred by interested bidders in any way associated with the development, preparation, and submission of responses, including but not limited to the attendance at meetings, discussions, demonstrations, etc. and providing any additional information required by J&K BANK, will be borne entirely and exclusively by the Bidder.

The bidder shall not assign or outsource the works undertaken by them under this RFP assignment awarded by the Bank without the written consent of the Bank. The Bidders can take advantage of any Government order which applies to any tendering process and whereby there is any relaxation that is in conflict with the terms and conditions mentioned in this RFP, if and only if, any such Government order/ notification comes into force before the last date of submission of bids. Further, in case of any such orders that may affect/ contradict with the terms and conditions of this RFP, the Bidders need to seek clarification through the online procurement portal before the last date for submission of bids. The Bidder hereby agrees and undertakes to Indemnify the Bank and keep it indemnified against any losses, damages suffered and claims, action/ suits brought against the Bank on account of any act or omission on part of the Bidder, its agent, representative, employees and sub-contractors in relation to the performance or otherwise of the Services to be provided under the RFP. The bidders shall not assign or outsource the works undertaken by them under this RFP awarded by the Bank, without the written consent of the Bank.

List of Abbreviations

DC	Data Centre
DR	Disaster Recovery
HA	High Availability
BG	Bank Guarantee
OEM	Original Equipment Manufacturer
PBG	Performance Bank Guarantee
SP	Service Provider
EMD	Earnest Money Deposit
SLA	Service Level Agreement
NDA	Non-Disclosure Agreement
SI	System Integrator
TCO	Total Cost of Ownership
API	Application Program Interface
PO	Purchase Order
LTE	Limited Tender Enquiry
CBS	Core Banking Solution
UAT	User Acceptance Testing
Cyber GRC	Cyber Governance, Risk and Compliance
BCP	Business Continuity Plan

Contents

A. INTRODUCTION

Brief About Bank:

The Jammu and Kashmir Bank Limited (J&K Bank / Bank) having its Corporate Headquarters at M.A Road Srinagar, J&K -19001 has its presence throughout the country with 1000+ Branches and more than 1400 ATMs. The Bank uses Information Technology in all spheres of its functioning by connecting all its branches and offices through its WAN.J&K Bank functions as a universal Bank in Jammu & Kashmir and as a specialized Bank in the rest of the country. Bank functions as a leading bank in the Union Territories of Jammu & Kashmir and Ladakh and is designated by Reserve Bank of India as its exclusive agent for carrying out banking business for the Government of Jammu & Kashmir and Ladakh. J&K bank caters to banking requirements of various customer segments which includes Business enterprises, employees of government, semi-government and autonomous bodies, farmers, artisans, public sector organizations and corporate clients. The bank also offers a wide range of retail credit products, including home, personal loans, education loan, agriculture, trade credit and consumer lending, a number of unique financial products tailored to the needs of various customer segments. The Bank, incorporated in 1938, is listed on the NSE and the BSE. Further details of Bank including profile, products and services are available on Bank's website at **https://jkb.bank.in/**

Purpose of RFP

The purpose of this Request for Proposal is to solicit technically and commercially competitive bids from experienced and qualified vendors for the design, delivery, implementation, integration, and maintenance of an enterprise-grade Cyber Governance, Risk, and Compliance (Cyber GRC) solution for the Bank.

The Bank seeks to deploy a scalable, modular, and interoperable Cyber GRC platform that enables centralized orchestration and automation of core cyber risk functions, including:

Risk Identification, Assessment, and Treatment:
Capability to model and assess cyber risks across business processes, IT assets, and emerging threat landscapes, leveraging ISO/IEC 27005 aligned risk methodologies and semi-quantitative scoring models.

Control Framework Management:
Centralized management and mapping of internal controls to multiple regulatory frameworks (e.g., ISO 27001:2022, NIST CSF, RBI Cybersecurity Guidelines, DPDP Act, PCI DSS), with support for control testing, maturity tracking, and evidence management.

Policy, Exception, and Compliance Management:
Automation of policy lifecycle workflows, exception tracking with approval hierarchies, and real-time compliance monitoring against internal baselines and regulatory requirements.

Cybersecurity Incident and Vulnerability Governance:

Integration with existing security controls SIEM, SOAR, vulnerability scanners, Ani-Virus / Anti-Malware solutions, NAC solutions, DLP Solutions, ITSM tools, threat intel platforms etc. to support incident lifecycle governance, root cause mapping, remediation tracking, Cyber Risk Quantification and residual risk evaluation.

Audit and Regulatory Readiness:

Support for end-to-end cyber audit lifecycle, including planning, execution, control validation, and regulatory reporting, with role-based access controls and immutable audit logs.

The solution must support cloud-native, on-premises, or hybrid deployment models, with secure APIs for integration with existing control systems, ticketing platforms, and enterprise architecture repositories.

The selected vendor will be responsible for the end-to-end implementation, including solution customization, knowledge transfer, training, and ongoing technical support under a defined SLA framework. The Cyber GRC platform will be a critical enabler of the Bank’s cybersecurity governance objectives, driving real-time visibility, accountability, and assurance across the Bank’s digital ecosystem.

Eligibility Criteria

J&K Bank shall scrutinize the Eligibility bid submitted by the bidder. A thorough examination of supporting documents to meet each **General Eligibility Criteria (Annexure D - Compliance to Eligibility Criteria)** shall be conducted to determine the Eligible bidders. Bidders not complying with the eligibility criteria are liable to be rejected and shall not be considered for Technical Evaluation.

The bidders meeting the General Eligibility Criteria as per Annexure D will be considered for technical evaluation. Any credential/supporting detail mentioned in “**Annexure D - Compliance to Eligibility Criteria**” and not accompanied by relevant proof documents will not be considered for evaluation. All credential letters should be appropriately bound, labelled and segregated in the respective areas. There is no restriction on the number of credentials a Bidder can provide.

Scope of Work

The scope of work under this Cyber GRC requirement is to supply, implementation and support services towards Cyber GRC solution as per scope of work & specifications prescribed under.

Detailed Scope of Work:

The Bidders should have the capability which includes end to end solution deliverables such as provision of software licenses including Third Party Software, Database etc., implementation, customization, business case testing and result summarisation, production rollout, operational service support, and proposed integration capabilities within the Cyber GRC platform. The existing technologies related integrations including but not limited MS Active Directory, IBM Q-Radar (SIEM), Vulnerability Management (Qualysis), Patch Management, ARCON PAM, BMC ITSM tool, Anti-Virus (Symantec), TrendMicro Deep Security & EDR, MDM Solution, NAC, DLP, DSPM, XSOAR, TIM, Squal1(VAPT Management Tool) relevant tools/application developed in house or procured outside etc. It includes all the tools as applicable as per business needs to meet Information Technology and Cyber Security fulfilment from Governance, Compliance and Risk Management perspective.

The listed modules shall provide collective status in a graphical representation which will help to automate the process to closure. Details of required modules are shown below:

a) Information Security Risk Management

b) Information Security Policy & Procedure Management

c) Information Security Audit Management (Internal & External)

d) Compliance Management – (IT Risk, Cyber Risk)

e) Business Continuity Management

f) Workflow automation and integration (integration with existing tools)

g) Reporting and Dashboard (Strong reporting tools and dashboard)

h) User Access & RBAC (granular access controls) and Scope Based Access Controls to provide granular permissions specific to Assets, Audits, Risks etc.

i) Scalability and cloud (scale up for future requirements)

j) Exception Management

k) Third Party Risk Management (TPRM)

Implementation of the proposed modules shall be carried out by prioritizing key modules as proposed in the scope of work.

Bidder is suggested to provide adequate supporting database/middleware software licenses except OS licenses in order to deliver the working solution in the various environment as applicable and necessary. Server OS related licenses will be provisioned by Bank including baseline infrastructure however optimisation of the computing resources shall be done by the shortlisted bidder.

Gap Analysis and Customisation

a) The Cyber GRC platform should be able to consider the addition new cyber module and/or modification of the existing modules.

b) The Bidder, in coordination with OEM should do Bank's actual requirements analysis and submit a detailed study of Bank's technology landscape, Information security policies, Cyber Security Policies, IT policies vs the Cyber GRC Solution architecture in line with proposed scope.

c) Also, bidder shall submit a detailed study of the requirements, current state, desired state and road map mentioning all the pre-requisites, timeframe of milestones/ achievements leading to the full operationalization of the solution vis-à-vis Bank's requirement to achieve the desired state.

d) The Bidder has to develop the high level and detailed project plan (including the Cyber security requirements), get it approved by the Bank and then implement the project based on timelines agreed.

e) In the solution design, the cyber-Security best practices should be taken care of by design and ensure those requirements are being implemented by team adequately.

f) The Solution’s Architecture deployment and related configurations done at the Bank which should be vetted by OEM / Bank personnel before Sign-Off.

The Cyber GRC platform shall provide the below features:

i. The Platform should have option to store Content (policies, controls, report templates, reference documentation).

ii. The Platform should have predefined risk assessment templates for global standards and allow and customizable assessment template as per Bank defined policies, standards, and other requirements.

iii. The Platform 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, DPDPA, ITIL v4.0. (The Bidder must provide the complete list of standards supported by the Platform.)

iv. Platform should support complete automation of applicable frameworks like RBI, NBFC, SEBI CSCRF CCI , PFRDA ICSPG , UPI ISCF , IRDAI ICSG, SOC Efficacy Automation and other regulatory frameworks should be supported. RBI Master Directions, IT Outsourcing and other relevant frameworks should be supported out of box. Platform should have pre-mapped controls for regional and regulatory frameworks like SEBI, RBI,IRDAI,PFRDA,UADIA, NBFC and others applicable to Bank.

v. The Platform should have the ability to document and maintain external benchmarks, frameworks, laws, and regulations identified for meeting the corporate objectives.

vi. The Platform should provide top-down or bottom-up approaches to developing key control procedures aligned with Bank’s compliance requirements.

vii. The Platform should have the ability to provide built-in assessments, Control Self Assessments (CSA) and questionnaires as well as manually create assessments and questionnaires per defined guidelines for conducting compliance testing.

viii. The Platform should support applying weight to questions and responses.

ix. The Platform should be able to collect and store the Management responses.

x. Platform should provide the ability to report on ISO 27001 conformance in conjunction with a certification effort.

xi. The Platform should be able to generate report of ISO 27001 statement of applicability based on controls already existing or controls which are planned to be implemented.

xii. The Platform should provide aging reports to track findings and remediation plans that are overdue.

xiii. The Platform should be able to generate report on control effectiveness metrics for continual improvement of ISMS.

xiv. The Platform should be able to generate report on Risk levels on risk assessment and risk treatment to showcase mitigation status.

xv. The Platform should be able to generate Risk Treatment Plan implementation progress report.

xvi. The Platform should be able to demonstrate open risk status with implementation progress, control gaps and assets affected.

xvii. The Platform should provide the ability to create a risk summary report that describes key risks, how they are being managed and monitored, remediation of key issues and accountability.

xviii. The Platform should show dashboard including current audit findings, remediation status, remediation progress and responsibility.

xix. The Platform should be able to generate reports on audit findings, remediation, and responsibility

xx. The Platform should have options to display all the asset, risk, audit, action items and training related metrics in one single dashboard

xxi. The Platform should provide a variety of layout options enabling user to alter the user interface/dashboard.

xxii. The Platform should allow for aggregation of risks across the organization and generate the various dashboards and reports basis senior leader’s requirement such as CISO Dashboard, CEO Dashboard.

xxiii. The system should provide reports on critical findings, progress of remediation, and status.

xxiv. The Platform should allow users to perform keyword searches to quickly find specific information among various Information Security policies.

xxv. The system should have the ability to define frequency of various review and reporting for outstanding issues and assigned task.

xxvi. The Platform should have the ability to document control activities and capture details like control owners, testing requirements, mapping with compliance, risk, business unit etc

xxvii. The Platform should support cyber risk assessments for both inherent and residual risk.

xxviii. The Platform should have ability to provide a clear way to score quantitatively the vulnerabilities and risks identified based on threat, impact and compensating controls

xxix. The Platform should provide an out of the box risk register in order to capture currently maintained and tracked risks as well as ability to configure the application via no coding to accommodate our requirements.

xxx. The Platform shall have capabilities to perform risk assessments as per risk category and/or threat category

xxxi. The Platform should have capability to define and automate the frequency of conducting the Cyber Security risk assessment and automatically generating reports across various levels such as vertical head/business unit head / business/practice manager, asset owner as well as board and management levels.

xxxii. The Platform should include multiple impact categories to evaluate criticality of the business process.

xxxiii. The Platform should be able to capture robust details about each risk item including objectives, products and services, business processes, risks, threats, vulnerability, impact, like hood controls, physical facilities, technology assets, policies, and procedures.

xxxiv. Risk assessments must have both qualitative and quantitative approaches.

xxxv. The Platform should calculate, display, and report risk scores. Risk calculations must be transparent to users.

xxxvi. The Platform should give users full control over risk calculation parameters, weightings.

xxxvii. The Platform should support custom risk assessment methodologies and algorithms.

xxxviii. The Platform must keep the History of last 7 years risk.

xxxix. The Platform should have the ability to capture and document risk response procedures as well as mitigating controls.

xl. The Platform should have the ability to link, and map identified risk to Authoritative Sources, departments, asset, and divisions

xli. The Platform should capture recovery time objective (RTO) and recovery point objective (RPO) for business processes and calculate the result as overall business criticality rating for the asset and/or process.

xlii. The Platform should be able to demonstrate control effectiveness metrics measurements in a comparable way against thresholds decided for metrics.

xliii. The Platform should include workflow for multiple participants in the BIA (Business Impact Analysis) process, including the business process owner and others that may need to provide input, as well as review by another level and the BCM (Business Continuity Management) team

xliv. To support the BIA, the Platform should enable mapping of business processes to their supporting IT Service, Process, and Personnel.

xlv. The Platform should provide Cyber Risk Management system and Cyber Audit Management.

xlvi. The Platform should be enabled to manage exceptions with appropriate risk sign-off/acceptance based on the current process in line with best security practices

xlvii. The Platform should have capability to integrate with various security and IT controls such MS Active Directory, IBM Q-Radar (SIEM), Vulnerability Management (Qualysis), Patch Management, ARCON PAM, BMC ITSM tool, Anti-Virus (Symantec), TrendMicro Deep Security & EDR, MDM Solution, NAC, DLP, DSPM, XSOAR, TIM, Squal1(VAPT Management Tool) relevant tools/application developed in house or procured outside etc. It includes all the tools as applicable as per business needs to meet Information Technology and Cyber Security fulfilment from Governance, Compliance and Risk Management perspective xlviii. The communication between various components of the Platform & with other integrated systems must use authenticated and encrypted channels.

xlix. The Platform should offer a library of technical baseline configuration procedures mapped to various technologies.

l. The Platform should have capability to use external data by having an API connection or any alternate connection method with the data source. The Platform should also allow the importing the actual data in standard file format, such as csv, xls, etc.

li. The Platform administrative console and user application must be accessible by latest browser across Bank locations

lii. The Platform should maintain the audit trail/logs sufficiently for all user access and all the changes done on it.

liii. The Platform 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.

liv. The Platform should work in high availability module and vendor should provide the Platform within the defined SLA

lv. The Platform should be implemented with latest security hardening standard and comply with security standards such as CIS Benchmark, NIST CSF and OWASP etc.

lvi. The Cyber GRC Platform based solution must be an on-premises and use the existing Bank's virtualization platform for successful deployment and operationalisation.

lvii. The Platform licenses must be provided an access to 100 users with all functionalities in the proposed SOW which can be expanded as per need.

lviii. The Platform must allow the Role based user access and must have nonrepudiation control. Access to the application must be as per role and template configured for the user.

lix. Platform should have the capability to move from one tool to another, to allow that migration will full backup of data along with proper data integrity

lx. The Platform should facilitate that Compliance Management Process requirements can be mapped to a business function.

lxi. The Platform should have capability to record the consequences of non-compliance and adequate dashboards as well as reporting.

lxii. The Platform should be able to calculate compliance scores as per standard, framework, regulation, department, including dynamically defined groups.

lxiii. The Platform should have capability to perform compliance gap analysis.

lxiv. The Platform should provide built in as well as customizable workflows to track, IT Risk issues, Cyber threats, vulnerabilities, VAPT Findings, Audit Findings, Compliance findings, internal/external audits, critical incidents etc. It should support the automation of workflows to the extent possible to meet the GRC goals defined in the scope of work.

lxv. The platform shall have AI support for analysis and recommendations & Integration with Chatbot

lxvi. The solution should have automated risk and compliance workflows to minimize manual effort in assessments and approvals. It should include AI-driven risk prediction capabilities to proactively identify emerging risks.

lxvii. The solution should feature an AI-powered compliance chatbot to provide instant support for policy queries and risk recommendations.

lxviii. Platform should allow for performance evaluation questionnaires to be filled for each audit member as part of the audit closure with appropriate workflow authorization and approval.

lxix. Platform should have capability to onboard Third Party Vendors and do complete end to end life cycle management of Vendor Risks and conduct Vendor Risk Assessments

General Implementation to be carried out by supplier:

For the purpose of implementation, the following points should be noted:

The Cyber GRC Platform, services, all software's and all other associated components would be provided by the successful Bidder. The supplier / service provider should ensure the implementation of Cyber GRC platform with the help of OEM (if applicable).

a) Bidder is responsible of making the OEM support available during the implementation and maintenance.

b) Bank will only provide hardware and OS to host the solution. To make the solution work , software and all other associated components workable shall be under bidder's scope

c) Bidder has to adhere to agreed Service Level Agreements (SLA) and periodic monitoring and reporting requirements of Bank.

d) The licenses should be in the name of J&K Bank or specifically purchased for J&K Bank, where Bank's name shall be mentioned in license copies.

e) The project may be subjected to audit from RBI and/or third party. It shall be responsibility of the Bidder to co-operate and provide necessary information and support to the auditors.

f) In addition to Operations Management of their own solutions, the SI/OEM will be responsible for closure of findings of Security Assessments conducted by Bank or third-party assessor on underlying assets of these solutions.

g) Periodic health check should be carried out by SI/OEM annually to ensure the quality of implementation and operations.

h) Data captured in the solution should not be stored outside the Bank's Infrastructure.

i) No Additional payment apart from the final tender bid value will be processed/released by Bank to the Bidder under any circumstances

Dashboard requirements to be provided by supplier:

a) Cyber GRC platform should provide generic/ personalized dashboard and widgets for users and top management.

b) Dashboards should contain graphical depictions that would reveal, for instance, extent and degree of compliance & risk, potential threats, remedial measures across various activities, tasks, applications etc. It should also contain other crucial information related to Cyber Governance, risk & compliance.

c) There should also be a dedicated consolidated as well individual level dashboard for showing real-time positions, risk and exposure.

Miscellaneous features / support required:

a) Cyber GRC platform should facilitate easy monitoring of various Security applications, tools as defined, and in case of any breach/exceptions, it should invariably prompt an appropriate user. There must also be a dashboard providing dynamic view.

b) Reports pertaining to all the modules in user readable formats (pdf, xlsx, csv, txt, etc.) should be available in the Cyber GRC. While there should be some standardized/scanned reports, the application should also support a fully user configurable / query-based report generation system.

c) Supplier should also specify details of integration carried out with third party systems that are available with the product.

d) The supplier should supply and install all the required Software at Bank site.

e) The supplier should implement complete Platform till Handover Takeover operationalization.

f) The detailed Product Specifications / Bill of Material along with Make, Model number and quantity shall be submitted

g) The successful supplier expected to provide all necessary back-to-back support from OEM for delivery, installation & support till the expiry of contract period.

h) Software licenses effective date shall be effective as on Go-LIVE operational sign off or put in use for Bank operations.

i) The product proposed / supplied by the Bidder shall be compatible with the latest version of Operating System (Windows / Linux).

j) Supplier shall supply only those products, which would not be declared end of life until March 31, 2032. Further, the proposed products should also not go End of Support before March 31, 2032. However, in cases where the OEM decides to phase out any particular model, the vendor is required to substitute (upgrade) the product with another product. The Bidder must inform well in advance about such changes. In case no substitute model is available, the OEM shall give the notice for discontinuation in writing at least one month prior to such discontinuation. In case of software, the vendor shall supply the latest version available at the time of delivery & should meet all the business requirements as is with no extra cost to Bank.

k) Cyber GRC platform should support additional modules as listed (but not limited to) which may be required in future - Exception Management, Threat and Vulnerability Management, Information Security Incident and Change Management, Asset Management, Information Security Risk Management, Cyber Incident, Investigation & Advisory Management.

Support

Support the Cyber GRC Platform including future updates and upgrades of all components of the platform, shall be for a minimum period of 03 year from the date of go live (Extendable for another 2 or more years upon Bank's discretion)

Project Resources

All the resources provided for design and implementation of the Platform should be OEM certified with relevant 3 Yrs. of GRC context experience on the offered Platform in implementing and supporting the Platform at various other clients in an effective and efficient manner.

Implementation

Bank will provide adequate optimum hardware and operating systems to the bidder. The SI in consultation with the OEM is expected to suggest if the existing hardware is suitable for the Platform proposed with technical justifications and, if not, recommend additional hardware to meet the overall requirements of the Platform. The Bidder is expected to co-ordinate all the activities relating to implementation and operationalisations. In this regard the following points should be noted:

a) The Cyber GRC Platform, one time implementation services, software's and all other associated components would be required to be provided by the selected Bidder. The Bidder should ensure the adequate customised implementation of Cyber GRC platform with the help of OEM (if applicable).

b) Bidder must adhere to agreed Service Level Agreements (SLA) and periodic monitoring and reporting requirements of Bank.

c) Data captured in the Cyber GRC platform should not be stored outside Bank's Information Systems and computing environment.

d) All the proposed modules shall be implemented suitably as per Bank's custom requirements while meeting global standards and compliance requirements.

e) Bidder shall ensure the Cyber GRC platform deployment in fully HA mode at DC and DR centre in coordination with Bank. It should be fully made functional from Primary DC location along with suitable fault tolerance capability.

Operational Support:

The responsibilities of the selected Bidder include, but not limited to the following:

a) Support for all system and associated components of the Cyber GRC platform.

b) Ensuring that the system is available 24X7X365, resources for monitoring and emergency operation support should be on-boarded immediately on implementation of all modules.

c) The Bidder should provide training and certification to the resources as applicable to ensure seamless operationalisation of the modules.

d) Ensure timely fine tuning of the Cyber GRC platform to enhance the end-user experience.

e) System shall be able to enhance/ integrate the Cyber GRC platform - with new requirements implemented in Bank on ongoing basis with minimal effort.

Maintenance & Support

The Bidder will be responsible to provide maintenance and support services for the period of contract.

It will be the responsibility of Bidder to have strong backing of OEM support to seek extended support in cases wherever required and ensure all issues are addressed within the stipulated timeline as per SLA defined in the RFP. The Bidder will also be responsible to provide and install patches/ updates/ version upgrades of all software including any major or minor releases and fix vulnerabilities identified internally by organisation under their VA/PT procedures.

The activity should be planned as per the decision from Bank and may include weekends and non-business hours. The downtime resulting in such upgrades should not exceed the allowable downtime as mentioned in the RFP.

Training

The selected bidder shall provide the training to the Bank's personnel as described below:

i. The -Bidder should provide training and certification to the resources as applicable.

ii. The training should include the architecture, hardware, software, integration, and customization, policy installation, troubleshooting reporting and other aspects of the Platform. Should support the initial end user training and provide training materials.

iii. The -Bidder shall train Bank's personnel for independent operation, creation of policies/rules, generation of reports, and analysis of the reports, Troubleshooting and familiarization of features and functionalities, policy configuration, alert monitoring, etc. post implementation.

iv. Refresher training - selected Bidder shall conduct more refresher trainings for the Bank's team on yearly basis. The participants of these programs may or may not be same.

Technical Requirements

All technical bids of bidders who meet each **General Eligibility Criteria (Annexure D - Compliance to Eligibility Criteria)** will be evaluated for technical eligibility and thereof technical score would be arrived at. The bidder should meet the technical requirements as mentioned in the **Annexure E (Technical Bid Form)**.

Location of Work

The Selected bidder shall be required to work in close co-ordination with Bank's various teams during the engagement period & shall be required to primarily work at Bank's Corporate Headquarters (Srinagar) & other IT locations such as DC (Noida), DR (Mumbai), Service Operations (Srinagar/Jammu) etc. and other offices as per Banks requirement.

- **Corporate Headquarters (Srinagar)**
  The J&K Bank Ltd,
  Corporate Headquarters,
  MA Road Srinagar J&K – 190001

- **Datacentre Noida**

  Jammu & Kashmir Bank Ltd.
  7th Floor, Greenfort Data Center,
  Sify Technologies Limited, Opposite Jaypee Hospital,
  Plot No B7, Sector 132, Noida,UP-201304

- **DR Mumbai**

  Jammu & Kashmir Bank Ltd.
  CtrlS Datacenters Ltd. EL/72/1/A,
  TTC Industrial Area, MIDC,
  Mahape, Navi Mumbai 400701,
  Maharashtra, India

All expenses (travelling/lodging, etc.) shall be borne by the Service Providers.

Invitation for Tender Offer

J&K Bank invites tenders for technical bid (online) and Commercial bid (online) from suitable bidders. In this RFP, the term "bidder / prospective bidder" refers to the bidder delivering products / services mentioned in this RFP.

The prospective bidders are advised to note the following: The interested bidders are required to submit the Non-refundable Application Fees of **₹5000/=** by way of NEFT, details of which are mentioned at clause of Earnest Money Deposit in Part C

- Representatives of bidders who attend the pre-bid meeting are required to carry an authorization document from the company, an identity card for attending the meeting.

- Bidders are required to submit Bank guarantee drawn in favour of "J&K BANK LTD" payable at Srinagar, towards Earnest money Deposit (EMD) for **₹ 3,00,000/- (Three Lac rupees only).** The Bank may accept Bank guarantee in lieu of EMD for an equivalent amount valid for 6 months from the last date of bid submission and issued by any scheduled commercial Bank acceptable to the Bank. Offers made without EMD will be rejected.

- Technical Specifications, Price Bid, Terms and Conditions and various formats for submitting the tender offer are described in the tender document and Annexures.

Project Delivery Milestones

The solution as per the required scope needs to be rolled out as per the delivery timelines mentioned. The phases of the Schedule are as follows:

PROJECT PHASES:

a. PROJECT PLAN:

Successful Bidder shall submit the project plan for complete implementation of the solution as per the Scope of Work detailed in this RFP along with Solution Architecture. This plan should be submitted for review and bank's acceptance within two weeks after the issuance of PO to the successful bidder.

Bank shall issue a Project Plan signoff accepting the same. It shall be the responsibility of the successful bidder to submit and get the plan approved by the Bank authorities within the timelines mentioned above without any delay. Bank shall have the discretion to cancel the purchase order in lieu of delay in submission of the project plan.

b. PROJECT MILESTONES & DELIVERY

The Bank expects the selected bidder to meet the delivery milestones and payment terms of the engagement as per timelines detailed in the following table:

Sr. No.	Project Milestones	Deliverables/Key activities	Proposed Timeline	Payment Terms
01	Current State Assessment & Documentation.	▪ Project Kick-off: Study the Bank's requirement in detail and submit the detail project plan and detail Platform design. ▪ SLA & NDA sign-off	Within 2 Weeks from the date of the PO	10% of First year License cost

02	Delivery and installation of GRC software components / supporting licenses. Use cases development, testing, integration, Implementation and Operationalisation	▪ Implementation of complete Platform as per specifications. ▪ Support Portal Access ▪ Software & Licenses delivery ▪ Complete the User Acceptance Test (UAT) and Validations.	Within 8 Weeks from the date of the PO	30% of First year License cost
03	Go-Live Planning, End User and Administrative Training, Sufficient And Signoff requirements	▪ GRC platform customization as per Bank's need. ▪ GO LIVE Planning and Execution ▪ Admin Training and Transition ▪ Solution documentations from RFP sign-off perspective	After 11 Weeks from the date of the PO	60% of First year License cost. [2 months after go-Live]
04	Year 2 & 3 license	License payments shall be made yearly post activation for year 2 & 3.		Yearly in advance.
05	Annual Maintenance Support Services	▪ Quarterly performance review for solution and services. ▪ Preparing the improvement plan and execution.		Yearly in advance.
06	Training	Training	One time (within 13 weeks from the date of the PO)	100% training cost on completion of training program

c. EXTENSION OF DELIVERY SCHEDULE:

If, at any time during performance of the Contract, the Bidder should encounter conditions impeding timely delivery, the Bidder shall promptly notify the Bank in writing of the fact of the delay, its likely duration and its cause(s). As soon as practicable after receipt of the Bidder's notice, the Bank shall evaluate the situation and may at its discretion extend the Bidder's time for performance against suitable extension of the performance guarantee for delivery.

d. NON-DELIVERY:

Failure of the successful bidder to comply with the above delivery schedule, shall constitute sufficient grounds for the annulment of the award of contract and invocation of bank guarantee (delivery).

e. USER ACCEPTANCE TESTING:

Successful bidder shall assist Bank in the User Acceptance Testing of the solution for the functionalities stated in this tender document. Bank shall issue a UAT signoff on successful completion of the UAT. If the UAT fails or there is undue delay of the completion of the UAT due to reasons attributable to the successful bidder, Bank may at its own discretion cancel the purchase order and invoke the Bank guarantee for implementation.

f. OPERATIONALIZATION OF SOLUTION:

Bank shall issue Go Live Signoff on successful operationalization of the solution. If there is delay in the operationalization of the solution, Bank reserves the right to cancel the purchase order and invoke the Bank guarantee submitted for implementation.

g. REVIEW:

The solution shall remain under review for a period of 3 months from the date of Go Live Certificate as stated above. The Successful bidder shall be readily available during the review phase for troubleshooting and other support. During the review phase, Bank may request changes to the application as per its requirement and no extra costs shall accrue to the bank for the effort involved in the same. Bank shall issue final acceptance signoff at the end of the review phase.

B-EVALUATION PROCESS

The endeavour of the evaluation process is to fit the best fit Solutions as per the Banks requirement at the best possible price. The evaluation shall be done by the Banks internal committees formed for this purpose. Through this RFP, Bank aims to select a bidder/ application provider who would undertake the J&K Bank maintenance of the required solution. The bidder shall be entrusted with end-to-end responsibility for the execution of the project under the scope of this RFP. The bidder is expected to commit for the delivery of services with performance levels set out in this RFP in section: Service Level Agreements.

Responses from Bidders will be evaluated in three stages, sequentially, as below:

Stage A. Evaluation of Eligibility
Stage B. Technical Evaluation
Stage C. Commercial Evaluation

The three-stage evaluation shall be done sequentially on knock-out basis. This implies that those Bidders qualifying in Stage A will only be considered for Stage B and those who qualify in Stage B will only be considered for Stage C. Please note that the criteria mentioned in this section are only indicative and Bank, at its discretion, may alter these criteria without assigning any reasons. Bank also reserves the right to reject any / all proposal(s) without providing any specific reasons. All deliberations and evaluations performed by Bank will be strictly confidential and will be maintained as property of Bank exclusively and will not be available for discussion to any Bidder of this RFP.

Stage 1-Evaluation of Eligibility

The Bidders of this RFP will present their responses as detailed in this document. The Response includes details / evidences in respect of the Bidder for meeting the eligibility criteria, leading the Bank to evaluate the Bidder on eligibility criteria. The Bidder will meet the eligibility criteria mentioned in Annexure D in this document individually. Bank will evaluate the Bidders on each criterion severally and satisfy itself beyond doubt on the Bidders ability / position to meet the criteria. Those Bidders who qualify on ALL the criteria will only be considered as "**Qualified under Stage A**" of evaluation and will be considered for evaluation under Stage B. Those Bidders who do not qualify at this Stage A will not be considered for any further processing. The EMD money in respect of such Bidders will be returned on completion of the Stage A evaluation. Bank, therefore, requests that only those Bidders who are sure of meeting all the eligibility criteria only need to respond to this RFP process.

Stage 2-Evaluation of Technical Bid

All technical bids of bidders who have Qualified Stage A will be evaluated in this stage and a technical score would be arrived at. The bidder should meet the technical requirements as mentioned in the **Annexure E: Technical Bid Form.** The Bank will scrutinize the offers to determine their completeness (including signatures from the relevant personnel), errors, omissions in the technical & commercial offers of respective bidders. The Bank plans to, at its sole discretion, waive any minor non- conformity or any minor deficiency in an offer. The Bank reserves the right for such waivers and the Bank's decision in the matter will be final.

Bidders scoring at-least overall score of 84 marks or more out of 120 will be declared technically qualified.

Bank may seek clarifications from the any or each bidder as a part of technical evaluation. All clarifications received within stipulated time shall be considered for evaluation. In case a clarification is not received within the stipulated time, the respective technical parameter would be treated as non-compliant and decision to qualify the bidder shall be accordingly taken by the bidder. Those Bidders who meet the threshold score of **84 or more** will be considered as "**Qualified under Stage B**" and will be considered for evaluation under Stage C. Those who do not meet the above threshold will not be considered for further evaluation and their EMD monies will be returned.

The threshold score for technical qualification would be **84 marks out of 120 marks** based on the evaluation method given in Annexure E: Technical Bid Form

The bidders will submit the Technical Bid in the format as per **Annexure E: Technical Bid Form**. A copy of board resolution or power of attorney showing that the signatory has been duly authorized to sign the tender document

Bank at its own discretion may ask for POC / Demo of the solution for cross validation of technical evaluation points as per **Annexure E: Technical Bid Form**.

Stage 3-Evaluation of Commercial Bid

Scoring Methodology

The Commercial Bid may be submitted as per the format in **Annexure F: Commercial Bid Format.**

The selection of Bidder shall follow the **Quality and Cost Based Selection (QCBS).**

Only those Bidders scoring at least 84 marks out of 120 in the technical evaluation will be short-listed for commercial evaluation.

Financial proposals will be ranked in terms of their total evaluated cost. The least cost proposal will be ranked as L-1 and the next higher and so on will be ranked as L-2, L-3 etc. Bank may seek clarifications from the any or each bidder as a part of evaluation.

The Name of the successful bidder along with details of cost etc. shall be posted on the bank's website after the award to the successful bidder has been made and communicated to him in writing.

C-RFP SUBMISSION

E-Tendering Process

This RFP will follow e-Tendering Process (e-Bids) as under which will be conducted by Bank's authorized e-Tendering Vendor M/s. e-Procurement Technologies Ltd. through the website https://jkbank.abcprocure.com

a) Bidder Registration
b) Publishing of RFP
c) Pre-Bid Queries
d) Online Response of Pre-Bid Queries
e) Corrigendum/Amendment (if required)
f) Bid Submission
g) Bids Opening
h) Pre-Qualification
i) Bids Evaluation
a) Commercial Evaluation (Qualified Bidders)
j) Contract Award

Representative of bidder may contact the Help Desk of e-Tendering agency M/s. e-Procurement Technologies Ltd for clarifications on e-Tendering process:

Service Provider:
M/s. E-procurement Technologies Limited
(Auction Tiger), B-705, Wall Street- II, Opp. Orient Club, Ellis
Bridge, Near Gujarat College,
Ahmedabad- 380006, Gujarat

Help Desk:
Contact Persons: Nandan Velara
Mobile No.: 9081000427 / 9904407997
Landline: 079-68136831/ 6857 / 6820 / 6843 / 6853 / 6829 /
6835 / 6863 / 6852 / 6840

No consideration will be given to e-Bids received after the date and time stipulated in this RFP and no extension of time will normally be permitted for submission of e-Bids.

Bank reserves the right to accept in part or in full or extend or reject the bids received from the bidders participating in the RFP.

Bidders will have to abide by e-Business Rules framed by the Bank in consultation with M/s. eProcurement Technologies Ltd.

RFP Fees

The RFP application fees may be paid by the bidders through NEFT as per the following details:

Bank Details for RFP Fees	
Account Number	**9931530300000001**
Account Name	**Tender Fee/Cost Account**
Bank Name	The J&K Bank Ltd
Branch Name	Corporate Headquarters MA Road Srinagar J&K - 190001
IFSC Code	JAKA0HRDCHQ
Amount	INR 5000/=

The Bidder shall solely bear all expenses whatsoever associated with or incidental to the preparation and submission of its Bid and the Bank shall in no case be held responsible or liable for such expenses, regardless of the conduct or outcome of the bidding process including but not limited to cancellation / abandonment / annulment of the bidding process.

Earnest Money Deposit

Prospective bidders are required to submit Bank Guarantee drawn in favor of “Jammu and Kashmir Bank Ltd” payable at Srinagar, towards earnest money deposit (EMD) of **₹ 3,00,000/- (INR Three Lacs only)**. The Bank may accept Bank guarantee in lieu of EMD for an equivalent amount valid for 6 months from the last date of bid submission and issued by any scheduled commercial Bank in India (other than Jammu & Kashmir Bank). The Bank will not pay any interest on the EMD. The bidder can also submit the EMD through NEFT as per the following details:

Bank Details for Earnest Money Deposit	
Account Number	**9931070690000001**
Account Name	**Earnest Money deposit (EMD)**
Bank Name	The J&K Bank Ltd
Branch Name	Corporate Headquarters MA Road Srinagar J&K - 190001
IFSC Code	JAKA0HRDCHQ
Amount	**₹ 3,00,000/-**

In case of a Bank Guarantee from a Foreign Bank, prior permission of the Bank is essential. The format of Bank Guarantee is enclosed in **Annexure G: Bank Guarantee Format**.

EMD submitted through Bank Guarantee/Demand Draft should be physically send in an envelope mentioning the RFP Subject, RFP No. and date to the following address:

Address:	Information Security Department, J&K Bank Ltd. 2nd Floor Annex building, Corporate Headquarters, M. A. Road, Srinagar, J&K Pin-190001

Note: EMD is exempted for all Start-ups as recognized by DPIIT/DIPP.

The EMD made by the bidder will be forfeited if:

a. The bidder withdraws his tender before processing of the same.

b. The bidder withdraws his tender after processing but before acceptance of the PO issued by Bank.

c. The selected bidder withdraws his tender before furnishing an unconditional and irrevocable Performance Bank Guarantee.

d. The bidder violates any of the provisions of the terms and conditions of this tender specification.

The EMD will be refunded to:

a. The Successful Bidder, only after furnishing an unconditional and irrevocable Performance Bank Guarantee (other than Jammu & Kashmir Bank) from any scheduled commercial bank in India for 5% of the total project cost for 3 years and valid for 42 months including claim period of 6 months, validity starting from its date of issuance of PO. The PBG shall be submitted within 15 days of the PO issued from the Bank.

b. The Unsuccessful Bidder, only after acceptance of the PO by the selected bidder.

Performance Bank Guarantee (PBG)

The Selected bidder will furnish unconditional performance bank guarantees (other than Jammu & Kashmir Bank) from any scheduled commercial bank in India, for 5% of the total project cost for the entire duration of the contract plus 3 months' validity starting from its date of issuance. The format of the PBG is given as per **Annexure H: Performance Bank Guarantees**. The PBG shall be submitted within 15 days from the date of issuance of Purchase order by the Bank. The PBG shall be denominated in Indian Rupees. All charges whatsoever such as premium, commission etc. with respect to the PBG shall be borne by the Selected bidder. The PBG so applicable must be duly accompanied by a forwarding letter issued by the issuing Bank on the printed letterhead of the issuing Bank. Such forwarding letter shall state that the PBG has been signed by the lawfully constituted authority legally competent to sign and execute such legal instruments. The executor (BG issuing Bank Authorities) is required to mention the Power of Attorney number and date of execution in his / her favour with authorization to sign the documents. Each page of the PBG must bear the signature and seal of the BG issuing Bank and PBG number. In the event of delays by Selected bidder in implementation of project beyond the schedules given in the RFP, the Bank may invoke the PBG. Notwithstanding and without prejudice to any rights whatsoever of the Bank under the contract in the matter, the proceeds of the PBG shall be payable to Bank as compensation by the Selected bidder for its failure to complete its obligations under the contract. The Bank shall also be entitled to make recoveries from the Selected bidder's bills, Performance Bank Guarantee, or any other amount due to him, the equivalent value of any payment made to him by the Bank due to inadvertence, error, collusion, misconstruction or misstatement. The PBG may be discharged / returned by Bank upon being satisfied that there has been due performance of the obligations of the Selected bidder under the contract. However, no interest shall be payable on the PBG.

Tender Process

i. Three-stage bidding process will be followed. The response to the tender should be submitted in three parts: Eligibility, Technical Bid and Commercial Bid through online e-tendering portal with a tender document fee mentioned.

ii. The Bidder shall submit their offers strictly in accordance with the terms and conditions of the RFP. Any Bid, which stipulates conditions contrary to the terms and conditions given in the RFP, is liable for rejection. Any decision of Bank in this regard shall be final, conclusive and binding on the Vendor.

iii. Bank will enter in to contract with the L1 bidder (in normal cases). Rates fixed at the time of contract will be non-negotiable for the whole contract/SLA period and no revision will be permitted. This includes changes in taxes or similar government decisions.

iv. In normal course L1 vendor will get 100% of the work order. However, the Bank reserves the right to distribute the work among the shortlisted firms if required, keeping in view their performance, relative strengths and operational convenience. Therefore, the lowest tendering firm shall not have sole claim over the entire order. The L1-rate Vendor will get at least 50% of the work contract and the remaining work orders will be may be given to L2 and/or L3 rate vendor, provided they accept the L1 Rates. Vendors of L4 rate and beyond will not be considered. Bank's decision in this regard will be final.

v. This contract will be awarded for a period of 3 years from date of signing the AMC contract. It may be further renewed if both parties wish to continue on the same terms of service.

vi. If the service provided by the vendor is found to be unsatisfactory or if at any time it is found that the information provided by the vendor is false, the Bank reserves the right to revoke the awarded contract without giving any notice to the vendor. Bank's decision in this regard will be final.

vii. If any of the shortlisted Vendors are unable to fulfil the orders within the stipulated period, then the Bank will have the right to allot those unfulfilled orders to other participating vendors after giving 30 days" notice to the defaulting Vendor. Also during the period of the AMC contract due to unsatisfactory service to our branches/offices, Bank will have the right to cancel the contract and award the contract to other participating vendors.

Bidding Process

i. The bids in response to this RFP must be submitted in three parts:
   a. Confirmation of Eligibility Criteria
   b. Technical Bid" (TB) including and
   c. Commercial Bid" (CB).

ii. The mode of submission of Confirmation of Eligibility Criteria, Technical Bid (TB) and Commercial Bid (CB) shall be online.

iii. Bidders are permitted to submit only one Technical Bid and relevant Commercial Bid. More than one Technical and Commercial Bid should not be submitted.

iv. The Bidders who qualify the Eligibility Criteria & Technical Evaluation will be qualified for commercial bid evaluation. The successful Bidder will be determined based on as defined in Section B as per the stated Commercial Evaluation process.

v. Receipt of the bids shall be closed as mentioned in the bid schedule. Bid received after the scheduled closing time will not be accepted by the Bank under any circumstances.

vi. Earnest Money Deposit must accompany all tender offers as specified in this tender document. EMD amount / Bank Guarantee in lieu of the same should accompany the Technical Bid. Bidders, who have not paid Cost of RFP and Security Deposit (EMD amount) will not be permitted to participate in the bid and bid shall be summarily rejected.

vii. All Schedules, Formats, Forms and Annexures should be stamped and signed by an authorized official of the bidder'.

viii. The bidder is expected to examine all instructions, forms, terms and conditions and technical specifications in the bidding documents. Failure to furnish all information required by the bidding documents or submission of a bid not substantially responsive to the bidding documents in every respect will be at the bidder's risk and may result in rejection of the bid.

ix. No rows or columns of the tender should be left blank. Offers with insufficient information are liable to rejection.

x. The bid should contain no interlineations, erasures or over-writings except as necessary to correct errors made by the bidder. In such cases, the person/s signing the bid should initial such corrections.

xi. Bank reserves the right to re-issue / re-commence the entire bid process in case of any anomaly, irregularity or discrepancy in regard thereof. Any decision of the Bank in this regard shall be final, conclusive and binding on the Bidder.

xii. Modification to the Bid Document, if any, will be made available as an addendum/corrigendum on the Bank's website and Online tendering portal.

xiii. All notices regarding corrigenda, addenda, amendments, time-extension, clarification, response to bidders' queries etc., if any to this RFP, will not be published through any advertisement in newspapers or any other mass media. Prospective bidders shall regularly visit Bank's website or online tendering portal to get themselves updated on changes / development in relation to this RFP.

xiv. Prices quoted should be exclusive of GST.

xv. Applicable taxes would be deducted at source, if any, as per prevailing rates.

xvi. The price ("Bid Price") quoted by the Bidder cannot be altered or changed due to escalation on account of any variation in taxes, levies, and cost of material.

xvii. During the period of evaluation, Bidders may be asked to provide more details and explanations about information they have provided in the proposals. Bidders should respond to such requests within the time frame indicated in the letter/e-mail seeking the explanation.

xviii. The Bank's decision in respect to evaluation methodology and short-listing Bidders will be final and no claims whatsoever in this respect will be entertained.

xix. The Bidder shall bear all the costs associated with the preparation and submission of its bid and the bank, will in no case be responsible or liable for these costs, regardless of the conduct or outcome of the bidding process.

Deadline for Submission of Bids:

i. Bids must be received at the portal and by the date and time mentioned in the "Schedule of Events".
ii. In case the Bank extends the scheduled date of submission of Bid document, the Bids shall be submitted at the portal by the time and date rescheduled. All rights and obligations of the Bank and Bidders will remain the same.
iii. Any Bid received after the deadline for submission of Bids prescribed at the portal, will be rejected.

Bid Validity Period

i. Bid shall remain valid for duration of 6 calendar months from Bid submission date.

ii. Once Purchase Order or Letter of Intent is issued by the Bank, the said price will remain fixed for the entire Contract period and shall not be subjected to variation on any account, including exchange rate fluctuations and custom duty. A Bid submitted with an adjustable price quotation will be treated as non-responsive and will be rejected.

Bid Integrity

Willful misrepresentation of any fact within the Bid will lead to the cancellation of the contract without prejudice to other actions that the Bank may take. All the submissions, including any accompanying documents, will become property of the Bank. The Bidders shall be deemed to license, and grant all rights to the Bank, to reproduce the whole or any portion of their Bid document for the purpose of evaluation and to disclose the contents of submission for regulatory and legal requirements.

Cost of Bid Document

The participating Bidders shall bear all the costs associated with or relating to the preparation and submission of their Bids including but not limited to preparation, copying, postage, delivery fees, expenses associated with any demonstration or presentations which may be required by the Bank or any other costs incurred in connection with or relating to their Bid. The Bank shall not be liable in any manner whatsoever for the same or for any other costs or other expenses incurred by a Bidder regardless of the conduct or outcome of the bidding process.

Contents of Bid Document

i. The Bidder must thoroughly study/analyse and properly understand the contents of this RFP, its meaning and impact of the information contained therein.

ii. Failure to furnish all information required in this RFP or submission of Bid not responsive to this RFP in any respect will be at the Bidder’s risk and responsibility and the same may finally result in rejection of its Bid. The Bank has made considerable effort to ensure that accurate information is contained in this RFP and is supplied solely as guidelines for Bidders.

iii. The information provided by the Bidders in response to this RFP will become the property of the Bank and will not be returned. Incomplete information in Bid document may lead to non-consideration of the proposal.

iv. The Bid prepared by the Bidder, as well as all correspondences and documents relating to the Bid exchanged by the Bidder and the Bank and supporting documents and printed literature shall be submitted in **English**.

Modification and Withdrawal of Bids

i. The Bidder may modify or withdraw its Bid after the Bid’s submission, provided that written notice of the modification, including substitution or withdrawal of the Bids, is received at the portal, prior to the deadline prescribed for submission of Bids.

ii. No modification in the Bid shall be allowed, after the deadline for submission of Bids.

iii. No Bid shall be withdrawn in the interval between the deadline for submission of Bids and the expiration of the period of Bid validity specified in this RFP. Withdrawal of a Bid during this interval may result in the forfeiture of EMD submitted by the Bidder.

Payment Terms

The Company must accept the payment terms proposed by the Bank as proposed in this section. Payment shall be made in Indian Rupees.

The Company's requests for payment shall be made to the Bank in writing accompanied by Original Invoice detailing the systems, software delivered, installed and accepted by the bank.

The payments shall be made after deducting applicable TDS from the date of receipt of valid claims that are supported by original invoice, original Proof of Delivery (POD), acceptance by the bank and upon fulfilment of other conditions stipulated in the contract. The invoices and other documents are to be duly authenticated by Company. The Company therefore has to furnish the bank account number to where the funds have to be transferred for effecting payments.

Payments as per the schedule given below will be released only on acceptance of the order and on signing the SLA / NDA by the selected Company.

The Bidder must accept the payment terms proposed by the Bank as proposed in this section.
The Payments shall be made on the achievement of the following project milestones:

Sr. #	Project Milestones	Payment Terms
01	Current State Assessment & Documentation.	10% of First year License cost
02	Delivery and installation of GRC software components / supporting licenses. Use cases development, testing, integration, Implementation and Operationalisation.	30% of First year License cost
03	Go-Live Planning, End User and Administrative Training, Sufficient and Signoff requirements	60% of First year License cost. [2 months after go-Live]
04	Year 2 & 3 license	Yearly in advance.
05	Annual Maintenance Support Services	Yearly in advance.
06	Training	100% training cost on completion of training program

Payment terms: -

a) Rates to be quoted exclusive of GST.

b) Invoices to be raised after submission of PBG & execution of SLA and NDA with the Bank.

c) Payments will be done rendering of services on production of invoices and confirmation from J&K Bank.

d) All other terms and conditions as per RFP.

The Bidder must accept the payment terms proposed by the Bank as proposed in this section.

Payments shall be released on acceptance of the purchase order and:

a) Post Signing of Service Level Agreement (SLA) between Bank and Selected bidder.

b) Post Signing of Non-Disclosure Agreement (NDA) between Bank and Selected bidder.

c) All taxes, if any, applicable shall be deducted at source as per current rate while making any payment.

D-GENERAL TERMS & CONDITIONS

Standard of Performance

The bidder shall perform the service(s) and carry out its obligations under the Contract with due diligence, efficiency and economy, in accordance with generally accepted techniques and practices used in industry and with professional engineering standards recognized by the international professional bodies and shall observe sound management, technical and engineering practices. It shall employ appropriate advanced technologies, procedures and methods. The Bidder shall always act, in respect of any matter relating to the Contract, as faithful advisors to J&K Bank and shall, at all times, support and safeguard J&K Bank's legitimate interests.

Indemnity

The Successful bidder shall indemnify and hold the Bank harmless from and against all claims, losses, costs, damages, expenses, action suits and other proceedings (including attorney fees), relating to or resulting from: -

i. Intellectual Property infringement or misappropriation of any third-party trade secrets or infringement of any patent, trademarks, copyrights etc. or such other statutory infringements in respect of all components provided to fulfil the scope of this project.

ii. Claims made by the employees who are deployed by the Successful bidder.

iii. Breach of confidentiality obligations by the Successful bidder,

iv. Negligence (including but not limited to any acts or omissions of the Successful bidder, its officers, principals or employees) or misconduct attributable to the Successful bidder or any of the employees deployed for the purpose of any or all of the its obligations,

v. Any loss or damage arising out of loss of data;

vi. Bonafide use of deliverables and or services provided by the successful bidder;

vii. Non-compliance by the Successful bidder with applicable laws/Governmental/ Regulatory Requirements.

The Successful bidder shall be responsible for any loss of data, loss of life etc. due to acts of its representatives, and not just arising out of negligence or misconduct, as such liabilities pose significant risk.

It is hereby agreed that the above said indemnity obligations shall apply notwithstanding anything to the contrary contained in this Tender document and subsequent Agreement and shall survive the termination of the agreement for any reason whatsoever. The Successful bidder will have sole control of its defence and all related settlement negotiations

Cancellation of Contract and Compensation

The Bank reserves the right to cancel the contract of the selected Bidder and recover expenditure incurred by the Bank on the following circumstances. The Bank would provide 30 days' notice to rectify any breach/ unsatisfactory progress:

a. The selected Bidder commits a breach of any of the terms and conditions of the RFP/contract.
b. The selected Bidder becomes insolvent or goes into liquidation voluntarily or otherwise.
c. Delay in completion of Supply, Installation of Project Deliverables.
d. Serious discrepancies noted in the inspection.
e. Breaches in the terms and conditions of the Order.
f. Non submission of acceptance of order within 7 days of order.
g. Excessive delay in execution of order placed by the Bank.
h. The progress regarding execution of the contract, made by the selected Bidder is found to be unsatisfactory.
i. If the selected Bidder fails to complete the due performance of the contract in accordance with the agreed terms and conditions.

Liquidated Damages

If bidder fails to perform services within stipulated time schedule, the Bank shall, without prejudice to its other remedies under the contract, deduct from the contract price, as liquidated damages, a sum equivalent to 2% of the total project cost for delay of each week for maximum of 5 weeks. Once the maximum is reached, Bank may consider termination of Contract pursuant to the conditions of contract. However, the bank reserves the right to impose / waive any such penalty.

Fixed Price

The Commercial Offer shall be on a fixed price basis, inclusive of all taxes and levies (excluding GST). No price increase due to increases in customs duty, excise, tax, dollar price variation etc. will be permitted.

Right to Audit

Bank reserves the right to conduct an audit/ ongoing audit of the services provided by Bidder.

The Selected Bidder (Service Provider) shall be subject to annual audit by internal/ external Auditors appointed by the Bank/ inspecting official from the Reserve Bank of India or any regulatory authority or the person authorised by it, covering the risk parameters finalized by the Bank/ such auditors in the areas of products (IT hardware/ Software) and services etc. provided to the Bank and Service Provider is required to submit such certification by such Auditors to the Bank.

Bidder should allow the J&K Bank or persons authorized by it to access Bank documents, records or transactions or any other information given to, stored or processed by Bidder within a reasonable time failing which Bidder will be liable to pay any charges/ penalty levied by the Bank without prejudice to the other rights of the Bank. Bidder should allow the J&K Bank to conduct audits or inspection of its Books and account with regard to Bank's documents by one or more officials or employees or other persons duly authorized by the Bank.

Force Majeure

i. The Selected Bidder shall not be liable for forfeiture of its performance security, Liquidated damages or termination for default, if any to the extent that its delay in performance or other failure to perform its obligations under the contract is the result of an event of Force Majeure.

ii. For purposes of this Clause, "Force Majeure" means an event explicitly beyond the reasonable control of the Contractor and not involving the contractors fault or negligence and not foreseeable. Such events may be due to or as a result of or caused by act of God, wars, insurrections, riots, earth quake and fire, revolutions, civil commotion, floods, epidemics, pandemics, quarantine restrictions, trade embargos, declared general strikes in relevant industries, satellite failure, act of Govt. of India, events not foreseeable but does not include any fault or negligence or carelessness on the part of the parties, resulting in such a situation. In the event of any such intervening Force Majeure, either party shall notify the other in writing of such circumstances or the cause thereof immediately within five calendar days.

iii. Unless otherwise directed by the Bank in writing, the selected contractor shall continue to perform its obligations under the Contract as far as is reasonably practical, and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.

iv. In such a case the time for performance shall be extended by a period(s) not less than duration of such delay. If the duration of delay continues beyond a period of three months, the Bank and the contractor shall hold consultations in an endeavor to find a solution to the problem.

v. Notwithstanding above, the decision of the Bank shall be final and binding on the successful bidder regarding termination of contract or otherwise

Publicity

Bidders, either by itself or through its group companies or Associates, shall not use the name and/or trademark/logo of Bank, in any sales or marketing publication or advertisement, or in any other manner.

Amendments

Any provision of hereof may be amended or waived if, and only if such amendment or waiver is in writing and signed, in the case of an amendment by each Party, or in the case of a waiver, by the Party against whom the waiver is to be effective.

Assignment

The Selected Bidder shall not assign, in whole or in part, the benefits or obligations of the contract to any other person without the prior written consent of the Bank. However, the Bank may assign any of its rights and obligations under the Contract to any of its affiliates without prior consent of Bidder.

Severability

If any provision of this agreement or any document, if any, delivered in connection with this agreement is partially or completely invalid or unenforceable in any jurisdiction, then that provision shall be ineffective in that jurisdiction to the extent of its invalidity or unenforceability. However, the invalidity or unenforceability of such provision shall not affect the validity or enforceability of any other provision of this Agreement, all of which shall be construed and enforced as if such invalid or unenforceable provision was/were omitted, nor shall the invalidity or unenforceability of that provision in one jurisdiction affect its validity or enforceability in any other jurisdiction. The invalid or unenforceable provision will be replaced in writing by a mutually acceptable provision, which being valid and enforceable comes closest to the intention of the Parties underlying the invalid or unenforceable provision.

Applicable law and jurisdictions of court

The Contract with the selected Bidder shall be governed in accordance with the Laws of UT Of J&K read with laws of India so far as they are applicable to the UT of J&K for the time being enforced and will be subject to the exclusive jurisdiction of Courts at Srinagar (with the exclusion of all other Courts). However, the services from the bidder during the period of dispute or pending resolution shall continue as far as is reasonably practical.

Resolution of Disputes and Arbitration clause

The Bank and the Bidder shall make every effort to resolve any disagreement or dispute amicably, arising in connection with the Contract, by direct and informal negotiation between the designated Officer of the Bank and designated representative of the Bidder. If designated Officer of the Bank and representative of Bidder, for **Supply, Implementation and Support Services for Cyber Governance, Risk and Compliance Platform** are unable to resolve the dispute within reasonable period, which in any case shall not exceed 30 days, they shall immediately escalate the dispute to the senior authorized personnel designated by the Bank and Bidder respectively. If even after elapse of reasonable period, which in any case shall not exceed 30 days, the senior authorized personnel designated by the Bank and Bidder are unable to resolve the dispute amicably OR any party fails to designate its officer/representative/ senior authorized personnel within 30 days from the date of request in writing for the same by the other party for amicable settlement of dispute, the same shall be referred to a sole arbitrator to be appointed by Bank. The Arbitration and Conciliation Act, 1996 will be applicable to the arbitration proceeding and the venue of the arbitration shall be at Srinagar. The language of the arbitration proceedings shall be in English. The award of the arbitrator shall be final and binding. The courts at Srinagar shall have exclusive jurisdiction at Srinagar.

Execution of Service Level Agreement (SLA)/ Non-Disclosure Agreement (NDA)

The Selected bidder shall have to execute service level agreement for deliverables and successful execution of the Contract to meet Bank's requirement to its satisfaction. The Bank would stipulate strict penalty clauses for non-performance or any failure in the implementation/efficient performance of the project. The Bidder should execute the Agreement within 30 days from the date of acceptance of Work Order. The date of agreement shall be treated as date of engagement and the time-line for completion of the assignment shall be worked out in reference to this date. The Bidder hereby acknowledges and undertakes that terms and conditions of this RFP may be varied by the Bank in its absolute and sole discretion. The SLA/NDA to be executed with the Selected bidder shall accordingly be executed in accordance with such varied terms.

‘NO CLAIM’ Certificate

The Bidder shall not be entitled to make any claim(s) whatsoever, against J&K Bank, under or by virtue of or arising out of, the Contract/Agreement, nor shall J&K Bank entertain or consider any such claim, if made by the Bidder after he has signed a ‘No Claim’ Certificate in favor of J&K Bank in such form as shall be required by J&K Bank after the works are finally accepted.

Cost and Currency

The Offer must be made in Indian Rupees only, including the following:

a) Cost of the equipment/software/licenses specified
b) Installation, commissioning, maintenance, migration charges, hosting charges, if any,
c) Comprehensive on-site software support.
d) Packing, Forwarding and Transportation charges up to the sites to be inclusive.
e) All taxes and levies are for Destinations.
f) Bidder have to make their own arrangements for obtaining road permits wherever needed.

No Agency

The Service(s) of the Bidder herein shall not be construed as any agency of J&K Bank and there shall be no Principal - Agency relationship between J&K Bank and the Bidder in this regard.

Project Risk Management

The selected bidder shall develop a process & help Bank to identify various risks, threats & opportunities within the project. This includes identifying, analyzing & planning for potential risks, both positive & negative, that might impact the project & minimizing the probability of & impact of positive risks so that project performance is improved for attainment of business goals.

Information Security:

a. The Successful Bidder and its personnel shall not carry any written material, layout, diagrams, hard disk, flash / pen drives, storage tapes or any other media out of J&K Bank's premises without written permission from J&K Bank.

b. The Successful Bidder's personnel shall follow J&K Bank's information security policy and instructions in this regard.

c. The Successful Bidder acknowledges that J&K Bank 's business data and other proprietary information or materials, whether developed by J&K Bank or being used by J&K Bank pursuant to a license agreement with a third party (the foregoing collectively referred to herein as "proprietary information") are confidential and proprietary to J&K Bank; and the Successful Bidder agrees to use reasonable care to safeguard the proprietary information and to prevent the unauthorized use or disclosure thereof, which care shall not be less than that used by Successful Bidder to protect its own proprietary information. Successful Bidder recognizes that the goodwill of J&K Bank depends, among other things, upon the Successful Bidder keeping such proprietary information confidential and that unauthorized disclosure of the same by Successful Bidder could damage J&K Bank. By reason of Successful Bidder's duties and obligations hereunder, Successful Bidder may come into possession of such proprietary information, even though the Successful Bidder does not take any direct part in or furnish the Service(s) performed for the creation of said proprietary information and shall limit access thereto to employees with a need to such access to perform the Services required by the Contract/Agreement. Successful Bidder shall use such information only for the purpose of performing the Service(s) under the Contract/Agreement.

d. Successful Bidder shall, upon termination of the Contract/Agreement for any reason, or upon demand by J&K Bank, whichever is earliest, return any and all information provided to Successful Bidder by J&K Bank, including any copies or reproductions, both hardcopy and electronic.

e. That the Successful Bidder and each of its subsidiaries have taken all technical and organizational measures necessary to protect the information technology systems and Data used in connection with the operation of the Successful Bidder's and its subsidiaries' businesses. Without limiting the foregoing, the Successful Bidder and its subsidiaries have used reasonable efforts to establish and maintain, and have established, maintained, implemented and complied with, reasonable information technology, information security, cyber security and data protection controls, policies and procedures, including oversight, access controls, encryption, technological and physical safeguards and business continuity/disaster recovery and security plans that are designed to protect against and prevent breach, destruction, loss, unauthorized distribution, use, access, disablement, misappropriation or modification, or other compromise or misuse of or relating to any information technology system or Data used in connection with the operation of the Successful Bidder's and its subsidiaries' businesses.

f. The Successful Bidder shall certify that to the knowledge of the Successful Bidder, there has been no security breach or other compromise of or relating to any information technology and computer systems, networks, hardware, software, data, or equipment owned by the Successful Bidder or its subsidiaries or of any data of the Successful Bidder's, the Operating Partnership's or the Subsidiaries' respective customers, employees, suppliers, vendors that they maintain or that, to their knowledge, any third party maintains on their behalf (collectively, "IT Systems and Data") that had, or would reasonably be expected to have had, individually or in the aggregate, a Material Adverse Effect, and

g. That the Successful Bidder has not been notified of, and has no knowledge of any event or condition that would reasonably be expected to result in, any security breach or other compromise to its IT Systems and Data;

h. That the Successful Bidder is presently in compliance with all applicable laws, statutes, rules or regulations relating to the privacy and security of IT Systems and Data and to the protection of such IT Systems and Data from unauthorized use, access, misappropriation or modification. Besides the Successful Bidder confirms the compliance with Banks Supplier Security Policy.

i. That the Successful Bidder has implemented backup and disaster recovery technology consistent with generally accepted industry standards and practices.

j. That the Successful Bidder and its subsidiaries IT Assets and equipment, computers, Systems, Software's, Networks, hardware, websites, applications and Databases (Collectively called IT systems) are adequate for, and operate and perform in all material respects as required in connection with the operation of business of the Successful Bidder and its subsidiaries as currently conducted, free and clear of all material bugs, errors, defects, Trojan horses, time bombs, malware and other corruptants.

k. That the Successful Bidder shall be responsible for establishing and maintaining an information security program that is designed to:

- Ensure the security and confidentiality of Customer Data, Protect against any anticipated threats or hazards to the security or integrity of Customer Data, and

- That the Successful Bidder will notify Customer of breaches in Successful Bidder's security that materially affect Customer or Customer's customers. Either party may change its security procedures from time to time as commercially reasonable to address operations risks and concerns in compliance with the requirements of this section.

l. The Successful Bidder shall establish, employ and at all times maintain physical, technical and administrative security safeguards and procedures sufficient to prevent any unauthorized processing of Personal Data and/or use, access, copying, exhibition, transmission or removal of Bank's Confidential Information from Companies facilities. Successful Bidder shall promptly provide Bank with written descriptions of such procedures and policies upon request. Bank shall have the right, upon reasonable prior written notice to Successful Bidder and during normal business hours, to conduct on-site security audits or otherwise inspect Companies facilities to confirm compliance with such security requirements.

m. That Successful Bidder shall establish and maintain environmental, safety and facility procedures, data security procedures and other safeguards against the destruction, corruption, loss or alteration of the Client Data, and to prevent access, intrusion, alteration or other interference by any unauthorized third parties of the same, that are no less rigorous than those maintained by Successful Bidder for its own information or the information of its customers of a similar nature.

n. That the Successful Bidder shall perform, at its own expense, a security audit no less frequently than annually. This audit shall test the compliance with the agreed-upon security standards and procedures. If the audit shows any matter that may adversely affect Bank, Successful Bidder shall disclose such matter to Bank and provide a detailed plan to remedy such matter. If the audit does not show any matter that may adversely affect Bank, Bidder shall provide the audit or a reasonable summary thereof to Bank. Any such summary may be limited to the extent necessary to avoid a breach of Successful Bidder's security by virtue of providing such summary.

o. That Bank may use a third party or its own internal staff for an independent audit or to monitor the Successful Bidder's audit. If Bank chooses to conduct its own security audit, such audit shall be at its own expense. Successful Bidder shall promptly correct any deficiency found in a security audit.

p. That after providing 30 days prior notice to Successful Bidder, Bank shall have the right to conduct a security audit during normal business hours to ensure compliance with the foregoing security provisions no more frequently than once per year. Notwithstanding the foregoing, if Bank has a good faith belief that there may have been a material breach of the agreed security protections, Bank shall meet with Successful Bidder to discuss the perceived breach and attempt to resolve the matter as soon as reasonably possible. If the matter cannot be resolved within a thirty (30) day period, the parties may initiate an audit to be conducted and completed within thirty (30) days thereafter. A report of the audit findings shall be issued within such thirty (30) day period, or as soon thereafter as is practicable. Such audit shall be conducted by Successful Bidder's auditors, or the successors to their role in the event of a corporate reorganization, at Successful Bidder's cost.

q. Successful Bidders are liable for not meeting the security standards or desired security aspects of all the ICT resources as per Bank's IT/Information Security / Cyber Security Policy. The IT /Information Security/ Cyber Security Policy will be shared with successful Bidder. Successful Bidders should ensure Data Security and protection of facilities/application managed by them.

r. The deputed persons should aware about Bank's IT/IS/Cyber security policy and have to maintain the utmost secrecy & confidentiality of the bank's data including process performed at the Bank premises. At any time, if it comes to the notice of the bank that data has been compromised / disclosed/ misused/misappropriated then bank would take suitable action as deemed fit and selected vendor would be required to compensate the bank to the fullest extent of loss incurred by the bank. Besides bank will be at liberty to blacklist the bidder and take appropriate legal action against bidder.

s. The Bank shall evaluate, assess, approve, review, control and monitor the risks and materiality of vendor/outsourcing activities and Successful Bidder shall ensure to support baseline system security configuration standards. The Bank shall also conduct effective due diligence, oversight and management of third party vendors/service providers & partners.

t. Vendor criticality assessment shall be conducted for all partners & vendors. Appropriate management and assurance on security risks in outsources and partner arrangements shall be ensured.

Survival

Any provision of the Contract/Agreement which, either expressly or by implication, survives the termination or expiration of the Contract/Agreement, shall be complied with by the Parties including that of the provisions of indemnity, confidentiality, non- disclosure in the same manner as if the present Contract/Agreement is valid and in force and effect. The provisions of the clauses of the Contract/Agreement in relation to Documents, data, processes, property, Intellectual Property Rights, indemnity, publicity and confidentiality and ownership shall survive the expiry or termination of the Contract/Agreement and in relation to confidentiality, the obligations continue to apply unless J&K Bank notifies the Bidder of its release from those obligations.

No Set-Off, Counter-Claim and Cross Claims

In case the Bidder has any other business relationship(s) with J&K Bank, no right of set-off, counter-claim and cross-claim and or otherwise will be available under this Contract/Agreement to the Bidder for any payment's receivable under and in accordance with that business.

Statutory Requirements

During the tenure of the Contract/Agreement nothing shall be done by the Bidder in contravention of any law, act and/ or rules/regulations, there under or any amendment thereof governing inter-alia customs, foreign exchange, etc., and the Bidder shall keep J&K Bank, its directors, officers, employees, representatives, agents and consultants indemnified in this regard.

Bidder Utilization of Know-how

J&K Bank will request a clause that prohibits the finally selected bidder from using any information or know-how gained in this contract for another organization whose business activities are similar in part or in whole to any of those of the Bank anywhere in the world without prior written consent of the Bank during the period of the contract and one year thereafter.

Corrupt and Fraudulent practice.

i. It is required that Company observe the highest standard of ethics during the procurement and execution of such contracts and not to indulge in any corrupt and fraudulent practice.

ii. "Corrupt Practice" means the offering, giving, receiving or soliciting of anything of value to influence the action of an official in the procurement process or in contract execution.

iii. "Fraudulent Practice" means a misrepresentation of facts in order to influence a procurement process or the execution of contract to the detriment of the Bank and includes collusive practice among bidders (prior to or after bid submission) designed to establish bid prices at artificial non-competitive levels and to deprive the Bank of the benefits of free and open competition.

iv. The Bank reserves the right to reject a proposal for award if it determines that the Company recommended for award has engaged in corrupt or fraudulent practices in competing for the contract in question.

v. The Bank reserves the right to declare a bidder ineligible, either indefinitely or for a stated period of time, to be awarded a contract if at any time it becomes known that the firm has engaged in corrupt or fraudulent practices in competing for or in executing the contract.

Solicitation of Employees

Bidder will not hire employees of J&K Bank or solicit or accept solicitation (either directly, indirectly, or through a third party) from employees of the J&K Bank directly involved in this contract during the period of the contract and one year thereafter.

Proposal Process Management

The Bank reserves the right to accept or reject any/all proposal/ to revise the RFP, to request one or more re-submissions or clarifications from one or more BIDDERs, or to cancel the process in part or whole. No BIDDER is obligated to respond to or to continue to respond to the RFP. Additionally, the Bank reserves the right to alter the requirements, in part or whole, during the RFP process. Each party shall be entirely responsible for its own costs and expenses that are incurred while participating in the RFP, subsequent presentation and contract negotiation processes.

Confidentiality Provision

The bidder shall hold in confidence all the information, documentation ,etc which shall come to their knowledge (Confidential Information) and shall not disclose or divulge confidential information to any third party or use Confidential Information or any part thereof without written consent of the Bank.

Confidential Information means information which is by its nature confidential or is designated by the bank and confidential information and includes:

i. All information marked or otherwise designated as confident.
ii. Information which relates to the financial position, the internal management structure , the Personnel , policies and strategies of the Bank
iii. Data of the bank, customer lists, customer information, account information, and business information regarding business planning and operation of the Bank or otherwise information or data whether such data is permanent or otherwise.

The restriction imposed in this clause does not apply to any disclosure or information:

i. Which at the material time was in public domain other than breach of this clause; or

ii. Which is required to be disclosed on account of order of any competent court or tribunal provided that while disclosing any information, Bank shall be informed about the same vide prior notice unless such notice is prohibited by applicable law.

Sub-Contracting

The services offered to be undertaken in response to this RFP shall be provided by the Successful Bidder/ directly employing their employees, and there shall not be any subcontracting. All the resources deployed by the Successful Bidder should be on the Successful Bidders payroll.

Award Notification

The Bank will award the contract to the successful Bidder, out of the Bidders who have responded to Bank's tender as referred above, who has been determined to qualify to perform the contract satisfactorily, and whose Bid has been determined to be substantially responsive, and is the lowest commercial Bid.

The Bank reserves the right at the time of award of contract to increase or decrease of the quantity or change in location where services are required from what was originally specified while floating the tender without any change in unit price or any other terms and conditions.

Suspension of Work

The Bank reserves the right to suspend and reinstate execution of the whole or any part of the work without invalidating the provisions of the contract. The Bank will issue orders for suspension or reinstatement of the work to the Successful Bidder in writing. The time for completion of the work will be extended suitably to account for duration of the suspension

Taxes and Duties

a) Successful Bidder will be entirely responsible for all duties, levies, imposts, costs, charges, license fees, road permit etc, in connection with delivery of equipment at site including incidental services and commissioning.

b) Income/Corporate taxes in India: The Successful Bidder shall be liable to pay all corporate taxes and income tax that shall be levied according to the laws and regulations applicable from time to time in India

c) Tax Deduction at Source: Wherever the laws and regulations require deduction of such taxes at source of payment, Bank shall effect such deductions from the payment due to the Successful Bidder. The remittance of amounts so deducted and issuance of certificate for such deductions shall be made by Bank as per the laws and regulations in force. Nothing in the Contract shall relieve the Successful Bidder from his responsibility to pay any tax that may be levied in India on income and profits made by Successful Bidder in respect of this contract.

d) The Bank shall if so, required by applicable laws in force, at the time of payment, deduct income tax payable by the Successful Bidder at the rates in force, from the amount due to the Successful Bidder and pay to the concerned tax authority directly.

Annexure A: Confirmation of Terms and Conditions

To

Chief Information Security Officer

Information Security Department

The Jammu & Kashmir Bank M.A. Road, Srinagar,

190 001 J&K.

Dear Sir,

Sub: RFP No ………………………………………. For **Supply, Implementation and Support Services for Cyber Governance, Risk and Compliance Platform** dated …………………………

Further to our proposal dated ...., in response to the Request for Proposal for **Supply, Implementation and Support Services for Cyber Governance, Risk and Compliance Platform** (hereinafter referred to as "RFP") issued by The Jammu & Kashmir Bank (J&K BANK) we hereby covenant, warrant and confirm as follows:

We hereby agree to comply with all the terms and conditions / stipulations, payment terms, scope, SLAs etc. as contained in the RFP and the related addendums and other documents issued by the Bank.

Place:

Date: Seal and signature of the bidder

Annexure B: Tender Offer Cover Letter

To

Chief Information Security Officer

Information Security Department

The Jammu & Kashmir Bank M.A. Road, Srinagar,

190 001 J&K.

Dear Sir,

Sub: RFP no: ____________ for Supply, Implementation and Support Services for Cyber Governance, Risk and Compliance Platform dated _______________

Having examined the tender documents including all annexures the receipt of which is hereby duly acknowledged, we, the undersigned, offer **Supply, Implementation and Support Services for Cyber Governance, Risk and Compliance Platform** to Bank as mentioned in RFP document in conformity with the said tender documents in accordance with the Commercial bid and made part of this tender.

We understand that the RFP provides generic specifications about all the items and it has not been prepared by keeping in view any specific bidder.

We understand that the RFP floated by the Bank is a confidential document and we shall not disclose, reproduce, transmit or made available it to any other person.

We have read, understood and accepted the terms/ conditions/ rules mentioned in the RFP.

Until a formal contract is prepared and executed, this tender offer, together with the Bank's written acceptance thereof and the Bank's notification of award, shall constitute a binding contract between us.

We undertake that in competing for and if the award is made to us, in executing the subject Contract, we will strictly observe the laws against fraud and corruption in force in India and the UT of J&K.

We have never been barred/black-listed by any regulatory / statutory authority in India.

We understand that the Bank is not bound to accept the lowest or any offer the Bank may receive.

This Bid, together with your written acceptance thereof and your notification of award, shall constitute a binding Contract between us.

We certify that we have provided all the information requested by the Bank in the format requested for. We also understand that the Bank has the exclusive right to reject this offer in case the Bank is of the opinion that the required information is not provided or is provided in a different format. It is also confirmed that the information submitted is true to our knowledge and the Bank reserves the right to reject the offer if anything is found incorrect.

Place:

Date: Seal and signature of the bidder

Annexure C: Details of SI/OEM

Details filled in this form must be accompanied by sufficient documentary evidence, in order to facilitate the Bank to verify the correctness of the information.

S. No.	PARTICULARS	DETAILS
1	Name of the Company	
2	Postal Address	
3	Telephone / Mobile / Fax Numbers	
4	Constitution of Company	
5	Name & Designation of the Person Authorized to make commitments to the Bank	
6	Email Address	

7	Year of Commencement of Business	
8	Sales Tax Registration No	
9	Income Tax PAN No	
10	Service Tax / GST Registration No	
11	Whether OEM or System Integrator	
12	Name & Address of OEM/s.	
13	Brief Description of after sales services facilities available with the SI/OEM	
14	Web Site address of the Company	

Date:

Seal and signature of the bidder

Annexure D: Compliance to Eligibility Criteria

The bidder needs to comply with all the eligibility criteria mentioned below. Non-compliance to any of these criteria would result in outright rejection of the Bidder's proposal. The bidder is expected to provide proof for each of the points for eligibility evaluation criteria. Any credential detail not accompanied by required relevant proof documents will not be considered for evaluation. All credential letters should be appropriately bound, labelled and segregated in the respective areas. There is no restriction on the number of credentials a bidder can provide.

The decision of the Bank would be final and binding on all the Bidders to this document. The Bank may accept or reject an offer without assigning any reason what so ever.

The bidder must meet the following criteria to become eligible for bidding:

S.No	Financial and other requirement to be met by the bidder	Supporting document to be submitted	Bidder's response and Documents Submitted	Complied (Yes/No)
1	The Bidder must be registered with Registrar of Companies / a Govt Organization/ PSU / PSE/ LLP or Private/ Public Limited Company in India.	Copy of Certificate of LLP registration. (OR) Copy of Certificate of Incorporation and Certificate of Commencement of business in case of Public Limited Company (OR) Certificate of Incorporation in case of Private Limited Company, issued by the Registrar of Companies		
2	The Bidder should have been in existence in India for the last three years as on 31.12.2025.	Copy of Certificate of Incorporation / Certificate of commencement of business		
3	The Bidder should have a minimum annual turnover of Rs. 50 Crores (Rupees Fifty Crores Only) in each of the last three financial years viz. 2022-23 and 2023-2024 and 2024-25	a. Audited Financial statements for the financial years 2022-23 and 2023-2024 and 2024-25 with CA Certificate for the said period. b. Certificate from statutory auditor must be submitted mentioning Average Annual turnover, positive net worth and positive profit after tax for last three financial years i.e., 2022-23 and 2023-2024 and 2024-25		
4	The Bidder should have positive net worth in each of the last 3 financial Year's viz. 2022-23 and 2023-2024 and 2024-25. Net Worth is to be calculated as follows: *Capital Funds (Paid up equity capital + Paid up preference shares + Free reserves) - (Accumulated balance of loss + Balance of deferred*	Certificate from statutory auditor must be submitted mentioning Average Annual turnover, positive net worth and positive profit after tax for last three financial years i.e., 2022-23 and 2023-2024 and 2024-25. The CA certificate should be without any conditions.		

	revenue expenditure + other intangible assets)			
5	The Bidder should not have filed for Bankruptcy in any country.	Self-declaration confirming the Criteria.		
6	The Bidder should not have been blacklisted / barred by any Public Sector Bank, Government of India or any regulatory body in India at the time of bid submission.	Self-declaration confirming the criteria.		
7	The Bidder should not be involved in any legal case that may affect the solvency / existence of firm or in any other way affect the bidder's capability to provide / continue the services to Bank.	Self-declaration Confirming the criteria.		
8	Bidder should have minimum of 3 years of experience in proposed solution/ platform implementation within BFSI.	Bidder should submit PO or contract document.		
9	Bidder should have completed supply and implementation of at least 01 GRC project at any scheduled commercial bank during the last 03 years from the date of this RFP.	Bidder should submit PO or contract document.		

10	Bidder should have minimum two (2) resources on its pay roll which are OEM certified having sufficient levels of experience (at least 05 years) in implementing and operationalisation of the proposed Cyber GRC platform.	Bidder should submit the copy of relevant certificates. OR Self declaration by Bidder on company's letter head to be submitted signed by authorised signatory.		
11	The Bidder should be OEM or Authorized Bidder of the OEM (Original Equipment Manufacturer).	Manufacturers Authorization letter from OEM in favour of Bidder must be enclosed as per Annexure M / Self-declaration required on letter head in case of OEM participation.		

Please enclose documentary proof for all the above criteria. In absence of these, the bids will not be considered for further evaluation. No further correspondence will be entertained in this case.

Note: Please write description of items in brief instead of writing words like "Offered", "Complied with" etc.

Note: Point 2,3,4 is relaxed for all MSME.

1. Bidders need to ensure compliance to all the eligibility criteria points.

2. Purchase orders without relevant organization confirmation through a credential letter will not be considered as credentials.

3. Scheduled commercial Banks do not include Regional Rural Banks and Cooperative Banks.

Annexure E: Technical Bid Form

The technical requirements for scoring criteria are enlisted below. For each item 0.5 mark will be awarded.

Chief Information Security Officer

Information Security Department.
Corporate Headquarters
The Jammu & Kashmir Bank M.A. Road, Srinagar,
190 001 J&K.

SUB: **REQUEST FOR PROPOSAL (RFP) FOR Supply, Implementation and Support Services for Cyber Governance, Risk and Compliance Platform**.

PART A

Sr.	Functionality	Bidder's Remark (Yes / No) (Each point has 0.5 mark)
	Governance	
1	The Platform should have option to store Content (policies, controls, report templates, reference documentation).	
2	The Platform should have predefined risk assessment templates for global standards and allow and customizable assessment template as per Bank defined policies, standards, and other requirements.	
3	The Platform 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, DPDPA, ITIL v4.0. (The Bidder must provide the complete list of standards supported by the Platform.)	
4	The Platform should have the ability to document and maintain external benchmarks, frameworks, laws, and regulations identified for meeting the corporate objectives.	
5	The Platform should provide top-down or bottom-up approaches to developing key control procedures aligned with Bank's compliance requirements.	

6	The Platform should have the ability to provide built-in assessments, Control Self Assessments (CSA) and questionnaires as well as manually create assessments and questionnaires per defined guidelines for conducting compliance testing.	
7	The Platform should support applying weight to questions and responses.	
8	The Platform should be able to collect and store the Management responses.	
9	Platform should provide the ability to report on ISO 27001 conformance in conjunction with a certification effort.	
10	Platform should support complete automation of applicable frameworks like RBI, NBFC, SEBI CSCRF CCI , PFRDA ICSPG , UPI ISCF , IRDAI ICSG, SOC Efficacy Automation and other regulatory frameworks should be supported. RBI Master Directions, IT Outsourcing and other relevant frameworks should be supported out of box. Platform should have pre-mapped controls for regional and regulatory frameworks like SEBI, RBI,IRDAI,PFRDA,UADIA, NBFC and others applicable to Bank.	
	Reports & dashboard	
11	The Platform should be able to generate report of ISO 27001 statement of applicability based on controls already existing or controls which are planned to be implemented.	
12	The Platform should provide aging reports to track findings and remediation plans that are overdue.	
13	The Platform should be able to generate report on control effectiveness metrics for continual improvement of ISMS.	
14	The Platform should be able to generate report on Risk levels on risk assessment and risk treatment to showcase mitigation status.	
15	The Platform should be able to generate Risk Treatment Plan implementation progress report.	
16	The Platform should be able to demonstrate open risk status with implementation progress, control gaps and assets affected.	

17	The Platform should provide the ability to create a risk summary report that describes key risks, how they are being managed and monitored, remediation of key issues and accountability.	
18	The Platform should show dashboard including current audit findings, remediation status, remediation progress and responsibility.	
19	The Platform should be able to generate reports on audit findings, remediation, and responsibility	
20	The Platform should have options to display all the asset, risk, audit, action items and training related metrics in one single dashboard	
21	The Platform should provide a variety of layout options enabling user to alter the user interface/dashboard.	
22	The Platform should allow for aggregation of risks across the organization and generate the various dashboards and reports basis senior leader's requirement such as CISO Dashboard, CEO Dashboard.	
23	The system should provide reports on critical findings, progress of remediation, and status.	
24	The Platform should allow users to perform keyword searches to quickly find specific information among various Information Security policies.	
25	The system should have the ability to define frequency of various review and reporting for outstanding issues and assigned task.	
26	The Platform should have the ability to document control activities and capture details like control owners, testing requirements, mapping with compliance, risk, business unit etc	
27	The Platform should support explicit dashboards for SEBI, RBI,PFRDA,SEBI,IRDA and other relevant Bank regulations and frameworks.	
28	Should have all Cyber GRC components in a single product and a single dashboard to view and monitor Technical/Compliance/Vendor risks.	
	Technological Risk Management Features	

29	The Platform should support cyber risk assessments for both inherent and residual risk.	
30	The Platform should have ability to provide a clear way to score quantitatively the vulnerabilities and risks identified based on threat, impact and compensating controls	
31	The Platform should provide an out of the box risk register in order to capture currently maintained and tracked risks as well as ability to configure the application via no coding to accommodate our requirements.	
32	The Platform shall have capabilities to perform risk assessments as per risk category and/or threat category	
33	The Platform should have capability to define and automate the frequency of conducting the Cyber Security risk assessment and automatically generating reports across various levels such as vertical head/business unit head / business/practice manager, asset owner as well as board and management levels.	
34	The Platform should include multiple impact categories to evaluate criticality of the business process.	
35	The Platform should be able to capture robust details about each risk item including objectives, products and services, business processes, risks, threats, vulnerability, impact, like hood controls, physical facilities, technology assets, policies, and procedures.	
36	Risk assessments must have both qualitative and quantitative approaches.	
37	The Platform should calculate, display, and report risk scores. Risk calculations must be transparent to users.	
38	The Platform should give users full control over risk calculation parameters, weightings.	
39	The Platform should support custom risk assessment methodologies and algorithms.	
40	The Platform must keep the History of last 7 years risk.	
41	The Platform should have the ability to capture and document risk response procedures as well as mitigating controls.	

42	The Platform should have the ability to link, and map identified risk to Authoritative Sources, departments, asset, and divisions	
43	The Platform should capture recovery time objective (RTO) and recovery point objective (RPO) for business processes and calculate the result as overall business criticality rating for the asset and/or process.	
44	The Platform should be able to demonstrate control effectiveness metrics measurements in a comparable way against thresholds decided for metrics.	
45	The Platform should include workflow for multiple participants in the BIA (Business Impact Analysis) process, including the business process owner and others that may need to provide input, as well as review by another level and the BCM (Business Continuity Management) team	
46	To support the BIA, the Platform should enable mapping of business processes to their supporting IT Service, Process, and Personnel.	
47	The Platform should provide Cyber Risk Management system and Cyber Audit Management.	
48	The Platform should be enabled to manage exceptions with appropriate risk sign-off/acceptance based on the current process in line with best security practices	
49	The Platform should have capability for multiple levels of approvals for Exception Management	
	IT & Cyber Risk Integration	
50	The Platform should have capability to integrate with various security and IT controls such MS Active Directory, IBM Q-Radar (SIEM), Vulnerability Management (Qualysis), Patch Management, ARCON PAM, BMC ITSM tool, Anti-Virus (Symantec), TrendMicro Deep Security & EDR, MDM Solution, NAC, DLP, DSPM, XSOAR, TIM, Squal1(VAPT Management Tool) relevant tools/application developed in house or procured outside etc. It includes all the tools as applicable as per business needs to meet Information Technology and Cyber Security fulfilment from Governance, Compliance and Risk Management perspective	

51	The communication between various components of the Platform & with other integrated systems must use authenticated and encrypted channels.	
52	The Platform should offer a library of technical baseline configuration procedures mapped to various technologies.	
53	The Platform should have capability to use external data by having an API connection or any alternate connection method with the data source. The Platform should also allow the importing the actual data in standard file format, such as csv, xls, etc.	
54	The Platform should have capability to do Risk Based Prioritization of vulnerabilities. Automatic differential analysis of closures across assessments	
55	The Platform should have capability to track Vendor Risks by onboarding Third Party Vendors and send out Questionnaires	
	General Requirements	
56	The Platform administrative console and user application must be accessible by latest browser across Bank locations	
57	The Platform should maintain the audit trail/logs sufficiently for all user access and all the changes done on it.	
58	The Platform 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.	
60	The Platform should work in high availability module and vendor should provide the Platform within the defined SLA	
61	The Platform should be implemented with latest security hardening standard and comply with security standards such as CIS Benchmark, NIST CSF and OWASP etc.	
62	The Cyber GRC Platform based solution must be an on-premises and use the existing Bank's virtualization platform for successful deployment and operationalisation.	
63	The Platform licenses must be provided an access to 100 users with all functionalities in the proposed SOW which can be expanded as per need.	

64	The Platform must allow the Role based user access and must have nonrepudiation control. Access to the application must be as per role and template configured for the user.	
65	Platform should have the capability to move from one tool to another, to allow that migration will full backup of data along with proper data integrity	
66	The Platform must allow the Scope Based User access and must have capability to restrict access to Audits and Risk assessments based on Asset, Asset Groups, Business Units	
67	The Platform must allow configurable Notification Settings which are granular to send out Email Notifications and Reminders	
	Compliance Management Features	
68	The Platform should facilitate that Compliance Management Process requirements can be mapped to a business function.	
69	The Platform should have capability to record the consequences of non-compliance and adequate dashboards as well as reporting.	
70	The Platform should be able to calculate compliance scores as per standard, framework, regulation, department, including dynamically defined groups.	
71	The Platform should have capability to perform compliance gap analysis.	
72	The Platform should have capability to track checklists and assign to different stake holders with clear Dashboards to track Task completion and Observations	
73	The Platform should have capability to track RBI and related Regulatory Circulars on an ongoing basis and also notify any changes to track the compliance.	
	Workflow Automation & AI Capabilities	
74	The Platform should provide built in as well as customizable workflows to track, IT Risk issues, Cyber threats, vulnerabilities, VAPT Findings, Audit Findings, Compliance findings, internal/external audits, critical incidents etc. It should support the automation of workflows to the extent possible to meet the GRC goals defined in the scope of work.	

75	The platform shall have AI support for analysis and recommendations & Integration with Chatbot	
76	The solution should have automated risk and compliance workflows to minimize manual effort in assessments and approvals. It should include AI-driven risk prediction capabilities to proactively identify emerging risks.	
77	The solution should feature an AI-powered compliance chatbot to provide instant support for policy queries and risk recommendations.	
78	The Platform should provide calendarization capabilities of VAPT assessments of all types (Change Requests, Retest Requests) for Application Assessments, Red Teaming exercises , Internal and External VAPT to send automated reminders and notifications as per Bank's policies	
79	AI capabilities to reduce effort and improve efficacy	
80	Should have all Cyber GRC components in a single product and a single dashboard to view and monitor Technical/Compliance/Vendor risks.	

PART B

The consolidated scoring matrix:

Sr. No.	**Evaluation category**	**Evaluation criteria**	**Scoring Logic**	**Criteria Weightage**

01	Solution Implementation and Service Experience in the BFSI	Number of years' Experience in providing and successful implementation of the similar platform / solution to the BFSI organisation.	1 Year - 5 Marks 2 years-10 Marks 3 years - 15 Marks >3 years - 20 Marks	20 Marks
02	Solution Implementation and Service Experience in the BFSI	Experience in terms of completed number of projects.	1 Year - 5 Marks 2 years-10 Marks 3 years - 15 Marks >3 years - 20 Marks	20 Marks
03	Presentation for Approach and Methodology	Presentation	Presentation representing proposed implementation plan and detailed approach/ methodology to be adopted for delivering the project deliverables. (Maximum duration for presentation - 45 minutes)	40 Marks
04		The Bidder's ability to meet Technical Requirements (Part A)		40 Marks
Cut off Marks = 84			**Total Score**	**120 Marks**

We confirm that our proposed Solution meet all the specifications mentioned as above.

Signature and Seal of Company

Annexure F: Commercial Bid Format

1. Please be guided by RFP terms, subsequent amendments and replies to pre-bid queries (if any) while quoting.
2. Do not change structure of format nor add any extra items.

3. No counter condition/assumption in response to commercial bid will be accepted. Bank has a right to reject such bid.

The Commercial Bid shall be submitted in the following format:

Sr. No.	Product Name	Product Description	Qty (Nos)	Unit cost	Total cost for One year	Total cost for Three Years
1	Supply, Implementation and Support Services for Cyber Governance, Risk and Compliance Platform.	License Type: Annual subscription base. If the Product license is based on only the Perpetual license, then you may quote for a perpetual price which we will consider. Cyber GRC users required =100 users (minimum) Security solution integration required=500 (minimum)	1			
2	Database License Cost (non-oracle) + Database AMC	Perpetual licenses (HA + DR)	3			
3	Training	As per Scope of work (10 resources on site)	1			
4	Annual Technical Support		1			
5	Total Amount (Excluding of GST)					

OPTIONAL

Sr. No.	Product Name	Product Description	Qty (Nos)	Unit cost	Total cost for One year	Total cost for Three Years
1	**[Optional]** Supply, Implementation and Support Services for TPRM Platform.	License Type: Annual subscription base. If the Product license is based on only the Perpetual license, then you may quote for a perpetual price which we will consider. Cyber GRC users required =100 users (minimum)	1			

Note: In case of oracle Database, bank will procure license itself.

In case of any additional license requirement during the contract period, the Bidder shall provide the additional licenses at the same rate as finalized in purchase order. The price of additional licenses shall remain applicable from the date of activation of such licenses till the end of the contract period.

a) These details should be on the letter head of the bidder and each & every page should be signed by an authorized signatory with name and seal of the company.

b) Please be guided by RFP terms, subsequent amendments and replies to pre-bid queries (if any) while quoting.

c) Do not change structure of format nor add any extra items.

d) No counter condition/assumption in response to commercial bid will be accepted. Bank has a right to reject such bid.

e) The bidder needs to clearly indicate if there are any recurring costs included in the above bid and quantify the same. In the absence of this, the bidder would need to provide the same without any charge. Bidder should make no changes to the quantity.

f) If the cost for any line item is indicated as zero then it will be assumed by the Bank that the said item is provided to the Bank without any cost.

g) All prices are to be in Indian Rupee (INR) only.

h) Prices quoted by the Bidder should be inclusive of all taxes, duties, levies etc. except GST which will be paid extra at actuals.

i) All Quoted Commercial Values should comprise of values only up to 2 decimal places. Bank for evaluation purpose will consider values only up to 2 decimal places for all calculations & ignore all figures beyond 2 decimal places.

Signature with Seal
Date:
Name:
Designation:

Annexure G: Bank Guarantee Format

Dated:____________________________

Bank:______________________________

To

Jammu & Kashmir Bank M.A. Road, Srinagar, 190 001 J&K.

WHEREAS.. (Company Name) and having its Registered Office at.. India (hereinafter referred to as "the Bidder") proposes to respond to RFP No ...., dated .... of Jammu and Kashmir Bank Ltd for selection of vendor for

Supply, Implementation and Support Services for Cyber Governance, Risk and Compliance Platform (Herein after called the "RFP") AND

WHEREAS, in terms of the conditions as stipulated in the RFP, the bidder is required to furnish a Bank Guarantee in lieu of the Earnest Money Deposit (EMD), issued by a scheduled commercial bank in India in your favour to secure the order under Schedule 1 of the RFP in accordance with the RFP Document (which guarantee is hereinafter called as "BANK GUARANTEE") AND WHEREAS the bidder has approached us, ... for providing the BANK GUARANTEE.

AND WHEREAS at the request of the bidder and in consideration of the proposed RFP to you, We ,...having Branch Office/Unit amongst others at.., India and registered office/Headquarter at..have agreed to issue the BANK GUARANTEE.

THEREFORE, We, ………………………………………………, through our local office at……………………………………… India furnish you the Bank GUARANTEE in manner hereinafter contained and agree with you as follows:

1) We………………………………, undertake to pay the amounts due and payable under this Guarantee without any demur, merely on demand from you and undertake to indemnify you and keep you indemnified from time to time to the extent of

   Rs……………………(Rupees …………………………only) an amount equivalent to the EMD against any loss or damage caused to or suffered by or that may be caused to or suffered by you on account of any breach or breaches on the part of the bidder of any of the terms and conditions contained in the RFP and in the event of the bidder commits default or defaults in carrying out any of the work or discharging any obligation in relation thereto under the RFP or otherwise in the observance and performance of any of the terms and conditions relating thereto in accordance with the true intent and meaning thereof, we shall forthwith on demand pay to you such sum or sums not exceeding the sum of

   Rs…………………(Rupees………………………………… only) as may be claimed by you on account of breach on the part of the bidder of their obligations in terms of the RFP.

   Any such demand made on the Bank shall be conclusive as regards amount due and payable by the Bank under this guarantee.

2) Notwithstanding anything to the contrary contained herein or elsewhere, we agree that your decision as to whether the bidder has committed any such default or defaults and the amount or amounts to which you are entitled by reasons thereof will be binding on us and we shall not be entitled to ask you to establish your claim or claims under Bank Guarantee but will pay the same forthwith on your demand without any protest or demur.

3) This Bank Guarantee shall continue and hold good until it is released by you on the application by the bidder after expiry of the relative guarantee period of the RFP and after the bidder had discharged all his obligations under the RFP and produced a certificate of due completion of work under the said RFP and submitted a “ No Demand Certificate “ provided always that the guarantee shall in no event remain in force after the day of ………………………without prejudice to your claim or claims arisen and demanded from or otherwise notified to us in writing before the expiry of the said date which will be enforceable against us notwithstanding that the same is or are enforced after the said date.

4) Should it be necessary to extend Bank Guarantee on account of any reason whatsoever, we undertake to extend the period of Bank Guarantee on your request under intimation to the SI/OEM till such time as may be required by you. Your decision in this respect shall be final and binding on us.

5) You will have the fullest liberty without affecting Bank Guarantee from time to time to vary any of the terms and conditions of the RFP or extend the time of performance of the RFP or to postpone any time or from time to time any of your rights or powers against the bidder and either to enforce or forbear to enforce any of the terms and conditions of the said RFP and we shall not be released from our liability under Bank Guarantee by exercise of your liberty with reference to matters aforesaid or by reason of any time being given to the bidder or any other forbearance, act or omission on your part of or any indulgence by you to the bidder or by any variation or modification of the RFP or any other act, matter or things whatsoever which under law relating to sureties, would but for the provisions hereof have the effect of so releasing us from our liability hereunder provided always that nothing herein contained will enlarge our liability hereunder beyond the limit of Rs.................(Rupees..................................only) as aforesaid or extend the period of the guarantee beyond the said day of .... unless expressly agreed to by us in writing.

6) The Bank Guarantee shall not in any way be affected by your taking or giving up any securities from the bidder or any other person, firm or company on its behalf or by the winding up, dissolution, insolvency or death as the case may be of the bidder

7) In order to give full effect to the guarantee herein contained, you shall be entitled to act as if we were your principal debtors in respect of all your claims against the bidder hereby guaranteed by us as aforesaid and we hereby expressly waive all our rights of surety ship and other rights, if any, which are in any way inconsistent with any of the provisions of Bank Guarantee.

8) Subject to the maximum limit of our liability as aforesaid, Bank Guarantee will cover all your claim or claims against the bidder from time to time arising out of or in relation to the said RFP and in respect of which your claim in writing is lodged on us before expiry of Bank Guarantee.

9) Any notice by way of demand or otherwise hereunder may be sent by special courier, telex, fax or registered post to our local address as aforesaid and if sent accordingly it shall be deemed to have been given when the same has been posted.

10) The Bank Guarantee and the powers and provisions herein contained are in addition to and not by way of limitation of or substitution for any other guarantee or guarantees here before given to you by us (whether jointly with others or alone) and that Bank Guarantee is not intended to and shall not revoke or limit such guarantee or guarantees.

11) The Bank Guarantee shall not be affected by any change in the constitution of the bidder or us nor shall it be affected by any change in your constitution or by any amalgamation or absorption thereof or therewith but will ensure to the benefit of and be available to and be enforceable by the absorbing or amalgamated company or concern.

12) The Bank Guarantee shall come into force from the date of its execution and shall not be revoked by us any time during its currency without your previous consent in writing.

13) We undertake to pay to you any money so demanded notwithstanding any dispute or disputes raised by the bidder in any suit or proceeding pending before any court or Tribunal relating thereto our liability under this present being absolute and unequivocal.

14) The Bank Guarantee needs to be submitted in online form also via SFMS Application.

15) Notwithstanding anything contained herein above;

    a. our liability under this Guarantee shall not exceed Rs...(Rupees......................................only);

    b. this Bank Guarantee shall be valid up to and including the date .... ______and claim period shall be upto_____; and

    c. We are liable to pay the guaranteed amount or any part thereof under this Bank Guarantee only and only if you serve upon us a written claim or demand on or before the expiry of the claim period.

16) 16. We have the power to issue this Bank Guarantee in your favour under the Memorandum and Articles of Association of our Bank and the undersigned has full power to execute this Bank Guarantee under the Power of Attorney issued by the Bank.

For and on behalf of BANK

Authorized Signatory

Seal

Address

Annexure H: Performance Bank Guarantee Format

To
The Jammu & Kashmir Bank M.A. Road, Srinagar,
190 001 J&K.

WHEREAS.................................. (Company Name) registered under the Indian Companies Act 1956 and having its Registered Office at ...., hereinafter referred to as the VENDOR has for taken up for........ ....in terms of the Purchase Order bearing No. .... Dated ...., hereinafter referred to as the CONTRACT. AND WHEREAS in terms of the Conditions stipulated in the said Contract, the VENDOR is required to furnish, performance Bank Guarantee issued by a Scheduled Commercial Bank in your favor to secure due and satisfactory compliance of the obligations of the VENDOR in accordance with the Contract; THEREFORE, WE, ..., through our local office at .... Furnish you this Performance Guarantee in the manner hereinafter contained and agree with you as follows:

1. We, ... do hereby undertake to pay the amounts of ₹.............. and payable under this Guarantee without any demur, merely on a demand, which has to be

served on us before the expiry of this guarantee, time being essence of the contract, from you stating that the amount claimed is due by way of loss or damage caused to or would be caused to or suffered by you by reason of breach by the said vendor of any of the terms and conditions contained in the Contract or by reason of the vendor's failure to perform the said contract. Any such demand made on us within the time stipulated above shall be conclusive as regards the amount due and payable by us under this guarantee. However, our liability under this guarantee shall be restricted to an amount not exceeding............. (Rupees .... Only).

2. We undertake to pay to you any money so demanded notwithstanding any dispute/s raised by the vendor in any suit or proceeding before any Court or Tribunal relating thereto, our liability under these presents being absolute and unequivocal. The payment so made by us under this guarantee shall be a valid discharge of our liability for payment there under and the vendor shall have no claim against us for making such payment.

3. We further agree that, if demand, as stated above, is made on us within the stipulated period, the guarantee herein contained shall remain in full force and effect and that it shall continue to be enforceable till all your dues under or by virtue of the said contract have been fully paid and your claims satisfied or discharged or till you certify that the terms and conditions of the said contract have been fully and properly carried out by the said vendor and accordingly discharge this guarantee. Provided, however, serving of a written claim / demand in terms hereof on us for payment under this guarantee on or before the stipulated period , time being the essence of contract, shall be a condition precedent for accrual of our liability / your rights under this guarantee.

4. We further agree with you that you shall have the fullest liberty without our consent and without affecting in any manner our obligations hereunder, to vary any of the terms and conditions of the said Contract or to extend time for performance by the said vendor from time to time or to postpone for any time or from time to time any of the powers exercisable by us against the said VENDOR and to forbear or enforce any of the terms and conditions relating to the said Contract and we shall not be relieved from our liability by reason of such variation, or extension being granted to the said Vendor or for any forbearance, act or omission on our part or any indulgence by us to the said vendor or by any such matter or thing whatsoever which under the law relating to sureties would, but for this provision, have effect of so relieving us.

5. This Guarantee will not be discharged due to the change in the constitution of our Bank or the Vendor.

6. We further agree and undertake unconditionally without demur and protest to pay you the amount demanded by you in writing irrespective of any dispute or controversy between you and the VENDOR.

7. We lastly undertake not to revoke this guarantee during its currency except with your written Consent. NOTWITHSTANDING anything contained herein above;

(i) Our liability under this Guarantee shall not exceed..Rupees......................................
.only);

(ii) This Guarantee shall be valid up to ....; and claim period of this Bank Guarantee shall be .... year/s after expiry of the validity period i.e., up to..........................; and

(iii) We are liable to pay the guaranteed amount or any part thereof under this Bank Guarantee only and only if you serve upon us a written claim or demand on or before the expiry of this guarantee.

Dated the................. Day of ....20.....
For...
BANK Authorized Signatory

Annexure I: Non-disclosure Agreement (NDA)

THIS NON DISCLOSURE AGREEMENT (the "Agreement") is made and entered into as of (____/____/2025) by and between

____, a company incorporated under the laws of India, having its registered address at ________________________________ (the "Receiving party/Company") and

"Jammu and Kashmir Bank Ltd, a Banking Company under Indian Companies Act,2013 having corporate and registered office at M.A.Road,Srinagar,J&K,India-190001 represented herein by Authorized Signatory (hereinafter referred as Bank/Disclosing Party which unless the context requires include its successors in interests and permitted assigns). (the "Bank/Disclosing Party").

The Company/Receiving party and Bank/Disclosing Party are hereinafter collectively referred to as parties and individually as a party.

Whereas the parties have entered into contract and for performance of contract, the parties may share/disclose certain proprietary/confidential information to each other. To protect the confidentiality of the confidential information shared/disclosed, the parties hereto have entered into this NDA.

NOW THEREFORE THIS AGREEMENT WITNESSETH AS FOLLOWS:

1. **Purpose** J&K Bank/Disclosing Party has engaged or wishes to engage the Company/Receiving party for undertaking the project vide Purchase Order No: ____ and each party may disclose or may come to know during the course of the project certain confidential technical and business information which the disclosing party desires the receiving party to treat as confidential.

2. **Confidential Information** means any information disclosed or acquired by other party during the course of the projects, either directly or indirectly, in writing, orally or by inspection of tangible objects (including without limitation documents, prototypes, samples, technical data, trade secrets, know-how, research, product plans, services, customers, markets, software, inventions, processes, designs, drawings, marketing plans, financial condition and the Company's plant and equipment), which is designated as "Confidential," "Proprietary" or some similar designation. Information communicated orally shall be considered Confidential Information if such information is confirmed in writing as being Confidential Information within a reasonable time after the initial disclosure. Confidential Information may also include information disclosed to a disclosing party by third parties. Confidential Information shall not, however, include any information which

i. was publicly known and made generally available in the public domain prior to the time of disclosure by the disclosing party;

ii. becomes publicly known and made generally available after disclosure by the disclosing party to the receiving party through no action or inaction of the receiving party;

iii. is already in the possession of the receiving party at the time of disclosure by the disclosing part as shown by the receiving party's files and records immediately prior to the time of disclosure;

iv. is obtained by the receiving party from a third party without a breach of such third party's obligations of confidentiality;

v. is independently developed by the receiving party without use of or reference to the disclosing party's Confidential Information, as shown by documents and other competent evidence in the receiving party's possession; or

vi. Is required by law to be disclosed by the receiving party, provided that the receiving party gives the disclosing party prompt written notice of such requirement prior to such disclosure and assistance in obtaining an order protecting the information from public disclosure.

3. Non-use and Non-disclosure. Each party agrees not to use any Confidential Information of the other party for any purpose except to evaluate and engage in discussions concerning a potential business relationship between the parties. Each party agrees not to disclose any Confidential Information of the other party to third parties or to such party's employees, except to those employees of the receiving party who are required to have the information in order to evaluate or engage in discussions concerning the contemplated business relationship. Neither party shall reverse engineer, disassemble, or decompile any prototypes, software or other tangible objects which embody the other party's Confidential Information and which are provided to the party hereunder.

4. Maintenance of Confidentiality. Each party agrees that it shall take reasonable measures to protect the secrecy of and avoid disclosure and unauthorized use of the Confidential Information of the other party. Each party shall take at least those measures that it takes to protect its own most highly confidential information and shall ensure that its employees who have access to Confidential Information of the other party have signed a non-use and non-disclosures agreement in content similar to the provisions hereof, prior to any disclosure of Confidential Information to such employees. Neither party shall make any copies of the Confidential Information of the other party unless the same are previously approved in writing by the other party. Each party shall reproduce the other party's proprietary rights notices on any such approved copies, in the same manner in which such notices were set forth in or on the original. Each party shall immediately notify the other party in the event of any unauthorized use or disclosure of the Confidential Information.

5. No Obligation. Nothing herein shall obligate either party to proceed with any transaction between them and each party reserves the right, in its sole discretion, to terminate the discussions contemplated by this Agreement concerning the business opportunity. This Agreement does not constitute a joint venture or other such business agreement.

6. No Warranty. All Confidential Information is provided by Bank as "AS IS." Bank/Disclosing Party makes no warranties, expressed, implied or otherwise, regarding its accuracy, completeness or performance.

7. Return of Materials. All documents and other tangible objects containing or representing Confidential Information which have been disclosed by either party to the other party, and all copies thereof which are in the possession of the other party, shall be and remain the property of the disclosing party and shall be promptly returned to the disclosing party upon the disclosing party's written request.

Receiving Party shall immediately return and redeliver to Disclosing Party/ Bank all tangible material embodying the Confidential Information provided hereunder and all notes, summaries, memoranda, , records, excerpts or derivative information deriving there from and all other documents or materials ("Notes") (and all copies of any of the foregoing, including "copies" that have been converted to computerized media in the form of image, data or word processing files either manually or by image capture) based on or including any Confidential Information, in whatever form of storage or retrieval, upon the earlier of (i) the completion or termination of the dealings between the parties contemplated hereunder; (ii) the termination of the Master Agreement; or (iii) at such time as the Disclosing Party/ Bank may so request.

The receiving party shall destroy /dispose off the confidential information provided by the disclosing party together with its copies upon written request of the disclosing party, as per the directions issued by the disclosing party and such destruction shall be confirmed in writing by receiving party.

8. No License. Nothing in this Agreement is intended to grant any rights to either party under any patent, mask work right or copyright of the other party, nor shall this Agreement grant any party any rights in or to the Confidential Information of the other party except as expressly set forth herein.

9. Term. The Obligations of each receiving party hereunder shall survive even after this agreement except as provided herein above.

10. Adherence. The content of the agreement is subject to adherence audit by J&K Bank. It shall be the responsibility of the Company/Receiving party to fully cooperate and make available the requisite resources/evidences as mandated by J&K Bank Supplier Security policy.

11. Remedies. Each party agrees that any violation or threatened violation of this Agreement may cause irreparable injury to the other party, entitling the other party to seek injunctive relief in addition to all legal remedies.

12. Arbitration, Governing Law & Jurisdiction. In the case of any dispute arising upon or in relation to or in connection with this Agreement between parties, the disputes shall at the first instance be resolved through negotiations. If the dispute cannot be settled amicably within fourteen (14) days from the date on which either Party has served written notice on the other of the dispute then any party can submit the dispute for arbitration under Arbitration and conciliation Act,1996 through sole arbitrator to be appointed mutually by the parties.

The place of Arbitration shall be Srinagar, India and the language of the arbitration proceedings and that of all the documents and communications between the parties shall be English.

The decision of the arbitrator shall be final and binding upon the parties. The expenses of the arbitrator as determined by the arbitrator shall be borne equally.

The parties shall continue to be performing their respective obligations under this Agreement, despite the continuance of the arbitration proceedings, except for the disputed part under arbitration. This agreement shall, in all respects, be governed by, and construed in accordance with the Laws of the UT of J&K read with applicable Laws of India. The Courts in Srinagar India shall have exclusive jurisdiction in relation to this agreement.

All notices or other communication under or in connection with this agreement shall be given in writing and may be sent by personal delivery, or post or courier or facsimile or email. Any such notice or other communication will be deemed to be effective if sent by personal delivery, when delivered, if sent by post, five days after being deposited in the post office and if sent by courier, three days after being deposited with the courier, if sent by facsimile, when sent (on receipt of a confirmation of having been sent to correct facsimile number) and if sent my mail (on receipt of confirmation).

_____________(contact details of Company/Receiving party)

_____________(contact details of Bank/Disclosing Party).

13. Miscellaneous. This Agreement shall bind and intended for the benefit of the parties hereto and their successors and assigns. This document contains the entire Agreement between the parties with respect to the subject matter hereof, and neither party shall have any obligation, express or implied by law, with respect to trade secret or propriety information of the other party except as set forth herein. Any failure to enforce any provision of this Agreement shall not constitute a waiver thereof or of any other provision.

Any provision of this Agreement may be amended or waived if, and only if such amendment or waiver is in writing and signed, in the case of amendment by each Party, or in the case of a waiver, by the party against whom the waiver is to be effective".

COMPANY NAME	**Bank**
By:______________________________	By:______________________________
Name: ___________________________	Name: ___________________________
Title: ____________________________	Title: ____________________________
Address:__________________________	Address:__________________________
__________________________________	__________________________________
Company Seal	Company Seal

The undersigned represent that they have the authority to enter into this Agreement on behalf of the person, entity or corporation listed above their names.

Bidder has to submit Undertaking on company letter head as per format given below

Annexure J: Undertaking

To

Chief Information Security Officer

Information Security Department

The Jammu & Kashmir Bank M.A. Road, Srinagar,

190 001 J&K.

Dear Sir,

Sub: RFP no: ___________ for selection of bidder Supply, Implementation and Support Services for Cyber Governance, Risk and Compliance Platform . Having examined the tender documents including all annexures the receipt of which is hereby duly acknowledged, we, the undersigned, offer to provide _____________to Bank as mentioned in RFP document in conformity with the said tender documents in accordance with the Commercial bid and made part of this tender.

We understand that the RFP provides generic specifications about all the items and it has not been prepared by keeping in view any specific bidder.

We understand that the RFP floated by the Bank is a confidential document and we shall not disclose, reproduce, transmit or made available it to any other person.

We have read, understood and accepted the terms/ conditions/ rules mentioned in the RFP

Until a formal contract is prepared and executed, this tender offer, together with the Bank's written acceptance thereof and the Bank's notification of award, shall constitute a binding contract between us.

We undertake that in competing for and if the award is made to us, in executing the subject Contract, we will strictly observe the laws against fraud and corruption in force in India and the UT of J&K including Prevention of Corruption Act 1988.

We have never been barred/black-listed by any regulatory / statutory authority in India.

We understand that the Bank is not bound to accept the lowest or any offer the Bank may receive.

This Bid, together with your written acceptance thereof and your notification of award, shall constitute a binding Contract between us.

We certify that we have provided all the information requested by the Bank in the format requested for. We also understand that the Bank has the exclusive right to reject this offer in case the Bank is of the opinion that the required information is not provided or is provided in a different format. It is also confirmed that the information submitted is true to our knowledge and the Bank reserves the right to reject the offer if anything is found incorrect.

Place:

Seal and signature of the bidder

Annexure K: Know Your Employee (KYE) Clause

Bidder has to submit Undertaking on company letter head as per format given below.

We on the behalf of ________________________ (name of the company) hereby confirm that all the resources (both on-site and off-site) working on the Bank's project ie **Supply, Implementation and Support Services for Cyber Governance, Risk and Compliance Platform** (Name of the RFP) have undergone KYE (Know Your Employee) process and all the required checks have been performed prior to employment of said employees as per our policy.

We confirm to defend and keep the bank indemnified against all loss, cost, damages, claim penalties expenses, legal liability because of non-compliance of KYE and of misconduct of the employee deployed by us to the Bank.

We further agree to submit the required supporting documents (Process of screening, Background verification report, police verification report, character certificate, ID card copy, Educational document, etc.) to Bank before deploying officials in Bank premises for ________________ (Name of the RFP)."

Sign and seal of Competent Authority

Name of Competent Authority

Dated

Annexure L: Service Level Agreement

This Service Level agreement (“Agreement”) is made at Srinagar (J&K) on this ……….day of ……….2023 between

i. “The Jammu and Kashmir Bank Ltd, a Banking Company under Indian Companies Act,2013 having corporate and registered office at M.A.Road,Srinagar,J&K,India-190001 represented herein by Authorized Signatory (hereinafter referred as **Bank** which unless the context requires include its successors in interests and permitted assigns) of the

ONE PART, through its authorized signatory Mr.……………………………………………….

and

ii. M/S ………………………………………………….., registered under the …………………………………….

Act, having its Registered Office at ……………………………………………………………………………… (Hereinafter referred to as the "Company" which expression shall unless it be repugnant to the context or meaning thereof, include its successors and assigns) of the OTHER PART, through its authorized signatory Mr.…………………………………………….

The Bank and Company are hereinafter collectively referred to as ‘Parties’ and individually as a ‘Party’.

Now therefore, this Agreement is witnessed as under:

Definitions of the terms

The Bank/J&K Bank:	Reference to the “the Bank”, “Bank” and “Purchaser” shall be determined in context and may mean without limitation “The Jammu & Kashmir Bank”.
Bidder/Vendor/Supplier:	An eligible entity/firm submitting a Proposal/Bid in response to this RFP.1

Proposal/Bid:	The Bidder's written reply or submission in response to this RFP.
RFP:	The request for proposal (this document) in its entirety, inclusive of any addenda that may be issued by the Bank.
The Contract:	The agreement entered into between the Bank and the Company, as recorded in this Contract Form signed by the parties, including all attachments and appendices thereto and all documents incorporated by reference therein.
The Contract Price:	The price payable to the Company under the Contract for the full and proper performance of its contractual obligations.
The Product:	All of the software or software, all hardware, database, middleware, operating systems and/or other materials which the Company is required to supply to the Bank under the Contract.
System:	A Computer System consisting of all Hardware, Software, etc., which should work together to provide the services as mentioned in the Bid and to satisfy the Technical and Functional Specifications mentioned in the Bid.
Specified Bank Location:	Banks Data Centre located at Noida and Banks Disaster Recovery Site Located at Mumbai.
PBG:	Performance Bank Guarantee.
Data Centre (DC):	Banks Data Centre located at Noida.
Disaster Recovery (DR):	Banks Disaster Recovery Site located at Mumbai.
Material Breach:	Company failure to perform a major part of this Agreement.

Charges:	Commercials as per Purchase Order.
Confidential Information:	It includes all types of Information that will be found on BANK systems that the Company may support or have access to including, but are not limited to, Information subject to special statutory protection, legal actions, disciplinary actions, complaints, IT security, pending cases, civil and criminal investigations, etc.

Scope of Work

The scope of work under this Cyber GRC requirement is to supply, implementation and support services towards Cyber GRC solution as per scope of work & specifications prescribed under.

Detailed Scope of Work:

The Bidders should have the capability which includes end to end solution deliverables such as provision of software licenses including Third Party Software, Database etc., implementation, customization, business case testing and result summarisation, production rollout, operational service support, and proposed integration capabilities within the Cyber GRC platform. The existing technologies related integrations including but not limited MS Active Directory, IBM Q-Radar (SIEM), Vulnerability Management (Qualysis), Patch Management, ARCON PAM, BMC ITSM tool, Anti-Virus (Symantec), TrendMicro Deep Security & EDR, MDM Solution, NAC, DLP, DSPM, XSOAR, TIM, Squal1(VAPT Management Tool) relevant tools/application developed in house or procured outside etc. It includes all the tools as applicable as per business needs to meet Information Technology and Cyber Security fulfilment from Governance, Compliance and Risk Management perspective.

The listed modules shall provide collective status in a graphical representation which will help to automate the process to closure. Details of required modules are shown below:

a) Information Security Risk Management

b) Information Security Policy & Procedure Management

c) Information Security Audit Management (Internal & External)

d) Compliance Management – (IT Risk, Cyber Risk)

e) Business Continuity Management

f) Workflow automation and integration (integration with existing tools)

g) Reporting and Dashboard (Strong reporting tools and dashboard)

h) User Access & RBAC (granular access controls) and Scope Based Access Controls to provide granular permissions specific to Assets, Audits, Risks etc.

i) Scalability and cloud (scale up for future requirements)

j) Exception Management

k) Third Party Risk Management (TPRM)

Implementation of the proposed modules shall be carried out by prioritizing key modules as proposed in the scope of work.

Bidder is suggested to provide adequate supporting database/middleware software licenses except OS licenses in order to deliver the working solution in the various environment as applicable and necessary. Server OS related licenses will be provisioned by Bank including baseline infrastructure however optimisation of the computing resources shall be done by the shortlisted bidder.

Gap Analysis and Customisation

a) The Cyber GRC platform should be able to consider the addition new cyber module and/or modification of the existing modules.

b) The Bidder, in coordination with OEM should do Bank's actual requirements analysis and submit a detailed study of Bank's technology landscape, Information security policies, Cyber Security Policies, IT policies vs the Cyber GRC Solution architecture in line with proposed scope.

c) Also, bidder shall submit a detailed study of the requirements, current state, desired state and road map mentioning all the pre-requisites, timeframe of milestones/ achievements leading to the full operationalization of the solution vis-à-vis Bank's requirement to achieve the desired state.

d) The Bidder has to develop the high level and detailed project plan (including the Cyber security requirements), get it approved by the Bank and then implement the project based on timelines agreed.

e) In the solution design, the cyber-Security best practices should be taken care of by design and ensure those requirements are being implemented by team adequately.

f) The Solution’s Architecture deployment and related configurations done at the Bank which should be vetted by OEM / Bank personnel before Sign-Off.

The Cyber GRC platform shall provide the below features:

i. The Platform should have option to store Content (policies, controls, report templates, reference documentation).

ii. The Platform should have predefined risk assessment templates for global standards and allow and customizable assessment template as per Bank defined policies, standards, and other requirements.

iii. The Platform 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, DPDPA, ITIL v4.0. (The Bidder must provide the complete list of standards supported by the Platform.)

iv. Platform should support complete automation of applicable frameworks like RBI, NBFC, SEBI CSCRF CCI , PFRDA ICSPG , UPI ISCF , IRDAI ICSG, SOC Efficacy Automation and other regulatory frameworks should be supported. RBI Master Directions, IT Outsourcing and other relevant frameworks should be supported out of box. Platform should have pre-mapped controls for regional and regulatory frameworks like SEBI, RBI,IRDAI,PFRDA,UADIA, NBFC and others applicable to Bank.

v. The Platform should have the ability to document and maintain external benchmarks, frameworks, laws, and regulations identified for meeting the corporate objectives.

vi. The Platform should provide top-down or bottom-up approaches to developing key control procedures aligned with Bank's compliance requirements.

vii. The Platform should have the ability to provide built-in assessments, Control Self Assessments (CSA) and questionnaires as well as manually create assessments and questionnaires per defined guidelines for conducting compliance testing.

viii. The Platform should support applying weight to questions and responses.

ix. The Platform should be able to collect and store the Management responses.

x. Platform should provide the ability to report on ISO 27001 conformance in conjunction with a certification effort.

xi. The Platform should be able to generate report of ISO 27001 statement of applicability based on controls already existing or controls which are planned to be implemented.

xii. The Platform should provide aging reports to track findings and remediation plans that are overdue.

xiii. The Platform should be able to generate report on control effectiveness metrics for continual improvement of ISMS.

xiv. The Platform should be able to generate report on Risk levels on risk assessment and risk treatment to showcase mitigation status.

xv. The Platform should be able to generate Risk Treatment Plan implementation progress report.

xvi. The Platform should be able to demonstrate open risk status with implementation progress, control gaps and assets affected.

xvii. The Platform should provide the ability to create a risk summary report that describes key risks, how they are being managed and monitored, remediation of key issues and accountability.

xviii. The Platform should show dashboard including current audit findings, remediation status, remediation progress and responsibility.

xix. The Platform should be able to generate reports on audit findings, remediation, and responsibility

xx. The Platform should have options to display all the asset, risk, audit, action items and training related metrics in one single dashboard

xxi. The Platform should provide a variety of layout options enabling user to alter the user interface/dashboard.

xxii. The Platform should allow for aggregation of risks across the organization and generate the various dashboards and reports basis senior leader's requirement such as CISO Dashboard, CEO Dashboard.

xxiii. The system should provide reports on critical findings, progress of remediation, and status.

xxiv. The Platform should allow users to perform keyword searches to quickly find specific information among various Information Security policies.

xxv. The system should have the ability to define frequency of various review and reporting for outstanding issues and assigned task.

xxvi. The Platform should have the ability to document control activities and capture details like control owners, testing requirements, mapping with compliance, risk, business unit etc

xxvii. The Platform should support cyber risk assessments for both inherent and residual risk.

xxviii. The Platform should have ability to provide a clear way to score quantitatively the vulnerabilities and risks identified based on threat, impact and compensating controls

xxix. The Platform should provide an out of the box risk register in order to capture currently maintained and tracked risks as well as ability to configure the application via no coding to accommodate our requirements.

xxx. The Platform shall have capabilities to perform risk assessments as per risk category and/or threat category

xxxi. The Platform should have capability to define and automate the frequency of conducting the Cyber Security risk assessment and automatically generating reports across various levels such as vertical head/business unit head / business/practice manager, asset owner as well as board and management levels.

xxxii. The Platform should include multiple impact categories to evaluate criticality of the business process.

xxxiii. The Platform should be able to capture robust details about each risk item including objectives, products and services, business processes, risks, threats, vulnerability, impact, like hood controls, physical facilities, technology assets, policies, and procedures.

xxxiv. Risk assessments must have both qualitative and quantitative approaches.

xxxv. The Platform should calculate, display, and report risk scores. Risk calculations must be transparent to users.

xxxvi. The Platform should give users full control over risk calculation parameters, weightings.

xxxvii. The Platform should support custom risk assessment methodologies and algorithms.

xxxviii. The Platform must keep the History of last 7 years risk.

xxxix. The Platform should have the ability to capture and document risk response procedures as well as mitigating controls.

xl. The Platform should have the ability to link, and map identified risk to Authoritative Sources, departments, asset, and divisions xli. The Platform should capture recovery time objective (RTO) and recovery point objective (RPO) for business processes and calculate the result as overall business criticality rating for the asset and/or process.

xlii. The Platform should be able to demonstrate control effectiveness metrics measurements in a comparable way against thresholds decided for metrics.

xliii. The Platform should include workflow for multiple participants in the BIA (Business Impact Analysis) process, including the business process owner and others that may need to provide input, as well as review by another level and the BCM (Business Continuity Management) team

xliv. To support the BIA, the Platform should enable mapping of business processes to their supporting IT Service, Process, and Personnel.

xlv. The Platform should provide Cyber Risk Management system and Cyber Audit Management.

xlvi. The Platform should be enabled to manage exceptions with appropriate risk sign-off/acceptance based on the current process in line with best security practices

xlvii. The Platform should have capability to integrate with various security and IT controls such MS Active Directory, IBM Q-Radar (SIEM), Vulnerability Management (Qualysis), Patch Management, ARCON PAM, BMC ITSM tool, Anti-Virus (Symantec), TrendMicro Deep Security & EDR, MDM Solution, NAC, DLP, DSPM, XSOAR, TIM, Squal1(VAPT Management Tool) relevant tools/application developed in house or procured outside etc. It includes all the tools as applicable as per business needs to meet Information Technology and Cyber Security fulfilment from Governance, Compliance and Risk Management perspective

xlviii. The communication between various components of the Platform & with other integrated systems must use authenticated and encrypted channels.

xlix. The Platform should offer a library of technical baseline configuration procedures mapped to various technologies.

l. The Platform should have capability to use external data by having an API connection or any alternate connection method with the data source. The Platform should also allow the importing the actual data in standard file format, such as csv, xls, etc.

li. The Platform administrative console and user application must be accessible by latest browser across Bank locations

lii. The Platform should maintain the audit trail/logs sufficiently for all user access and all the changes done on it.

liii. The Platform 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.

liv. The Platform should work in high availability module and vendor should provide the Platform within the defined SLA

lv. The Platform should be implemented with latest security hardening standard and comply with security standards such as CIS Benchmark, NIST CSF and OWASP etc.

lvi. The Cyber GRC Platform based solution must be an on-premises and use the existing Bank's virtualization platform for successful deployment and operationalisation.

lvii. The Platform licenses must be provided an access to 100 users with all functionalities in the proposed SOW which can be expanded as per need.

lviii. The Platform must allow the Role based user access and must have nonrepudiation control. Access to the application must be as per role and template configured for the user.

lix. Platform should have the capability to move from one tool to another, to allow that migration will full backup of data along with proper data integrity

lx. The Platform should facilitate that Compliance Management Process requirements can be mapped to a business function.

lxi. The Platform should have capability to record the consequences of non-compliance and adequate dashboards as well as reporting.

lxii. The Platform should be able to calculate compliance scores as per standard, framework, regulation, department, including dynamically defined groups.

lxiii. The Platform should have capability to perform compliance gap analysis.

lxiv. The Platform should provide built in as well as customizable workflows to track, IT Risk issues, Cyber threats, vulnerabilities, VAPT Findings, Audit Findings, Compliance findings, internal/external audits, critical incidents etc. It should support the automation of workflows to the extent possible to meet the GRC goals defined in the scope of work.

lxv. The platform shall have AI support for analysis and recommendations & Integration with Chatbot

lxvi. The solution should have automated risk and compliance workflows to minimize manual effort in assessments and approvals. It should include AI-driven risk prediction capabilities to proactively identify emerging risks.

lxvii. The solution should feature an AI-powered compliance chatbot to provide instant support for policy queries and risk recommendations.

lxviii. Platform should allow for performance evaluation questionnaires to be filled for each audit member as part of the audit closure with appropriate workflow authorization and approval.

lxix. Platform should have capability to onboard Third Party Vendors and do complete end to end life cycle management of Vendor Risks and conduct Vendor Risk Assessments

General Implementation to be carried out by supplier:

For the purpose of implementation, the following points should be noted:

The Cyber GRC Platform, services, all software's and all other associated components would be provided by the successful Bidder. The supplier / service provider should ensure the implementation of Cyber GRC platform with the help of OEM (if applicable).

a) Bidder is responsible of making the OEM support available during the implementation and maintenance.

b) Bank will only provide hardware and OS to host the solution. To make the solution work , software and all other associated components workable shall be under bidder's scope

c) Bidder has to adhere to agreed Service Level Agreements (SLA) and periodic monitoring and reporting requirements of Bank.

d) The licenses should be in the name of J&K Bank or specifically purchased for J&K Bank, where Bank's name shall be mentioned in license copies.

e) The project may be subjected to audit from RBI and/or third party. It shall be responsibility of the Bidder to co-operate and provide necessary information and support to the auditors.

f) In addition to Operations Management of their own solutions, the SI/OEM will be responsible for closure of findings of Security Assessments conducted by Bank or third-party assessor on underlying assets of these solutions.

g) Periodic health check should be carried out by SI/OEM annually to ensure the quality of implementation and operations.

h) Data captured in the solution should not be stored outside the Bank's Infrastructure.

i) No Additional payment apart from the final tender bid value will be processed/released by Bank to the Bidder under any circumstances

Dashboard requirements to be provided by supplier:

a) Cyber GRC platform should provide generic/ personalized dashboard and widgets for users and top management.

b) Dashboards should contain graphical depictions that would reveal, for instance, extent and degree of compliance & risk, potential threats, remedial measures across various activities, tasks, applications etc. It should also contain other crucial information related to Cyber Governance, risk & compliance.

c) There should also be a dedicated consolidated as well individual level dashboard for showing real-time positions, risk and exposure.

Miscellaneous features / support required:

a) Cyber GRC platform should facilitate easy monitoring of various Security applications, tools as defined, and in case of any breach/exceptions, it should invariably prompt an appropriate user. There must also be a dashboard providing dynamic view.

b) Reports pertaining to all the modules in user readable formats (pdf, xlsx, csv, txt, etc.) should be available in the Cyber GRC. While there should be some standardized/scanned reports, the application should also support a fully user configurable / query-based report generation system.

c) Supplier should also specify details of integration carried out with third party systems that are available with the product.

d) The supplier should supply and install all the required Software at Bank site.

e) The supplier should implement complete Platform till Handover Takeover operationalization.

f) The detailed Product Specifications / Bill of Material along with Make, Model number and quantity shall be submitted

g) The successful supplier expected to provide all necessary back-to-back support from OEM for delivery, installation & support till the expiry of contract period.

h) Software licenses effective date shall be effective as on Go-LIVE operational sign off or put in use for Bank operations.

i) The product proposed / supplied by the Bidder shall be compatible with the latest version of Operating System (Windows / Linux).

j) Supplier shall supply only those products, which would not be declared end of life until March 31, 2032. Further, the proposed products should also not go End of Support before March 31, 2032. However, in cases where the OEM decides to phase out any particular model, the vendor is required to substitute (upgrade) the product with another product. The Bidder must inform well in advance about such changes. In case no substitute model is available, the OEM shall give the notice for discontinuation in writing at least one month prior to such discontinuation. In case of software, the vendor shall supply the latest version available at the time of delivery & should meet all the business requirements as is with no extra cost to Bank.

k) Cyber GRC platform should support additional modules as listed (but not limited to) which may be required in future - Exception Management, Threat and Vulnerability Management, Information Security Incident and Change Management, Asset Management, Information Security Risk Management, Cyber Incident, Investigation & Advisory Management.

Support

Support the Cyber GRC Platform including future updates and upgrades of all components of the platform, shall be for a minimum period of 03 year from the date of go live (Extendable for another 2 or more years upon Bank’s discretion)

Project Resources

All the resources provided for design and implementation of the Platform should be OEM certified with relevant 3 Yrs. of GRC context experience on the offered Platform in implementing and supporting the Platform at various other clients in an effective and efficient manner.

Implementation

Bank will provide adequate optimum hardware and operating systems to the bidder. The SI in consultation with the OEM is expected to suggest if the existing hardware is suitable for the Platform proposed with technical justifications and, if not, recommend additional hardware to meet the overall requirements of the Platform. The Bidder is expected to co-ordinate all the activities relating to implementation and operationalisations. In this regard the following points should be noted:

a) The Cyber GRC Platform, one time implementation services, software’s and all other associated components would be required to be provided by the selected Bidder. The Bidder should ensure the adequate customised implementation of Cyber GRC platform with the help of OEM (if applicable).

b) Bidder must adhere to agreed Service Level Agreements (SLA) and periodic monitoring and reporting requirements of Bank.

c) Data captured in the Cyber GRC platform should not be stored outside Bank's Information Systems and computing environment.

d) All the proposed modules shall be implemented suitably as per Bank's custom requirements while meeting global standards and compliance requirements.

e) Bidder shall ensure the Cyber GRC platform deployment in fully HA mode at DC and DR centre in coordination with Bank. It should be fully made functional from Primary DC location along with suitable fault tolerance capability.

Operational Support:

The responsibilities of the selected Bidder include, but not limited to the following:

f) Support for all system and associated components of the Cyber GRC platform.

g) Ensuring that the system is available 24X7X365, resources for monitoring and emergency operation support should be on-boarded immediately on implementation of all modules.

h) The Bidder should provide training and certification to the resources as applicable to ensure seamless operationalisation of the modules.

i) Ensure timely fine tuning of the Cyber GRC platform to enhance the end-user experience.

j) System shall be able to enhance/ integrate the Cyber GRC platform - with new requirements implemented in Bank on ongoing basis with minimal effort.

Maintenance & Support

The Bidder will be responsible to provide maintenance and support services for the period of contract.

It will be the responsibility of Bidder to have strong backing of OEM support to seek extended support in cases wherever required and ensure all issues are addressed within the stipulated timeline as per SLA defined in the RFP. The Bidder will also be responsible to provide and install patches/ updates/ version upgrades of all software including any major or minor releases and fix vulnerabilities identified internally by organisation under their VA/PT procedures.

The activity should be planned as per the decision from Bank and may include weekends and non-business hours. The downtime resulting in such upgrades should not exceed the allowable downtime as mentioned in the RFP.

Training

The selected bidder shall provide the training to the Bank's personnel as described below:

v. The -Bidder should provide training and certification to the resources as applicable.

vi. The training should include the architecture, hardware, software, integration, and customization, policy installation, troubleshooting reporting and other aspects of the Platform. Should support the initial end user training and provide training materials.

vii. The -Bidder shall train Bank's personnel for independent operation, creation of policies/rules, generation of reports, and analysis of the reports, Troubleshooting and familiarization of features and functionalities, policy configuration, alert monitoring, etc. post implementation.

viii. Refresher training - selected Bidder shall conduct more refresher trainings for the Bank's team on yearly basis. The participants of these programs may or may not be same.

Contract Uptime

a) The "**Downtime**" shall mean the time period when the Service/Application is not available as per the service standards of this SLA resulting failure. "**Failure**" is the condition that renders the solution not available to customers. "**Restoration**" is the condition when the Company demonstrates that the solution is in working order and the Bank acknowledges the same. It excludes the scheduled outages planned in advance and when Bank denies access to the Company Engineer for carrying out repair activities.

b) **Percentage down time"** shall mean the aggregate of downtime of the particular system during the quarter expressed as a percentage of total available time in a year i.e. 90 * 24 hours. Thus, if the aggregate downtime of System works out to 2 hours during a year then the percentage downtime shall be calculated as follows:

$$\frac{2 \times 100}{90 \times 24} = 0.09\% \text{ (Considering days in a quarter as 90)}$$

(A quarter is taken as a calendar quarter and number of days are actually number of days in each quarter)

c) **Uptime"**: The Company shall guarantee and ensure the following SLA's are met during the Contract Period of the Hardware/Software/License:

Service Window	24*7
Uptime Commitment	99.99%
Data Availability	100%

The "**Uptime**", for calculation purposes, equals to the Total number of hours of the day in a quarter, less Downtime in number of hours. Any part of hour is treated as full hour.

The percentage uptime is calculated on quarterly basis as follows:

$$\frac{\text{(Total hours in a quarter - downtime hours within the quarter)}}{\text{Total hours in a quarter}} * 100$$

(A quarter is taken as a calendar quarter and number of days are actually number of days in each quarter)

d) **“Response Time”** shall mean the interval from receipt of first information from Bank to the company, or to the local contact person of the Company by way of any means of communication informing them of the malfunction in System/Solution to the time Company Engineer attends the problem.

e) **“Restoration Time”** shall mean the period of time from the problem occurrence to the time in which the service returns to operational status. This may include temporary problem circumvention / workaround and does not necessarily include root cause removal.

f) **“Resolution Time”** shall mean the period of time from the problem occurrence to the time in which the root cause of the problem is removed and a permanent fix has been applied to avoid problem reoccurrence.

i. During Period of contract, Company will maintain the services as per SLAs.

ii. Any bugs and enhancement in services shall be rectified immediately.

iii. Any requirements amendments/modifications required by bank will have to be carried out by the identified Company during the contract.

iv. The maximum response time for a support/complaint from the site shall not exceed time defined, else it will fall under penalty clause.

v. Company shall solve the software problem immediately after reporting of the problem by the Bank to the Company

vi. Any rectification required in the Application Software due to inherent bugs in the System Software/ off-the-shelf software shall also be rectified by the Company, at no additional cost with timelines as defined in the SLA.

The Company shall guarantee an uptime of 99.90% during warranty and also during AMC, which shall be calculated on quarterly basis. The "**Uptime**", for calculation purposes, equals to the Total number of hours of the day in a quarter, less Downtime in number of hours. Any part of hour is treated as full hour.

Service Management

Uptime:

The company shall ensure the following SLA’s are met during the service life of the Application procured:

Uptime of the solution	99.90%

a) **“Uptime”** of the solution/each component shall be calculated using a standard formula as:

Uptime %age of the Solution = (X-Y)/X where X is the number of Hours within the quarter, Y is the downtime Hours.

b) **“Percentage down time”** shall mean the aggregate of downtime of the particular system during the quarter expressed as a percentage of total available time in a quarter i.e. 90 * 24 hours. Thus, if the aggregate downtime of System works out to 2 hours during a quarter then the percentage downtime shall be calculated as follows:

(2 x 100)/ (90 x 24) =0.09%

c) **“Response Time”** shall mean the interval from receipt of first information from Bank to the company, or to the local contact person of the Company by way of any means of communication informing them of the malfunction in System/Solution to the time Company Engineer attends the problem.

d) **“Restoration Time”** shall mean the period of time from the problem occurrence to the time in which the service returns to operational status. This may include temporary problem circumvention / workaround and does not necessarily include root cause removal.

e) **“Resolution Time”** shall mean the period of time from the problem occurrence to the time in which the root cause of the problem is removed and a permanent fix has been applied to avoid problem reoccurrence.

f) **“Down Time”** shall mean the period when the Application is not available due to the problem in it and shall be the interval between the times of reporting of failure to the time of completion of repair. Down Time is the sum of response time and restoration time with the following exclusions:

Period when Bank denies access to the Company Engineer for carrying out repair activities.

Penalties shall be imposed in case of total uptime of Setup/Solution during the Contract period is less than the committed uptime. For every drop of 0.05 % than committed Uptime, warranty for the entire project shall be extended for 1 month. However, if the downtime percentage exceeds 2 % or if the number of downtime occurrences is more than 8 per year, the Bank shall be within its rights to invoke the Performance Bank Guarantee submitted by the Company in regards to the supply and maintenance etc. of the solution without any notice.

Service Levels:
This SLA document provides for minimum level of services required as per contractual obligations based on performance indicators and measurements thereof. The Company shall ensure provisioning

of all required services while monitoring the performance of the same to effectively comply with the performance levels. The services provided by the Company shall be reviewed by Bank that shall:

- Regularly check performance of the Company against this SLA.
- Discuss escalated problems, new issues and matters still outstanding for resolution.
- Review of statistics related to rectification of outstanding faults and agreed changes.
- Obtain suggestions for changes to improve the service levels.

Non-Availability: Is defined as, the service(s) is not-available as per levels below.

a. **Severity Level 1:** Is defined as, the Service is not available or there is a major degradation in performance of the system.

b. **Severity Level 2:** Is defined as, the service is available but the performance is degraded or there are intermittent failures and there is an urgent need to fix the problem to restore the service

c. **Severity Level 3:** Is defined as, the moderate degradation in the application performance. Has no impact on the normal operations/day-to-day working.

The violation of any of the above SLA's will attract a penalty as set out in the table below:

Severity Level	**Response**	**Restoration**	**Resolution**
Severity-1	02 hrs.	04 hrs.	02 day
Severity-2	4 hrs.	06 hrs.	03 days
Severity-3	8 hrs.	24 hrs.	07 days

Penalties for Non-Compliance to Restoration and Resolution Time:

Severity Level	**Restoration Breach**	**Resolution Breach**
Severity-1	15 days of Warranty period Cost for every 4 hrs. of delay in restoration	15 days of Warranty period Cost for every 1 day of delay in resolution
Severity-2	10 days of Warranty period Cost for every 12hrs of delay in restoration	10 days of Warranty period Cost for every 2 days of delay in resolution

Severity-3	5 days of Warranty period Cost for every 24 days delay in restoration	5 days of Warranty period Cost for every 3 days of delay in resolution

Penalties shall be imposed in case of total uptime of Setup/Solution during the Contract period is less than the committed uptime. During the warranty period, for every drop of 0.05 % than committed Uptime, warranty for the entire project shall be extended for 1 month. However, if the downtime percentage exceeds 2% or if the number of downtime occurrences is more than 8 per year, the Bank shall be within its rights to invoke the Performance Bank Guarantee submitted by the Company in regards to the supply and maintenance etc. of the solution without any notice.

Penalties shall also be applicable if the technical declines from the service provider are more than the threshold/ acceptable level of 2%.

Technical declines	Penalty/Quarter
2%	NA
2-3%	2% of the project Cost/Quarter
4-5%	3% of the project Cost/Quarter
5-8%	5% of the project Cost/Quarter
8-10%	10% of the project Cost/Quarter

Delivery:

Without prejudice to the rights of Bank to terminate this agreement/ the related purchase order, in case of the failure to deliver and /or install the solution within the stipulated timelines, penalty shall be levied for every 01-week delay at the rate of 2% of the order value (in which delay has occurred) up to a maximum of 05 weeks from the original date committed by the Company. The bank may in its sole discretion and without being bound to do so extend the date of delivery. In the event of the Bank agrees to extend the date of delivery at the request of the Company, it is a condition precedent that the validity of the Performance Bank Guarantee submitted by the Company in regard to the supply and maintenance etc. of the solution shall be extended by further period as required by the Bank before the expiry of the original Bank Guarantee. Failure to do so will be treated as breach of contract.

Any component has not been delivered or if delivered is not operational, will be deemed / treated as non-delivery thereby excluding the Bank from all payment obligations under the terms of this contract. Partial delivery of products is not acceptable and payment for such products will not be made until full delivery is completed.

Contract Period

The tenure of the Contract will be for a period of 3 years, effective from the date of successful go live unless or until terminated by Bank in accordance with the terms of this SLA, which may be extended for a further period of 2 year term at the same rate and same terms & conditions, provided services of the bidder is satisfactory and both parties agreeing to do so. Thereafter the contract may further extended if both parties wish to continue on the mutually agreed terms and conditions.

Exit Clause

The Bank reserves the right to cancel the contract in the event of happening one or more of the following conditions:

a) Failure of the successful bidder to accept the contract and furnish the Performance Bank Guarantee within 15 days from receipt of purchase contract.

b) Delay in delivery beyond the specified period.

c) Delay in completing implementation/customization and acceptance tests/ checks beyond the specified periods;

d) Serious discrepancy in functionality to be provided or the performance levels which have an impact on the functioning of the solution.

e) In addition to the cancellation of contract, Bank reserves the right to appropriate the damages through encashment of Bid Security /Performance Guarantee given by the Bidder. Bank reserves right to exit at any time after giving notice period of one month during the contract period.

Payment Terms

The Company must accept the payment terms proposed by the Bank as proposed in this section. Payment shall be made in Indian Rupees.

The Company's requests for payment shall be made to the Bank in writing accompanied by Original Invoice detailing the systems, software delivered, installed and accepted by the bank.

The payments shall be made after deducting applicable TDS within xx Working days from the date of receipt of valid claims that are supported by original invoice, original Proof of Delivery (POD), acceptance by the bank and upon fulfilment of other conditions stipulated in the contract. The invoices and other documents are to be duly authenticated by Company. The Company therefore has to furnish the bank account number to where the funds have to be transferred for effecting payments.

Payments as per the schedule given below will be released only on acceptance of the order and on signing the SLA / NDA by the selected Company.

The Bidder must accept the payment terms proposed by the Bank as proposed in this section.
The Payments shall be made on the achievement of the following project milestones:

Sr. #	Project Milestones	Payment Terms
01	Current State Assessment & Documentation.	10% of First year License cost
02	Delivery and installation of GRC software components / supporting licenses. Use cases development, testing, integration, Implementation and Operationalisation.	30% of First year License cost
03	Go-Live Planning, End User and Administrative Training, Sufficient and Signoff requirements	60% of First year License cost. [2 months after go-Live]
04	Year 2 & 3 license	Yearly in advance.
05	Annual Maintenance Support Services	Yearly in advance
06	Training	100% training cost on completion of training program

Payment terms: -

e) Rates to be quoted exclusive of GST.

f) Invoices to be raised after submission of PBG & execution of SLA and NDA with the Bank.

g) Payments will be done rendering of services on production of invoices and confirmation from J&K Bank.

h) All other terms and conditions as per RFP.

The Bidder must accept the payment terms proposed by the Bank as proposed in this section.

Payments shall be released on acceptance of the purchase order and:

d) Post Signing of Service Level Agreement (SLA) between Bank and Selected bidder.

e) Post Signing of Non-Disclosure Agreement (NDA) between Bank and Selected bidder.

f) All taxes, if any, applicable shall be deducted at source as per current rate while making any payment.

Assignment

The Company shall not assign, in whole or in part, the benefits or obligations of the contract to any other person without the prior written consent of the Bank. However, the Bank may assign any of its rights and obligations under the Contract to any of its affiliates without prior consent of the Company.

Entire Agreement, Amendments, Waivers.

i. This Master Agreement and each Service Attachment contains the sole and entire agreement of the parties with respect to the entire subject matter hereof, and supersede any and all prior oral or written agreements, discussions, negotiations, commitment, understanding , marketing brochures, and sales correspondence and relating thereto. In entering into this Master Agreement and each Service Attachment each party acknowledges and agrees that it has not relied on any express or implied representation, or other assurance (whether negligently or innocently made), out in this Master Agreement and each Service Attachment. Each party waives all rights and remedies which, but for

ii. this Section, might otherwise be available to it in respect of any such representation (whether negligently or innocently made), warranty, collateral contract or other assurance.

iii. Neither this Master Agreement nor any Service Attachment may be modified or amended except in writing and signed by the parties.

iv. No waiver of any provisions of this Master Agreement or any Service Attachment and no consent to any default under this Master Agreement or any Service Attachment shall be effective unless the same shall be in writing and signed by or on behalf of the party against whom such waiver or consent is claimed. No course of dealing or failure of any party to strictly enforce any term, right or condition of this Master Agreement or any Service Attachment shall be construed as a waiver of such term, right or condition. Waiver by either party of any default other party shall not be deemed a waiver of any other default.

Severability

If any or more of the provisions contained herein shall for any reason be held to be unenforceable in any respect under law, such unenforceability shall not affect any other provision of this Master Agreement, but this Master Agreement shall be construed as if such unenforceable provisions or provisions had never been contained herein, provided that the removal of such offending term or provision does not materially alter the burdens or benefits of the parties under this Master Agreement or any Service Attachment.

Remedies Cumulative

Unless otherwise provided for under this Master Agreement or any Service Attachment, all rights of termination or cancellation, or other remedies set forth in this Master Agreement, are cumulative and are not intended to be exclusive of other remedies to which the injured party may be entitled by law or equity in case of any breach or threatened breach by the other party of any provision in this Master Agreement. Use of one or more remedies shall not bar use of any other remedy for the purpose of enforcing any provision of this Master Agreement.

Partnership / Collaboration / Subcontracting

The services offered to be undertaken in response to this RFP shall be undertaken to be provided by the company directly and there shall not be any sub-contracting without prior written consent from the Bank. Bank will only discuss the solution with company's authorized representatives. The company authorized representatives shall mean their staff. In no circumstances any intermediary (which includes Liasoning Agents, marketing agents, commission agents etc.) should be involved during the course of project. No subletting of the contract by the will be allowed under any circumstances. Neither the subject matter of the contract nor any right arising out of the contract shall be transferred, assigned or delegated to any third party by Vendor without prior written consent of the Bank

Confidentiality

All the Bank's product and process details, documents, data, applications, software, systems, papers, statements and business/customer information etc. (hereinafter referred to as 'Confidential Information') which may be communicated to or come to the knowledge of the Company and /or its employees during the course of discharging their obligations shall be treated as absolutely confidential and the Company and its employees shall keep the same secret and confidential and not disclose the same, in whole or in part to any third party nor shall use or allow to be used any information other than as may be necessary for the due performance by the Company of its obligations. The Company shall indemnify and keep Bank indemnified safe and harmless at all times against all or any consequences arising out of any breach of this undertaking regarding Confidential Information by the Company and/or its employees and shall immediately reimburse and pay to the Bank on demand all damages, loss, cost, expenses or any charges that Bank may sustain suffer, incur or pay in connection therewith.

It is clarified that "Confidential Information" includes any and all information that is or has been received by the Company (Receiving Party) from the Bank (Disclosing Party) and that (a) relates to the Disclosing Party and (b) is designated by the Disclosing Party as being confidential or is disclosed in circumstances where the Receiving Party would reasonably understand that the disclosed information would be confidential (c) is prepared or performed by or on behalf of the Disclosing Party by its employees, officers, directors, agent, representatives or consultants.

In maintaining confidentiality, the Receiving Party on receiving the confidential information and material agrees and warrants that it shall take at least the same degree of care in safeguarding such confidential information and materials as it takes for its own confidential information of like importance and such degree of care shall be at least, that which is reasonably calculated to prevent any inadvertent disclosure. The Receiving Party shall also, keep the confidential information and confidential materials and any copies thereof secure and in such a way so as to prevent unauthorized access by any third Party.

The Receiving Party, who receives the confidential information and the materials, agrees that on receipt of a written demand from the Disclosing Party, they will immediately return all written confidential information and materials and all copies thereof provided to and which is in Receiving Party's possession or under its custody and control.

The Receiving Party to the extent practicable shall immediately destroy all analysis, compilation, notes studies memoranda or other documents prepared by it which contain, reflect or are derived from confidential information relating to the Disclosing Party AND shall also immediately expunge any confidential information, word processor or other device in its possession or under its custody & control, where after it shall furnish a Certificate signed by the Authorized person confirming that to the best of his/her knowledge, information and belief, having made all proper enquiries, the requirement of confidentiality aspect has been complied with.

The restrictions mentioned hereinabove shall not apply to:-

a) any information that publicly available at the time of its disclosure; or any information which is independently developed by the Receiving Party or acquired from a third party to the extent it is acquired with the valid right to disclose the same; or

b) any disclosure required by law or by any court of competent jurisdiction, the rules and regulations of any recognized stock exchange or any enquiry or investigation by any government, statutory or regulatory body which is lawfully entitled to require any such disclosure provided that, so far as it is lawful and practical to do so prior to such disclosures the Receiving Party shall promptly notify the Disclosing Party of such requirement with a view to providing the Disclosing Party an opportunity to obtain a protective order or to contest the disclosure or otherwise agree to the timing and content of such disclosure.

The confidential information and material and all copies thereof, in whatsoever form shall at all the times remain the property of the Disclosing Party and disclosure hereunder shall not confer on the Receiving Party any rights whatsoever beyond those contained in this document. The confidentiality obligations shall be observed by the Company during the term of this Agreement and thereafter and shall survive the expiry or termination of this Agreement between the Bank and Company.

The Company understands and agrees that any use or dissemination of information in violation of this Confidentiality Clause will cause BANK irreparable harm, may leave BANK with no adequate remedy at law and as such the Bank is entitled to proper indemnification for the loss caused by the Company. Further the BANK is entitled to seek to injunctive relief besides other remedies available to it under law and this Agreement.

Information Security:

a. The Successful Bidder and its personnel shall not carry any written material, layout, diagrams, hard disk, flash / pen drives, storage tapes or any other media out of J&K Bank's premises without written permission from J&K Bank.

b. The Successful Bidder's personnel shall follow J&K Bank's information security policy and instructions in this regard.

c. The Successful Bidder acknowledges that J&K Bank 's business data and other proprietary information or materials, whether developed by J&K Bank or being used by J&K Bank pursuant to a license agreement with a third party (the foregoing collectively referred to herein as "proprietary information") are confidential and proprietary to J&K Bank; and the Successful Bidder agrees to use reasonable care to safeguard the proprietary information and to prevent the unauthorized use or disclosure thereof, which care shall not be less than that used by Successful Bidder to protect its own proprietary information. Successful Bidder recognizes that the goodwill of J&K Bank depends, among other things, upon the Successful Bidder keeping such proprietary information confidential and that unauthorized disclosure of the same by Successful Bidder could damage J&K Bank. By reason of Successful Bidder's duties and obligations hereunder, Successful Bidder may come into possession of such proprietary information, even though the Successful Bidder does not take any direct part in or furnish the Service(s) performed for the creation of said proprietary information and shall limit access thereto to employees with a need to such access to perform the Services required by the Contract/Agreement. Successful Bidder shall use such information only for the purpose of performing the Service(s) under the Contract/Agreement.

d. Successful Bidder shall, upon termination of the Contract/Agreement for any reason, or upon demand by J&K Bank, whichever is earliest, return any and all information provided to Successful Bidder by J&K Bank, including any copies or reproductions, both hardcopy and electronic.

e. That the Successful Bidder and each of its subsidiaries have taken all technical and organizational measures necessary to protect the information technology systems and Data used in connection with the operation of the Successful Bidder's and its subsidiaries' businesses. Without limiting the foregoing, the Successful Bidder and its subsidiaries have used reasonable efforts to establish and maintain, and have established, maintained, implemented and complied with, reasonable information technology, information security, cyber security and data protection controls, policies and procedures, including oversight, access controls, encryption, technological and physical safeguards and business continuity/disaster recovery and security plans that are designed to protect against and prevent breach, destruction, loss, unauthorized distribution, use, access, disablement, misappropriation or modification, or other compromise or misuse of or relating to any information technology system or Data used in connection with the operation of the Successful Bidder's and its subsidiaries' businesses.

f. The Successful Bidder shall certify that to the knowledge of the Successful Bidder, there has been no security breach or other compromise of or relating to any information technology and computer systems, networks, hardware, software, data, or equipment owned by the Successful Bidder or its subsidiaries or of any data of the Successful Bidder's, the Operating Partnership's or the Subsidiaries' respective customers, employees, suppliers, vendors that they maintain or that, to their knowledge, any third party maintains on their behalf (collectively, "IT Systems and Data") that had, or would reasonably be expected to have had, individually or in the aggregate, a Material Adverse Effect, and

g. That the Successful Bidder has not been notified of, and has no knowledge of any event or condition that would reasonably be expected to result in, any security breach or other compromise to its IT Systems and Data;

h. That the Successful Bidder is presently in compliance with all applicable laws, statutes, rules or regulations relating to the privacy and security of IT Systems and Data and to the protection of such IT Systems and Data from unauthorized use, access, misappropriation or modification. Besides the Successful Bidder confirms the compliance with Banks Supplier Security Policy.

i. That the Successful Bidder has implemented backup and disaster recovery technology consistent with generally accepted industry standards and practices.

j. That the Successful Bidder and its subsidiaries IT Assets and equipment, computers, Systems, Software's, Networks, hardware, websites, applications and Databases (Collectively called IT systems) are adequate for, and operate and perform in all material respects as required in connection with the operation of business of the Successful Bidder and its subsidiaries as currently conducted, free and clear of all material bugs, errors, defects, Trojan horses, time bombs, malware and other corruptants.

k. That the Successful Bidder shall be responsible for establishing and maintaining an information security program that is designed to:

l. Ensure the security and confidentiality of Customer Data, Protect against any anticipated threats or hazards to the security or integrity of Customer Data, and

m. That the Successful Bidder will notify Customer of breaches in Successful Bidder's security that materially affect Customer or Customer's customers. Either party may change its security procedures from time to time as commercially reasonable to address operations risks and concerns in compliance with the requirements of this section.

n. The Successful Bidder shall establish, employ and at all times maintain physical, technical and administrative security safeguards and procedures sufficient to prevent any unauthorized processing of Personal Data and/or use, access, copying, exhibition, transmission or removal of Bank's Confidential Information from Companies facilities. Successful Bidder shall promptly provide Bank with written descriptions of such procedures and policies upon request. Bank shall have the right, upon reasonable prior written notice to Successful Bidder and during normal business hours, to conduct on-site security audits or otherwise inspect Companies facilities to confirm compliance with such security requirements.

o. That Successful Bidder shall establish and maintain environmental, safety and facility procedures, data security procedures and other safeguards against the destruction, corruption, loss or alteration of the Client Data, and to prevent access, intrusion, alteration or other interference by any unauthorized third parties of the same, that are no less rigorous than those maintained by Successful Bidder for its own information or the information of its customers of a similar nature.

p. That the Successful Bidder shall perform, at its own expense, a security audit no less frequently than annually. This audit shall test the compliance with the agreed-upon security standards and procedures. If the audit shows any matter that may adversely affect Bank, Successful Bidder shall disclose such matter to Bank and provide a detailed plan to remedy such matter. If the audit does not show any matter that may adversely affect Bank, Bidder shall provide the audit or a reasonable summary thereof to Bank. Any such summary may be limited to the extent necessary to avoid a breach of Successful Bidder’s security by virtue of providing such summary.

q. That Bank may use a third party or its own internal staff for an independent audit or to monitor the Successful Bidder’s audit. If Bank chooses to conduct its own security audit, such audit shall be at its own expense. Successful Bidder shall promptly correct any deficiency found in a security audit.

r. That after providing 30 days prior notice to Successful Bidder, Bank shall have the right to conduct a security audit during normal business hours to ensure compliance with the foregoing security provisions no more frequently than once per year. Notwithstanding the foregoing, if Bank has a good faith belief that there may have been a material breach of the agreed security protections, Bank shall meet with Successful Bidder to discuss the perceived breach and attempt to resolve the matter as soon as reasonably possible. If the matter cannot be resolved within a thirty (30) day period, the parties may initiate an audit to be conducted and completed within thirty (30) days thereafter. A report of the audit findings shall be issued within such thirty (30) day period, or as soon thereafter as is practicable. Such audit shall be conducted by Successful Bidder's auditors, or the successors to their role in the event of a corporate reorganization, at Successful Bidder’s cost.

s. Successful Bidders are liable for not meeting the security standards or desired security aspects of all the ICT resources as per Bank’s IT/Information Security / Cyber Security Policy. The IT /Information Security/ Cyber Security Policy will be shared with successful Bidder. Successful Bidders should ensure Data Security and protection of facilities/application managed by them.

t. The deputed persons should aware about Bank’s IT/IS/Cyber security policy and have to maintain the utmost secrecy & confidentiality of the bank’s data including process performed at the Bank premises. At any time, if it comes to the notice of the bank that data has been compromised / disclosed/ misused/misappropriated then bank would take suitable action as deemed fit and selected vendor would be required to compensate the bank to the fullest extent of loss incurred by the bank. Besides bank will be at liberty to blacklist the bidder and take appropriate legal action against bidder.

u. The Bank shall evaluate, assess, approve, review, control and monitor the risks and materiality of vendor/outsourcing activities and Successful Bidder shall ensure to support baseline system security configuration standards. The Bank shall also conduct effective due diligence, oversight and management of third party vendors/service providers & partners.

v. Vendor criticality assessment shall be conducted for all partners & vendors. Appropriate management and assurance on security risks in outsources and partner arrangements shall be ensured.

Termination of Contract

If the Termination is on account of failure of the Successful Bidder to perform the obligations under this agreement, the Bank shall have the right to invoke the Performance Bank Guarantee(s) given by the selected bidder. The Bank will be entitled to terminate this Contract, on the happening of any one or more of the following:

For Convenience: BANK by written notice sent to the Company may terminate the contract in whole or in part at any time for its convenience giving xx days prior notice.

In the event of termination of the Agreement for the Bank’s convenience, Service Provider shall be entitled to receive payment for the Services rendered (delivered) up to the effective date of termination.

For Insolvency: BANK may at any time terminate the contract by giving written notice to the Company, if the Company becomes bankrupt or insolvent.

For Non-performance: BANK shall have the right to terminate this agreement or/and to cancel the entire or unexecuted part of the related Purchase Order forthwith by a written notice in the event the company fails to deliver and/or install the solution within the stipulated time schedule or any extension, if any, thereof agreed by the Bank in writing in its sole discretion OR the Company fails to maintain the service levels prescribed by BANK in scope of work OR fails to discharge or commits breach of any of its obligations under this Agreement.

In the event of termination, the company shall compensate the Bank to the extent of loss suffered by the Bank on account of such termination provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to BANK. The Bank shall inter-alia have a right to invoke the Performance Bank Guarantee submitted by the Company in regard to the supply and maintenance etc. of the solution for realizing the payments due to it under this agreement including penalties, losses etc.

Exit Clause

The Bank reserves the right to cancel the contract in the event of happening one or more of the following conditions:

a) Failure of the successful bidder to accept the contract and furnish the Performance Bank Guarantee within 15 days from receipt of purchase contract.

b) Delay in delivery beyond the specified period.

c) Delay in completing implementation/customization and acceptance tests/ checks beyond the specified periods;

d) Serious discrepancy in functionality to be provided or the performance levels which have an impact on the functioning of the solution.

e) In addition to the cancellation of contract, Bank reserves the right to appropriate the damages through encashment of Bid Security /Performance Guarantee given by the Bidder. Bank reserves right to exit at any time after giving notice period of one month during the contract period.

Indemnity

The Successful bidder shall indemnify and hold the Bank harmless from and against all claims, losses, costs, damages, expenses, action suits and other proceedings (including attorney fees), relating to or resulting from:-

i. Intellectual Property infringement or misappropriation of any third party trade secrets or infringement of any patent, trademarks, copyrights etc. or such other statutory infringements in respect of all components provided to fulfil the scope of this project.

ii. Claims made by the employees who are deployed by the Successful bidder.

iii. Breach of confidentiality obligations by the Successful bidder,

iv. Negligence (including but not limited to any acts or omissions of the Successful bidder, its officers, principals or employees) or misconduct attributable to the Successful bidder or any of the employees deployed for the purpose of any or all of the its obligations,

v. Any loss or damage arising out of loss of data;

vi. Bonafide use of deliverables and or services provided by the successful bidder;

vii. Non-compliance by the Successful bidder with applicable Laws/Governmental/Regulatory Requirements.

The Successful bidder shall be responsible for any loss of data, loss of life etc. due to acts of its representatives, and not just arising out of negligence or misconduct, as such liabilities pose significant risk.

It is hereby agreed that the above said indemnity obligations shall apply notwithstanding anything to the contrary contained in this Tender document and subsequent Agreement and shall survive the termination of the agreement for any reason whatsoever. The Successful bidder will have sole control of its defense and all related settlement negotiations

Right to Audit

Bank reserves the right to conduct an audit/ ongoing audit of the services provided by Bidder.

The Selected Bidder (Service Provider) shall be subject to annual audit by internal/ external Auditors appointed by the Bank/ inspecting official from the Reserve Bank of India or any regulatory authority, covering the risk parameters finalized by the Bank/ such auditors in the areas of products (IT hardware/ Software) and services etc. provided to the Bank and Service Provider is required to submit such certification by such Auditors to the Bank.

Bidder should allow the J&K Bank or persons authorized by it to access Bank documents, records or transactions or any other information given to, stored or processed by Bidder within a reasonable time failing which Bidder will be liable to pay any charges/ penalty levied by the Bank without prejudice to the other rights of the Bank. Bidder should allow the J&K Bank to conduct audits or inspection of its Books and account with regard to Bank's documents by one or more officials or employees or other persons duly authorized by the Bank.

Limitation of Liability

Neither Party shall be liable for any indirect damages (including, without limitation, loss of revenue, profits, and business) under this agreement and the aggregate liability of Company, under this agreement shall not exceed more than the total contract value.

Relocation and Shifting

The relocation / Shifting, if any required, of all the quoted components shall be done by the Bank at its own cost and responsibility. However the Company shall supervise the de-installation and packing at the original site and re-installation at the new sites free of cost. The quoted components shall continue to remain within the scope of warranty for the transit period.

Force Majeure

i. The Selected Company shall not be liable for forfeiture of its performance security, Liquidated damages or termination for default, if any to the extent that its delay in performance or other failure to perform its obligations under the contract is the result of an event of Force Majeure.

ii. For purposes of this Clause, "Force Majeure" means an event explicitly beyond the reasonable control of the Contractor and not involving the contractors fault or negligence and not foreseeable. Such events may be due to or as a result of or caused by act of God, wars, insurrections, riots, earth quake and fire, revolutions, civil commotion, floods, epidemics, pandemics, quarantine restrictions, trade embargos, declared general strikes in relevant industries, satellite failure, act of Govt. of India, events not foreseeable but does not include any fault or negligence or carelessness on the part of the parties, resulting in such a situation. In the event of any such intervening Force Majeure, either party shall notify the other in writing of such circumstances or the cause thereof immediately within five calendar days.

iii. Unless otherwise directed by the Bank in writing, the selected contractor shall continue to perform its obligations under the Contract as far as is reasonably practical, and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.

iv. In such a case the time for performance shall be extended by a period(s) not less than duration of such delay. If the duration of delay continues beyond a period of three months, the Bank and the contractor shall hold consultations in an endeavor to find a solution to the problem.

v. Notwithstanding above, the decision of the Bank shall be final and binding on the successful Company regarding termination of contract or otherwise

Intellectual Property Rights

1.1 For any technology / software / product used by Company for performing Services for the Bank as part of this Agreement, Company shall have right to use as well as right to license such technology/ software / product. The Bank shall not be liable for any license or IPR violation on the part of Company.

1.2 Without the Bank’s prior written approval, Company will not, in performing the Services, use or incorporate link to or call or depend in any way upon, any software or other intellectual property that is subject to an Open Source or Copy left license or any other agreement that may give rise to any third-party claims or to limit the Bank’s rights under this Agreement.

1.3 Company shall, at its own expenses without any limitation, indemnify and keep fully and effectively indemnified the Bank against all costs, claims, damages, demands, expenses and liabilities whatsoever nature arising out of or in connection with all claims of infringement of Intellectual Property Right, including patent, trademark, copyright, trade secret or industrial design rights of any third party arising from the Services or use of the technology / software / products or any part thereof in India or abroad.

1.4 The Bank will give (a) notice to Company of any such claim without delay/provide reasonable assistance to Company in disposing of the claim; (b) sole authority to defend and settle such claim and; (c) will at no time admit to any liability for or express any intent to settle the claim provided that (i) Company shall not partially settle any such claim without the written consent of the Bank, unless such settlement releases the Bank fully from such claim, (ii) Company shall promptly provide the Bank with copies of all pleadings or similar documents relating to any such claim, (iii) Company shall consult with the Bank with respect to the defence and settlement of any such claim, and (iv) in any litigation to which the Bank is also a party, the Bank shall be entitled to be separately represented at its own expenses by counsel of its own selection.

1.5 Company shall have no obligations with respect to any infringement claims to the extent that the infringement claim arises or results from: (i) Company's compliance with the Bank's specific technical designs or instructions (except where Company knew or should have known that such compliance was likely to result in an Infringement Claim and Company did not inform the Bank of the same); or (ii) any unauthorized modification or alteration of the deliverable (if any) by the Bank.

Corrupt and Fraudulent practice.

i. It is required that Company observe the highest standard of ethics during the procurement and execution of such contracts and not to indulge in any corrupt and fraudulent practice.

ii. "Corrupt Practice" means the offering, giving, receiving or soliciting of anything of value to influence the action of an official in the procurement process or in contract execution.

iii. "Fraudulent Practice" means a misrepresentation of facts in order to influence a procurement process or the execution of contract to the detriment of the Bank and includes collusive practice among bidders (prior to or after bid submission) designed to establish bid prices at artificial non-competitive levels and to deprive the Bank of the benefits of free and open competition.

iv. The Bank reserves the right to reject a proposal for award if it determines that the Company recommended for award has engaged in corrupt or fraudulent practices in competing for the contract in question.

v. The Bank reserves the right to declare a bidder ineligible, either indefinitely or for a stated period of time, to be awarded a contract if at any time it becomes known that the firm has engaged in corrupt or fraudulent practices in competing for or in executing the contract.

Governing Laws and Dispute Resolution

This agreement shall be governed in accordance with the Laws of UT of J&K read with laws of India so far as they are applicable to the UT of J&K for the time being and will be subject to the exclusive jurisdiction of Courts at Srinagar with exclusion of all other Courts.

The Bank and the Company shall make every effort to resolve any disagreement or dispute amicably, arising in connection with the Contract, by direct and informal negotiation between the designated Officer of the Bank for **Supply, Implementation and Support Services for Cyber Governance, Risk and Compliance Platform** and designated representative of the Company. If designated Officer of the Bank and representative of the company are unable to resolve the dispute within reasonable period, which in any case shall not exceed____________ they shall immediately escalate the dispute to the senior authorized personnel designated by the Bank and the Company respectively. If even after elapse of reasonable period, which in any case shall not exceed ___________, the senior authorized personnel designated by the Bank and the Company are unable to resolve the dispute amicably OR any party fails to designate its officer/representative/ senior authorized personnel within days from the date of request in writing for the same by the other party for amicable settlement of dispute, the dispute shall be referred to arbitration.

All disputes/differences which may arise between the parties shall be resolved mutual and amicable settlement between the parties within 30 days from the date of receipt of a written notice raising such dispute by either of the party. In case there is no amicable settlement between the parties, the dispute or difference arising in relation to meaning or interpretation of terms and conditions, the same shall be referred to a sole arbitrator to be appointed by Bank. The Arbitration and Conciliation Act, 1996 will be applicable to the arbitration proceeding and the venue of the arbitration shall be at Srinagar. The language of the arbitration proceedings shall be in English. The award of the arbitrator shall be final and binding. The courts at Srinagar shall have exclusive jurisdiction at Srinagar.

Notices

Unless otherwise provided herein, all notices or other communications under or in connection with this Agreement shall be given in writing and may be sent by personal delivery or by post or courier or facsimile or e- mail to the address below, and shall be deemed to be effective if sent by personal delivery, when delivered, if sent by post, three days after being deposited in the post and if sent by courier, two days after being deposited with the courier, and if sent by facsimile, when sent (on receipt of a confirmation to the correct facsimile number) and if sent by e-mail (on receipt of a confirmation to the correct email)

Following shall be address of BANK for notice purpose:

Chief Information Security Officer

Information Security Department

The Jammu & Kashmir Bank M.A. Road, Srinagar,

190 001 J&K.

Following shall be address of Company for notice purpose:

____

____

____

____

Other Terms and Conditions

i. If any provision of this agreement or any document, if any, delivered in connection with this agreement is partially or completely invalid or unenforceable in any jurisdiction, then that provision shall be ineffective in that jurisdiction to the extent of its invalidity or unenforceability. However, the invalidity or unenforceability of such provision shall not affect the validity or enforceability of any other provision of this agreement, all of which shall be construed and enforced as if such invalid or unenforceable provision was/were omitted, nor shall the invalidity or unenforceability of that provision in one jurisdiction affect its validity or enforceability in any other jurisdiction. The invalid or unenforceable provision will be replaced in writing by a mutually acceptable provision, which being valid and enforceable comes closest to the intention of the Parties underlying the invalid or unenforceable provision.

ii. Bank reserves the right to conduct an audit/ ongoing audit of the services provided by Company. The Company agrees and undertakes to allow the Bank or persons authorized by it to access Bank documents, records or transactions or any other information given to, stored or processed by the Company within a reasonable time failing which Bidder will be liable to pay any charges/ penalty levied by the Bank without prejudice to the other rights of the Bank. The Company shall allow the Bank to conduct audits or inspection of its Books and account with regard to Bank's documents by one or more officials or employees or other persons duly authorized by the Bank.

iii. The company, either by itself or through its group companies or Associates, shall not use the name and/or trademark/logo of Bank, in any sales or marketing publication or advertisement, or in any other manner.

iv. Any addition, alteration, amendment, of this Agreement shall be in writing, signed by both the parties.

v. The invalidity or unenforceability for any reason of any covenant of this Agreement shall not prejudice or affect the validity or enforceability of its other covenants. The invalid or unenforceable provision will be replaced by a mutually acceptable provision, which being valid and enforceable comes closest to the intention and economic positions of the Parties underlying the invalid or unenforceable provision.

vi. Each party warrants that it has full power and authority to enter into and perform this Agreement, the respective executants are duly empowered and/or authorized to execute this Agreement, and performance of this Agreement will not result in breach of any provision of the Memorandum and Articles of Association or equivalent constitutional documents of the either party or any breach of any order, judgment or agreement by which the party is bound.

In witness whereof the parties have set their hands on this agreement in duplicate through their authorized signatories on the day, month and year first herein above mentioned.

Agreed and signed on behalf of

Company's Authorized Signatory

Name……………………………
Designation…………………..
Place……………………………
Date……………………………..

Witness (1):

Name……………………………
Designation…………………..
Place……………………………
Date……………………………..

Witness (2):

Agreed and signed on behalf of

J&K Bank Limited

Name……………………………
Designation…………………..
Place……………………………
Date ……………………………

Witness (1):

Name……………………………
Designation…………………..
Place……………………………
Date ……………………………

Witness (2):

Name...................................
Designation........................
Place...................................
Date......................................

Name...................................
Designation........................
Place...................................
Date ....

Annexure M: Manufacturer’s Authorisation Form (MAF)

(To be filled for hardware/ application software / system software/ RDBMS/ any other suites, whatsoever applicable separately)

To,

CISO

Information Security Department

CHQ, J&K Bank.

Srinagar.

Dear Sir,

We ____ who are established and reputed manufacturer /developer of _____________________________ having organization at_________ and __________ do hereby authorize M/s ___________________________ (Name and address of Agent/Dealer) to offer their quotation, negotiate and conclude the contract with you against the above RFP with reference number RFP: _____ _______________ dated ____________ 2025.

We hereby extend our full guarantee and warranty for the following software's / products offered by the above firm in response to J&K Bank's RFP/ tender and contract for supply, installation,commissioning, services and support for Products & Services as specified in tender / RFP as per the terms and conditions set out in the document for the purpose.

1. ____

2. ____

3. ____

4. ____

We duly authorise the said firm to act on our behalf in fulfilling all installations, technical support and maintenance obligations required by the contract.

(*Please mention the names of the Software, Desktop, laptop, Servers, System Software, RDBMS, any other suites, whatsoever applicable separately*)

Yours Faithfully,

(Name)

(Signature)

(OEM/Manufacturer Company Stamp/Seal)

Annexure N: Compliance Requirements

(For Outsource/Hosted Model)

The solution should be in accordance with the security norms of RBI/NPCI/IRDAI/Card Associations (VISA, MasterCard, Rupay) from time to time. The Regulatory mandates by any regulator pertaining to the application or solution provided by the bidder has to be complied during the validity of contract period without any extra cost to the Bank.

The solution proposed has to be in strict compliance with extant Laws and Regulations like but not limited to IT Act 2000 read with IT Amendment Act 2008, Draft Master Directions of RBI Directions on Outsourcing, RBI Digital Payment Security Directions 2021, RBI Cyber Security Framework Circular Dated 2nd June 2016, NPCI Circulars and Directions.

As the Bank is opting for Managed Services Model, the bidder must ensure strict compliance with the Technology & Security Standards Viz. PCI-DSS, ISO 27001 ISMS or Equivalent Standard, ITIL Framework, DevSecOps, ISO 27018 Code of Practice for Personally Identifiable Information and other Software Development Standards.

The bidder shall ensure that a strong Project Governance Framework is put in place for adequately addressing associated risks and measuring the success of the project at any given point of time. The same needs to be communicated as part of the RFP response along with the escalation matrix.

In case the bidder opts for providing the services via a Multi-tenancy environment, it must be protected against data integrity and confidentiality risks and against co-mingling of data. The architecture should enable smooth recovery and any failure of any one or combination of components across the managed services architecture should not result in data/ information security compromise.

The Bidder shall share the appropriate update and release cycles affecting the service features (Such as: Security, Continuity, legal and governance…etc.). The bidder must be flexible to align the same with the Banks Patch, Vulnerability and Change Management Processes.

The Bidder, as part of bid submission shall share the detailed information on how the Service Provider ensures and applies agile and rapid yet comprehensive risk management. This must include the Risk Control checking Methodology.

In case the Service Provider is proposing the solution on Virtualized mode, the Service Provider has to ensure that the controls are in place to guarantee that only authorized snapshots are taken, and that these snapshots level of classification and storage location and encryption is compatible in strength with the production virtualization environment. Besides, the Service Provider has to ensure that the complete logs of Virtualized environment that are provided to Bank are accessible to Bank.

The bidder shall provide the Bank with its Service Providers user list that will have access to the Bank's data; at any point throughout the duration of the agreement. Service Providers should also update the Bank with any change in the employee list.

The bidder shall ensure to submit the high-level/low level design document as part of the solution offering mentioning integration of the application with Banks Privileged Identity and Access Management Solution. The Bank shall be open to provide Identity Federated integration using SAML / OpenID /Open Auth, RADIUS etc.

The Admin & User Management Framework provided by the Service Provider must be in alignment with RBI's Authentication Framework for Customers, Privileged Accesses and other Internal Users.

The Service Provider must provide the Bank secure control for managing its identities (Including Identity Creation and Deletion / Modification & Termination).

The Service Provider shall ensure Authentication, Authorization, Accounting, Access control and logging (Format, retention and Access) meet the Bank's regulatory and legal requirements.

The Service Provider shall ensure that the logging is enabled for all activities including OS and, Application level for a period not less than 180 days online and then Backed up for the period of project. The Live logs as stipulated above shall as well be integrated with Bank's SIEM Solution.

The Service Provider shall have the information readily available on Location and time of access of the Service Provider Team.

The Service Provider shall ensure Micro-segmentation of Banks services. The Service Provider shall further shall ensure to put in place, in addition to the Infrastructure Security, the Application Layer Firewalls, conduct source code reviews prior to provisioning any application release, Adopt Secure web development best practices like OWASP secure development guidelines, Adopt OS and Applications security hardening best practices. Service Provider shall submit the source code audits reports mentioning closure of all identified vulnerabilities at yearly frequency to the Bank.

Service Provider shall ensure to conduct Periodic Vulnerability Assessment & Penetration testing of its Infrastructure and applications. The MPS shall ensure that these activities are done as part of Vulnerability Management and remediation program is defined, and it includes fixing the vulnerabilities based on priority. All vulnerabilities should be prioritized and must be fixed and patched within SLAs agreed upon by the Bank and the CSP in line with Banks Patch & Vulnerability Management procedure.

Service Provider shall ensure to follow a proper software development life cycle (SDLC) and that security is an integrated part in at least the following phases:

a. Planning and requirements gathering
b. Architecture and functional Design Phase Coding
c. Testing
d. Maintenance

The bidder shall ensure to adopt and is in compliance with Change Management and Incident Response Procedures as specified in (ITIL).

The Service Provider shall share its DR plan with Bank so as to ensure it matches the Bank's BCP requirements.

The Service Provider has the ability to retrieve and restore data following data loss incidents.

Service Provider to provide the Bank at least bi-annually with the DR testing reports. The reports should be comprehensive, covering from the exercise scope till the final outcome and recommendations.

Service Provider to ensure the DR solution is capable of maintaining the same levels of security measures and controls utilized in the normal operation mode.

Ensure that the DR solution is also owned and managed entirely by the Contracted Service Provider. Conducting DR Drills & DR compliances shall be the responsibility of Contracted Service Provider.

The Bidder shall ensure to meet the Maximum Time to Recover (MTTR) also known as RTO (Recovery Time Objective) of 3 Hours and Recovery Point Objective of Zero (0).

The Service Provider shall submit the data-segmentation and separation controls at each of the four main layers at the Service Provider: (1) Network, (2) physical, (3) system and (4) Application. The same must be kept updated and produced to the Bank as and when there are any changes or as sought by the Bank.

The bidder must be open for evaluation of each of the Data segmentation controls at each layer, as well as the number and type of controls at each layer every 6 months and after major system changes and upgrades.

The Service Provider shall ensure that data is encrypted at storage and in transit and in full compliance (at any given point in time) with Bank's Cryptographic Procedure, ISO 27001 and PCI-DSS Standard. The Databases must support the function of Encryption, Redaction/Masking and Comprehensive Audit Logging.

The Service Provider shall ensure that it is using a unique set of encryption key(s) for Bank. The unique encryption keys shall help protect data from being accessible in the event that it is inadvertently leaked from one Service Provider customer to another.

The Service Provider shall ensure to provide the "Exclusive" right to data ownership to the Bank throughout the duration of the agreement. The ownership includes all copies of data available with the Service Provider including backup media copies if any. The Service Provider is not permitted to use Bank's data for advertising or any other non-authorized secondary purpose.

The Service Provider shall contractually ensure that they inform the Bank "immediately" on any confirmed breach without any undue delay. The Service Provider shall ensure that Bank is notified within 4 hours of any "Suspected" breach from the time of breach discovery.

An "Exit Management Plan" must be put in place to define the rules of disengagement. Service Provider should provide the detailed description of the exit clause including agreed process, TAT for exit, data completeness and portability, secure purge of Bank's information, smooth transition of services, complete plan of how data shall be moved out from the hosted infrastructure with minimal impact on continuity of the Bank's operations.

It shall be responsibility of the service provider to ensure smooth transition of all the data of the Banks data including audit trails, logs, to Bank specified location/storage on the conclusion of services. It would be obligatory for the Service Provider not to delete any data without the written permission from the Bank.

Service Provider shall ensure to comply with the data and media destruction and sanitization controls as stipulated in Media Disposal and Sanitization Policies of Bank. The Service Provider shall further preserve documents as required by law and take suitable steps to ensure that Banks interests are protected, even post termination of the services. This would include ensuring full integrity data transition from service provider to alternate service provider or on premise setups.

The bidder shall ensure that the services are duly audited and certified by Cert-In Empaneled Audit Companies. The bidders are required to comply with requisite audit requirements as is specified under the security standards followed under the Information Technology Act and as stipulated by the Regulators from time to time.

Bank shall ensure that the Service Provider shall neither impede/ interfere with the ability of the Bank to effectively oversee and manage its activities nor impede the supervising authority in carrying out the supervisory functions and objectives.

The Service Provider shall ensure that the arrangement shall comply with all the policies of the Bank including, but not limit to, Information Security Policy, BCP, IT Outsourcing Policy, Incident Management Policy, etc. The service provider has to comply with all the laws/ regulations issued by RBI from time to time.

The Service Provider shall grant unrestricted and effective access to data related to the outsourced activities.

The relevant business premises of the Service Provider; subject to appropriate security protocols, for the purpose of effective oversight use by the Bank, their auditors, regulators and other relevant Competent Authorities, as authorized under law.

In case the technology/software platform/ hardware / infrastructure offered under the solution on hosted model reaches end of life / support during the contract period, the bidder has to ensure that the systems are either replaced or upgraded at their/bidders own cost without any disruption in the ongoing business transactions of the Bank.

Bidder shall not propose any solution/components which is near to end of life or end of support during the tenure of the contract.

The bidder has to ensure compliance with the Software Bill of Material (SBOM) issued by CERT-IN to manage potential risks, respond to security issues and comply with regulations. The bidder has to provide assurance regarding accuracy, completeness and timelines of SBOM.

The company shall comply to the Master Directions of RBI on IT outsourcing and bank's policy on IT Outsourcing with specifically on following points:

i. *The service provide shall ensure that the Bank has an effective access to all data, books, records, information, logs, alerts and business premises relevant to the outsourced activity of the Bank, available with the service provider;*

ii. *The service provider shall facilitate regular monitoring and assessment of the service provider by the Bank for continuous management of the risks holistically, so that any necessary corrective measure can be taken immediately;*

iii. *The service provider shall inform the Bank about the material adverse events (e.g., data breaches, denial of service, service unavailability, etc.) and the incidents required to be reported to Bank to enable Bank to take prompt risk mitigation measures and ensure compliance with statutory and regulatory guidelines;*

iv. *The service provider shall ensure that the services being offered are in compliance with the provisions of Information Technology Act, 2000, other applicable legal requirements and standards to protect the customer data;*

v. *The service provider shall ensure that storage of data (as applicable) is only in India as per extant regulatory requirements;*

vi. *The service provider shall provide bank with details of data (related to Bank and its customers) captured, processed and stored;*

vii. *The service provider shall not share any types of data/ information that the service provider (vendor) is not permitted to share with Bank's customer and / or any other party;*

viii. *The Service provider shall have in place effective contingency plan(s) to ensure business continuity and testing requirements, in line with the Banks BCP;*

ix. *Bank shall have right to seek information from the service provider about the third parties (in the supply chain) engaged by the former;*

x. *The service provider shall be contractually liable for the performance and risk management practices of its sub-contractors;*

xi. *It shall be obligation of the service provider to comply with directions issued by the RBI in relation to the activities outsourced to the service provider, through specific contractual terms and conditions specified by the Bank;*

xii. *It shall be obligation of the service provider to co-operate with the relevant authorities in case of insolvency/ resolution of the Bank;*

xiii. There shall be a provision to consider skilled resources of service provider who provide core services as "essential personnel" so that a limited number of staff with back-up arrangements necessary to operate critical functions can work on-site during exigencies (including pandemic situations);

xiv. The service provider should have a suitable back-to-back arrangements with the concerned OEM, if applicable

Annexure O: CSP Assessment Checklist

(For Cloud Based Solutions Only)

Provide your response in Yes / Not-Available / Work in Progress to all the points

	Control Domain	CID	CSP Assessment Questions	Requirement	Response (Y/N)
		CO.01	*Do you allow customers to view your third party audit reports?	Mandatory	
		CO.02	*Do you conduct network penetration tests of your cloud service infrastructure regularly? If yes please elaborate on your test and remediation process	Mandatory	
		CO.03	*Do you conduct regular application penetration tests of your cloud infrastructure according to the industry best practices? If yes please elaborate on your test and remediation process.	Mandatory	
		CO.04	*Do you conduct internal audits regularly according to the industry best practices? If yes please elaborate on your test and remediation process.	Mandatory	
		CO.05	*Do you conduct external audits regularly according to the industry best practices? If yes please elaborate on your test and remediation process.	Mandatory	
		CO.06	Are the results of the network penetration tests available to customers at their request?		
		CO.07	*Are the results of internal and external audits available to customers at their request?	Mandatory	
	Third Party Audits	CO.08	Do you permit customers to perform independent vulnerability assessments?		
	Contact /	CO.9	Do you maintain updated liaisons and points of contact with local		

	Authority Maintenance		authorities? If yes then how frequently you validate the contacts?		
	Information System Regulatory Mapping	CO.10	*Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single customer only, without inadvertently accessing another customer's data?	Mandatory	
		CO.11	*Do you have capability to logically segment, isolate and recover data for a specific customer in the case of a failure or data loss?	Mandatory	
	Intellectual Property	CO.12	*Do you have policies and procedures in place describing what controls you have in place to protect customer’s data marked as intellectual property?	Mandatory	
		CO.13	If utilization of customers services housed in the cloud is mined for cloud provider benefit, are the customers’ defined IP rights preserved?		
		CO.14	If utilization of customers services housed in the cloud is mined for cloud provider benefit, do you provide customers the ability to opt- out?		
INFORMATION GOVERNANCE	Ownership	IG.01	*Do you follow or support a structured data-labelling standard (ex. ISO 15489, Oasis XML Catalogue Specification, CSA data type guidance)? If yes please specify	Mandatory	
	Classification	IG.02	Do you provide a capability to identify virtual machines via policy tags/metadata?		
		IG.03	Do you provide a capability to identify hardware via policy tags/metadata/hardware tags?		

		IG.04	Do you have a capability to use system geographic location as an authentication factor?		
		IG.05	*Can you provide the physical location/geography of storage of a customer's data upon request?	Mandatory	
		IG.06	*Do you allow customers to define acceptable geographical locations for data routing or resource instantiation?	Mandatory	
	Handling / Labelling / Security Policy	IG.07	Do you consider all customer data to be "highly sensitive "and provide the same protection and controls across the board or you apply the controls according to the data specific classification or label?		
		IG.08	*Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?	Mandatory	
INFORMATION GOVERNANCE	Retention Policy	IG.09	*Do you have technical control capabilities to enforce customer data retention policies?	Mandatory	
		IG.10	*Do you have a documented procedure for responding to requests for customer data from governments or third parties?	Mandatory	
	Secure Disposal	IG.11	*Do you support secure deletion (ex. degaussing / cryptographic wiping) of archived data as determined by the customer?	Mandatory	
		IG.12	*Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of customer data once a customer has exited your environment or has vacated a resource?	Mandatory	

	Nonproduction Data	IG.13	*Do you have procedures in place to ensure production data shall not be replicated or used in your test environments?	Mandatory	
	Information Leakage	IG.14	*Do you have controls in place to prevent data leakage or intentional/accidental compromise between customers in a multi-customer environment?	Mandatory	
		IG.15	Do you have a Data Loss Prevention (DLP) or extrusion prevention solution in place for all systems which interface with your cloud service offering?		
PHYSICAL ACCESS	Policy	PA.01	*Can you provide evidence that policies and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities and secure areas?	Mandatory	
	User Access	PA.02	*Pursuant to local laws, regulations, ethics and contractual constraints are all employment candidates, contractors and third parties subject to background checks?	Mandatory	
	Controlled Access Points	PA.03	*Are physical security perimeters (fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols) implemented?	Mandatory	
	Secure Area Authorization	PA.04	*Do you allow customers to specify which of your geographic locations their data is allowed to traverse into/out of (to address legal jurisdictional considerations based on where data is stored vs. accessed)?	Mandatory	
	Unauthorized Persons Entry	PA.05	*Are ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises monitored, controlled and isolated from data storage and process?	Mandatory	

	Offsite Authorization	PA.06	Do you provide customers with documentation that describes scenarios where data may be moved from one physical location to another? (ex. Offsite backups, business continuity failovers, replication)		
	Offsite equipment	PA.07	Do you provide customers with documentation describing your policies and procedures governing asset management and repurposing of equipment?		
	Asset Management	PA.08	*Do you maintain a complete inventory of all of your critical assets?	Mandatory	
HR	Employment Agreements	HR.01	*Do you specifically train your employees regarding their role vs. the customer's role in providing information security controls?	Mandatory	
		HR.02	Do you document employee acknowledgment of training they have completed?		
	Employment Termination	HR.03	*Are Roles and responsibilities for following performing employment termination or change in employment procedures assigned, documented and communicated?	Mandatory	
INFORMATION SECURITY	Management Program	IS.01	*Do you provide customers with documentation describing your Information Security Management System (ISMS)?	Mandatory	
	Management Support / Involvement	IS.02	*Are policies in place to ensure executive and line management take formal action to support information security through clear documented direction, commitment, explicit assignment and verification of assignment execution?	Mandatory	

	Policy	IS.03	Does your information security and privacy policies align with particular standards (ISO- 27001, NIA, CeBIT, etc.)?		
		IS.04	Do you have agreements which ensure your providers adhere to your information security and privacy policies?		
		IS.05	*Can you provide evidence of due diligence mapping of your controls, architecture and processes to regulations and/or standards?	Mandatory	
	Baseline Require ments	IS.06	*Do you have documented information security baselines for every component of your infrastructure (ex. Hypervisors, operating systems, routers, DNS servers, etc.)?	Mandatory	
		IS.07	Do you have a capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?		
		IS.08	*Do you allow your clients to provide their own trusted virtual machine image to ensure conformance to their own internal standards?	Mandatory	
	Policy Reviews	IS.09	Do you notify your customers when you make material changes to your information security and/or privacy policies?		
INFORMATION SECURITY		IS.10	*Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	Mandatory	
		IS.11	*Are employees made aware of what action might be taken in the event of a violation and stated as such in the policies and procedures?	Mandatory	

	User Access Policy	IS.12	*Do you have controls in place ensuring timely removal of access rights and permissions which is no longer required?	Mandatory	
		IS.13	*Do you provide metrics which track the speed with which you are able to remove access rights following a request from us?	Mandatory	
	User Access Restriction / Authorization	IS.14	*Do you document how you grant and approve access to customer data?	Mandatory	
		IS.15	Do you have a method of aligning provider and customer data classification methodologies for access control purposes?		
	User Access Revocation	IS.16	*Is timely de-provisioning, revocation or modification of user access to the organizations systems, information assets and data implemented upon any change in status of employees, contractors, customers, business partners or third parties?	Mandatory	
	User Access Reviews	IS.17	*Do you require at least annual certification of entitlements for all system users and administrators (exclusive of users maintained by your customers)?	Mandatory	
		IS.18	*If users are found to have inappropriate entitlements, are all remediation and certification actions recorded?	Mandatory	
		IS.19	Will you share user entitlement remediation and certification reports with your customers, if inappropriate access may have been allowed to customer data?		

	Training / Awareness	IS.20	*Do you provide or make available a formal security awareness training program for cloud-related access and data management issues (i.e., multi-tenancy, nationality, cloud delivery model segregation of duties implications, and conflicts of interest) for all persons with access to customer data?	Mandatory	
		IS.21	*Are administrators properly educated on their legal responsibilities with regard to security and data integrity?	Mandatory	
	Industry Knowledge / Benchmarking	IS.22	Do you participate in industry groups and professional associations related to information security?		
		IS.23	*Do you benchmark your security controls against industry standards?	Mandatory	
	Roles / Responsibilities	IS.24	Do you provide customers with a role definition document clarifying your administrative responsibilities vs. those of the customer?		
	Management Oversight	IS.25	Are Managers responsible for maintaining awareness of and complying with security policies, procedures and standards that are relevant to their area of responsibility?		
INFORMATION SECURITY	Segregation of Duties	IS.26	Do you provide customers with documentation on how you maintain segregation of duties within your cloud service offering?		
	User Responsibility	IS.27	*Is your staff made aware of their responsibilities for maintaining awareness and compliance with our published security policies, procedures, standards and applicable regulatory requirements?	Mandatory	

		IS.28	Are users made aware of their responsibilities for maintaining a safe and secure working environment?		
		IS.29	Are users made aware of their responsibilities for leaving unattended equipment in a secure manner?		
	Workspace	IS.30	*Does your data management policies and procedures address customer and service level security requirements?	Mandatory	
		IS.31	Do your data management policies and procedures include a tamper audit or software integrity function for unauthorized access to customer data?		
		IS.32	*Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the build/configuration of the virtual machine?	Mandatory	
	Encryption	IS.33	*Do you have a capability to allow creation of unique encryption keys per customer?	Mandatory	
		IS.34	Do you support customer generated encryption keys or permit customers to encrypt data to an identity without access to a public key certificate. (E.g. Identity based encryption)?		
	Encryption Key Management	IS.35	*Do you encrypt customer data at rest (on disk/storage) within your environment?	Mandatory	
		IS.36	*Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?	Mandatory	

		IS.37	Do you have a capability to manage encryption keys on behalf of customers?		
		IS.38	Do you maintain key management procedures?		
	Vulnerability/Patch Management	IS.39	*Do you conduct network- layer vulnerability scans regularly?	Mandatory	
		IS.40	*Do you conduct application- layer vulnerability scans regularly?	Mandatory	
		IS.41	*Do you conduct local operating system- layer vulnerability scans regularly?	Mandatory	
		IS.42	*Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications, and systems?	Mandatory	
INFORMATION SECURITY		IS.43	Will you provide your risk- based systems patching timeframes to your customers upon request?		
	Antivirus / Malicious Software	IS.44	Do you deploy multi anti- malware engines in your infrastructure?		
		IS.45	Do you ensure that security threat detection systems which use signatures, lists, or behavioral patterns are updated across all infrastructure components within industry accepted timeframes?		
	Incident Management	IS.46	*Do you have a documented security incident response plan?	Mandatory	

		IS.47	Do you integrate customized customer requirements into your security incident response plans?		
		IS.48	Do you have a CERT function (Computer Emergency Response Team)?		
		IS.49	Do you publish a roles and responsibilities document specifying what you vs. your customers are responsible for during security incidents?		
	Incident Reporting	IS.50	Does your security information and event management (SIEM) system merge data sources (app logs, firewall logs, IDS logs, physical access logs, etc.) for granular analysis and alerting?		
		IS.51	Does your logging and monitoring framework allow isolation of an incident to specific customers?		
	Incident Response Legal Preparation	IS.52	*Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes & controls?	Mandatory	
		IS.53	*Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?	Mandatory	
		IS.54	*Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific customer without freezing other customer data?	Mandatory	
		IS.55	Do you enforce and attest to customer data separation when producing data in response to legal subpoenas?		
	Incident Respons	IS.56	Do you monitor and quantify the types, volumes, and impacts on all information security incidents?		

	e Metrics				
		IS.57	Will you share statistical information security incident data with your customers upon request?		
	Acceptable Use	IS.58	Do you provide documentation regarding how you may utilize or access customer data and/or metadata?		
		IS.59	Do you collect or create metadata about customer data usage through the use of inspection technologies (search engines, etc.)?		
		IS.60	Do you allow customers to opt- out of having their data/metadata accessed via inspection technologies?		
INFORMATION SECURITY	Asset Returns	IS.61	*Are systems in place to monitor for privacy breaches and notify customers expeditiously if a privacy event may have impacted their data?	Mandatory	
		IS.62	*Is your Privacy Policy aligned with industry standards and Indian Law	Mandatory	
	e-Commerce Transactions	IS.63	Do you provide standard encryption methodologies (3DES, AES, etc.) to customers in order for them to protect their data if it is required to traverse public networks? (ex. the Internet)		
		IS.64	*Do you utilize standard encryption methodologies any time your infrastructure components need to communicate to each other over public networks (ex. Internet-based replication of data from one environment to another)?	Mandatory	

	Audit Tools Access	IS.65	Do you restrict, log, and monitor access to your information security management systems? (Ex. Hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)		
	Diagnostic / Configuration Ports Access	IS.66	*Do you ensure hardening of admin workstations and Role Based Access Control to enforce the 'least privilege' principle	Mandatory	
	Network / Infrastructure Services	IS.67	Do you collect capacity and utilization data for all relevant components of your cloud service offering?		
		IS.68	Do you provide customers with capacity planning and utilization reports?		
	Portable / Mobile Devices	IS.69	*Do you allow mobile devises in your facility for administration purposes (e.g., tablets,)?	Mandatory	
	Source Code Access Restriction	IS.70	*Are controls in place to prevent unauthorized access to your application, program or object source code, and assure it is restricted to authorized personnel only?	Mandatory	
		IS.71	*Are controls in place to prevent unauthorized access to customer application, program or object source code, and assure it is restricted to authorized personnel only?	Mandatory	
	ESV Programs Access	IS.72	*Are utilities that can significantly manage virtualized partitions (ex. shutdown, clone, etc.) appropriately restricted and monitored?	Mandatory	
		IS.73	Do you have a capability to detect attacks which target the virtual		

			infrastructure directly (ex. shimming, Blue Pill, Hyper jumping, etc.)?		
		IS.74	*Are attacks which target the virtual infrastructure prevented with technical controls?	Mandatory	
LEGAL	Non-disclosure Agreements	LG.01	*Are requirements for non- disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented and reviewed at planned intervals?	Mandatory	
	Third Party Agreements	LG.02	*Can you provide a list of current 3rd party organization that will have access to the customer's (My) data?	Mandatory	
OPERATIONS MANAGEMENT	Policy	OM.01	Are policies and procedures established and made available for all personnel to adequately support services operations roles?		
	Documentation	OM.02	Are Information system documentation (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure Configuring, installing, and operating the information system?		
	Capacity / Resource Planning	OM.03	Do you provide documentation regarding what levels of system (network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios?		
		OM.04	*Do you restrict use of the memory oversubscription capabilities present in the hypervisor?	Mandatory	
	Equipment	OM.05	If using virtual infrastructure, does your cloud solution include hardware independent restore and recovery		

	Maintenance		capabilities including offsite storage of backups?		
		OM.06	*If using virtual infrastructure, do you provide customers with a capability to restore a Virtual Machine to a previous state in time?	Mandatory	
		OM.07	*If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?	Mandatory	
		OM.08	*If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?	Mandatory	
		OM.09	Do you share reports on your backup/recovery exercise results?		
		OM.10	Does your cloud solution include software / provider independent restore and recovery capabilities?		
RISK MANAGEMENT	Program	RM.01	Is your organization insured by a 3rd party for losses?		
		RM.02	*Do your organization's service level agreements provide customer remuneration for losses they may incur due to outages or losses experienced within your infrastructure?	Mandatory	
	Assessments	RM.03	*Are formal risk assessments aligned with the enterprise- wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods?	Mandatory	

		RM.04	Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance)?		
	Mitigation / Acceptance	RM.05	*Are risks mitigated to acceptable levels based on company-established criteria in accordance with reasonable resolution time frames?	Mandatory	
		RM.06	*Is remediation conducted at acceptable levels based on company-established criteria in accordance with reasonable time frames?	Mandatory	
	Business / Policy Change Impacts	RM.07	*Do risk assessment results include updates to security policies, procedures, standards and controls to ensure they remain relevant and effective?	Mandatory	
	Third Party Access	RM.08	Do you monitor service continuity with upstream internet providers in the event of provider failure?		
		RM.09	Do you have more than one provider for each service you depend on?		
		RM.10	Do you provide access to operational redundancy and continuity summaries which include the services on which you depend?		
		RM.11	Do you provide the customer the ability to declare a disaster?		
		RM.12	Do you provide a customer triggered failover option?		
		RM.13	*Do you share your business continuity and redundancy plans with your customers?	Mandatory	

SW DEPLOYMENT	New Development / Acquisition	SD.01	*Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations, and facilities?	Mandatory	
	Production Changes	SD.02	*Do you provide customers with documentation which describes your production change management procedures and their roles/rights/responsibilities within it?	Mandatory	
	Quality Testing	SD.03	Do you provide your customers with documentation which describes your quality assurance process?		
	Outsourced Development	SD.04	*Do you have controls in place to ensure that standards of quality are being met for all software development?	Mandatory	
		SD.05	*Do you have controls in place to detect source code security defects for any outsourced software development activities?	Mandatory	
	Unauthorized Software Installations	SD.06	*Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	Mandatory	
DISASTER RECOVERY	Impact Analysis	DR.01	Do you provide customers with on-going visibility and reporting into your operational Service Level Agreement (SLA) performance?		
		DR.02	Do you provide customers with on-going visibility and reporting into your SLA performance?		
	Business Continui	DR.03	Are you BS25999 or ISO 22301 certified?		

	ty Planning				
		DR.04	Do you provide customers with geographically resilient hosting options?		
	Business Continuity Testing	DR.05	*Are business continuity plans subject to test at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	Mandatory	
	Environmental Risks		*Is physical protection against damage from natural causes and disasters as well as deliberate attacks anticipated, designed and countermeasures applied?	Mandatory	
	Equipment Power Failures	DR.07	*Are Security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?	Mandatory	
	Power / Telecommunications	DR.08	Do you provide customers with documentation showing the transport route of their data between your systems?		
		DR.09	Can customers define how their data is transported and through which legal jurisdiction?		
ARCHITECTURE	Customer Access Requirement	AR.01	Are all identified security, contractual and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets and information systems?		
		AR.02	Do you use open standards to delegate authentication capabilities to your customers?		
		AR.03	*Do you support identity federation standards (SAML, SPML, WS-Federation,	Mandatory	

			etc.) as a means of authenticating/authorizing users?		
		AR.04	Do you have a Policy Enforcement Point capability (ex. XACML) to enforce regional legal and policy constraints on user access?		
		AR.05	Do you have an identity management system in place which enables both role-based and context-based entitlement to data (enables classification of data for a customer) if requested?		
		AR.06	*Do you provide customers with strong (multifactor) authentication options (digital certs, tokens, biometric, etc...) for user access?	Mandatory	
		AR.07	Do you allow customers to use third party identity assurance services?		
		AR.08	Do you utilize an automated source-code analysis tool to detect code security defects prior to production?		
		AR.09	*Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?	Mandatory	
	Data Integrity	AR.10	*Are data input and output integrity routines (i.e., reconciliation and edit checks) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?	Mandatory	
	Production / Nonproduction Environment	AR.11	*For your PaaS offering, do you provide customers with separate environments for production and test processes?	Mandatory	

		AR.12	For your IaaS offering, do you provide customers with guidance on how to create suitable production and test environments?		
	Remote User Multifactor Authentication	AR.13	*Is multi-factor authentication required for all remote user access?	Mandatory	
ARCHITECTURE	Network Security	AR.14	For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?		
	Wireless Security	AR.15	*Are policies and procedures established and mechanisms implemented to protect network environment perimeter and configured to restrict unauthorized traffic?	Mandatory	
		AR.16	*Are policies and procedures established and mechanisms implemented to ensure proper security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings? (e.g., encryption keys, passwords, SNMP community strings, etc.)	Mandatory	
		AR.17	*Are policies and procedures established and mechanisms implemented to protect network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?	Mandatory	
	Shared Networks	AR.18	*Is access to systems with shared network infrastructure restricted to authorized personnel in accordance with security policies, procedures and standards? Networks shared with	Mandatory	

			external entities shall have a documented plan detailing the compensating controls used to separate network traffic between organizations?		
	Clock Synchronization	AR.19	*Do you utilize a synchronized time-service protocol (ex. NTP) to ensure all systems have a common time reference?	Mandatory	
	Equipment Identification	AR.20	Is automated equipment identification used as a method of connection authentication to validate connection authentication integrity based on known equipment location?		
	Audit Logging / Intrusion Detection	AR.21	*Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis and response to incidents?	Mandatory	
		AR.22	*Is Physical and logical user access to audit logs restricted to authorized personnel?	Mandatory	
		AR.23	*Can you provide evidence that due diligence mapping of currently applicable regulations and standards to your controls/architecture/process has been done?	Mandatory	
	Mobile Code	AR.24	*Is mobile code tested (in terms of security) before its installation and use and the code configuration checked to ensure that the authorized mobile code operates according to a clearly defined security policy?	Mandatory	
		AR.25	*Is all unauthorized mobile code prevented from executing?	Mandatory	