ONLINE REQUEST FOR PROPOSAL (e-RFP)
FOR
CLOUD SECURITY POSTURE MANAGEMENT & WORKLOAD PROTECTION.

e-RFP Ref. No.JKB/CHQ/ISD/ CLOUD SECURITY/2025-1602

Dated: 17-12-2025

Issued By
J&K Bank
Information Security Department,
2nd Floor Annex Building,
Corporate Headquarters
M.A Road, Srinagar 190001
Phone No -01942713301
e-mail id – info.security@jkbmail.com

SCHEDULE OF RFP

e-RFP Reference No.	JKB/CHQ/ISD/ CLOUD SECURITY /2025-1602 Dated: 17-12-2025
Date of Issue of RFP	18-12-2025
e-RFP Description	REQUEST FOR PROPOSAL (RFP) FOR CLOUD SECURITY POSTURE MANAGEMENT & WORKLOAD PROTECTION.
Issuer of the RFP-Department	Information Security Department
Bank's Communication Details	J&K Bank Information Security Department, 2nd Floor , Annex Building, Srinagar
RFP Application Fee (Non - Refundable)	Rs.1,500/- (Rupees One Thousand Five Hundred 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)	₹ /5,00,000 (INR Five Lac Only) 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)
Bid Document Availability including changes/amendments, if any to be issued	NIT can be downloaded from and submitted on Bank's e-Tendering Services Provider's Portal https://jkbank.abcprocure.com from December 18, 2025 16.00 Hrs. January 07 , 2026 17.00 Hrs.
Last Date for Pre-Bid Queries & submission Mode	All Clarifications / Queries shall be raised online only through e-Tendering Portal https://jkbank.abcprocure.com by or before December 26, 2025 17.00 Hrs.
Pre-bid Queries Response date	All communications regarding points / queries requiring clarifications shall be given online through prescribed e-Tendering Portal on January 02, 2026
Last Date of Submission of RFP Bid	January 07 , 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

<table>
<tr>
<td>For e-Tender related Queries</td>
<td>
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

<u>Help Desk:</u>
<table>
<tr><th>Sr. No</th><th>Name</th></tr>
<tr><td>1</td><td>Sandhya Vekariya – 6352631968</td></tr>
<tr><td>2</td><td>Suraj Gupta – 6352632310</td></tr>
<tr><td>3</td><td>Ijlalaehmad Pathan – 6352631902</td></tr>
<tr><td>4</td><td>Imran Sodagar - 9328931942</td></tr>
</table>
</td>
</tr>
</table>

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

CONTENTS

SECTION D-General Terms & Conditions			
1	Standard of Performance	18	Project Risk Management
2	Indemnity	19	Information Security
3	Cancellation of Contract and Compensation	20	Survival
4	Liquidated Damages	21	Information Security
5	Fixed Price	22	No Set-Off, Counter-Claim and Cross Claims
6	Right to Audit	23	Statutory Requirements
7	Force Majeure	24	Bidder Utilization of Know-how
8	Publicity	25	Corrupt & Fraud Practices
9	Amendments	26	Solicitation of Employees
10	Assignment	27	Proposal Process Management
11	Severability	28	Confidentiality Provision
12	Applicable law and jurisdictions of court	29	Sub-Contracting
13	Resolution of Disputes and Arbitration clause	30	Reverse Auction
14	Execution of Service Level Agreement (SLA)/ Non-Disclosure Agreement (NDA)	31	Award Notification
15	NO CLAIM Certificate	32	Suspension of Work
16	Cost And Currency		
17	No Agency		

SECTION E-Annexures			
1	Annexure A-Confirmation of Terms and Conditions	7	Annexure G: Bank Guarantee Format

2	Annexure B: Tender Offer Cover Letter	8	Annexure H: Performance Bank Guarantee Format
3	Annexure C: Details of SI/OEM	9	Annexure I: Non-disclosure Agreement (NDA)
4	Annexure D: Compliance to Eligibility Criteria	10	Annexure J: Service Level Agreement
5	Annexure E: Technical Bid Form	11	Annexure K: Undertaking
6	Annexure F: Commercial Bid Format		

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 Automated Delivery Points. The Bank uses Information Technology in all spheres of its functioning and functions as a universal Bank in UT of Jammu & Kashmir & Ladakh and as a specialized Bank in the rest of the country. The Bank has its Data Centre in Noida and DR site in Mumbai. It is also the only private sector Bank designated as RBI's agent for banking business, and carries out the banking business of the Central Government, besides collecting central taxes for CBDT. 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

J&K Bank invites proposals from qualified bidder for the supply, implementation, and support of a Cloud Security Posture Management & Workload Protection. The objective is to strengthen the Bank's security framework by enabling continuous monitoring, compliance management, risk identification, and remediation across its cloud environments. This initiative aims to ensure adherence to regulatory requirements, safeguard sensitive data, and enhance the overall security posture of the Bank's cloud infrastructure in alignment with industry best practices.

Eligibility Criteria

J&K Bank shall scrutinize the Eligibility bid submitted by the bidder. A thorough examination of supporting documents to meet each eligibility criteria (Annexure D) 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

Bidder is required to supply, implement, and support of a Cloud Security Posture Management & Workload Protection. Bidder's project scope, includes, but not limited to:

1. **Platform Requirement**

i. The solution should be a Cloud Security Posture Management setup which can integrate over API with multiple accounts and multiple regions of in public cloud environment such as Amazon Web Services (AWS), Azure, Google Cloud Platform (GCP) and Oracle Cloud Infrastructure (OCI) with a single centralized console and generate alerts related to but not limited to improper network, misconfiguration, and for compliance related issues.

ii. The solution must support cloud security posture assessment i.e. misconfiguration detection, compliance without any dependency on snapshot based agentless scanning.

iii. The solution must have a centralized asset inventory and Configuration Management Database (CMDB) of all cloud assets across various cloud environments such as Amazon Web Services (AWS), Azure, Google Cloud Platform (GCP) and Oracle Cloud Infrastructure (OCI)

iv. The Solution shall continuously discover and automatically classify cloud resources as soon as they are deployed.

v. The Solution shall maintain full history of configuration changes over time for each cloud asset, to simplify compliance auditing and forensics. Should provide a quick diff/delta view of configuration add/delete/change for each cloud asset along with the line view.

vi. The solution shall provide the choice of agentless or agent-based deployment based on use cases.

vii. The solution shall support major cloud service providers including AWS, Google Cloud, Azure, OCI, IBM, Alibaba Cloud, and IBM Cloud etc.

viii. The solution shall leverage generative artificial intelligence (AI) for end users to ask any question about their environment and automate repetitive tasks.

ix. The solution must identify the riskiest infrastructure resources exposure to Internet by combining misconfiguration, vulnerability, internet exposure, threats, anomalies, excessive permission, identity related threats, web and api related risks, data security risks to prioritize remediation effort.

2. Enforce Policy Governance

i. The Solution should continually monitor all cloud resources for misconfigurations.
ii. The Solution should provide out-of-box policies to check for security best practices for Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) configuration.
iii. The Solution shall provide ability to clone, customize, and run an existing policy
iv. The Solution shall have ability to enforce policy governance guardrails that can automatically trigger alerts for misconfigurations and configuration drift.
v. The Solution shall have the ability to provide guided remediation details for issues detected out-of-the-box
vi. The Solution shall have the ability to auto-remediate infrastructure changes based on a specific policy requirement, without needing any external tools and functions.

3. Detecting Risks and Incidents and generating Alerting

i. The Solution shall have ability to detect and Alert on Risky Configurations:
ii. Provide facility to View configuration alerts in Graphical User Interface (GUI) Console and utilize tool to investigate the user activities that led to the misconfiguration.
iii. The Solution shall have ability to detect and Alert on Network Security:
iv. Check for unencrypted traffic, assets directly connected to the internet, compromised services, and traffic to and from suspicious IPs.
v. The Solution Should have ability to detect and Alert on Sensitive Audit Actions.
vi. Check report on sensitive user activities such as asset creation/deletion, security group changes, Identity Access Management (IAM) role changes and more.
vii. The Solution shall have ability to detect and Alert on Anomalous User Activities:
viii. Identify anomalous activities and provides guidance on how to take actions to prevent further incident.

4. **Cloud Compliance & Reporting**

i. The Solution shall provide a customizable view of entire compliance posture in compliance dashboard for all Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) services.
ii. The solution shall have the ability to automatically generate on demand reports of specific sets of controls and/or compliance for all Public Cloud Accounts

iii. The solution have the ability to report on compliance status for cloud infrastructure services as per: minimum compliance reporting for Industry and sectoral specific reports like PCI DSS, CIS (AWS, Azure, GCP), RBI Baseline Cyber Security and Resilience Requirements, SEBI - Consolidated Cybersecurity and Cyber Resilience Framework (CSCRF), SOC 2, PCI DSS, NIST 800-53 Rev5, HIPAA, GDPR, ISO 27001, NIST CSF, MiTRE ATT&CK. Also should have option & ability to create custom compliance templates based on business requirements.

iv. The solution shall have the ability to export reports to PDF. Also, shall have built-in ability to schedule daily, Monthly and weekly emailing of compliance PDF report to the required stakeholders.

5. Investigation capabilities

i. The Solution shall provide ability to perform ad hoc investigation for reviewing active resources and resource changes across multi-cloud environment.

ii. The Solution shall have ability to ingest Cloud Configuration and allow to run ad hoc query and investigation on them

iii. The Solution shall have ability to ingest Cloud audit logs of privilege user activity and allow to run ad hoc query and investigation on them. Also, shall provide user activity and a Geolocation details based on user login activity.

iv. The Solution shall have ability to ingest cloud flow logs from the cloud providers and allow to run ad hoc query and investigation on them. Also shall provide graph visualization of network flows to create a point in time the traffic flow in the Purchaser's cloud VPC.

v. The solution shall support granular queries across any IAM policies and events for investigations.

vi. The solution shall provide option to explore IAM permissions, relationships, and events with an intuitive graph.

6. Integrations

i. The solution shall have the ability to send alerts via integrations with 3rd party solutions like Security Information Event Management, Security Orchestration Automation Response and Helpdesk/Ticketing Platforms using industry standard integrations.

ii. The solution shall have the ability to ingest and display 3rd party host vulnerability and threat data from Vulnerability Assessment platforms (like Tenable Nessus, Qualys, etc), Cloud platforms.

iii. The solution shall have the ability to integrate with Bank's Single Sign On(SSO) solution and demonstrate user access for a valid user and deny for an invalid user.

iv. The solution shall have the ability to provide a fully supported Rest API for programmatic access to the tool, so that teams can take advantage of automating various tasks and reporting.

7. Cloud Network Traffic Analysis & Network anomaly detection

i. The solution shall have the ability to generate a snapshot in time visualization of network activity including auto classification of Suspicious IPs

ii. The Purchaser shall be able to automate Weekly, Monthly compliance report

iii. The solution shall have out-of-the-box security policies purpose- built to address threat vectors targeting public cloud environments, including detection of cloud-specific threats like crpytojacking activities.

iv. The solution shall detect unusual server port activity or unusual protocol activity from a client within or outside the Purchaser's cloud environment to a server host within or outside the Purchaser's network, using a server port or an IP protocol that is not typical to the Purchaser's network traffic flows.

v. Network reconnaissance - The solution shall detect port scan or port sweep activities that probe a server or host for open ports.

vi. The solution shall identify hosts within the Purchaser's cloud environment that may be compromised and sending out spam.

vii. Detect anomaly such as but not limited to:

- backdoor activity
- botnet activity
- cryptominer activity
- DDoS activity
- downloader activity
- dropper activity
- exploit kit activity
- file infector activity

- hacking tool activity
- infostealer activity
- Linux malware activity
- loader activity
- network data exfiltration activity
- port scan activity
- port sweep activity
- ransomware activity
- remote access trojan activity
- rootkit activity
- spambot activity
- unusual protocol activity
- unusual server port activity
- webshell activity
- wiper activity
- worm activity

8. IAM Monitoring & User Entity Behavior Analysis

i. The solution shall have ability to do Privileged activity monitoring and alert on unusual user activity—Discover insider threat and an account compromise using advanced data science. This shall be aided with profiling of a user's activities on the console, as well as the usage of access keys based on the location and the type of cloud resources.

ii. The solution shall have ability to do User and Entity Behavior Analytics (UEBA) and alert on Excessive login failures—Detect potential account hijacking attempts discovered by identifying brute force login attempts. Excessive login failure attempts shall be evaluated dynamically based on the models observed with continuous learning.

iii. The solution shall have ability to detect Account compromise, insider threat detection, and monitoring and alert on account hijacking attempts-Detect potential account hijacking attempts discovered by identifying unusual login activities. These shall be based on concurrent login attempts made in short duration from two different

geographic locations or login from a previously unknown browser, operating system, or location.

iv. Detect suspicious activity originating from The Onion Router (TOR) anonymity network to access resources related to services such as below that could lead to potentially malicious activities from the user:

- AI / ML services
- Analytics services
- Application Integration services
- Compute services
- Containers services
- Database services
- Dev Tools services
- IoT services
- Media services
- Migration services
- Monitoring / Management services
- Networking services
- Security services
- Storage services
- Web services

9. Remediation

i. The solution shall provide alerts with detailed context with suggested remediation steps.

ii. The solution shall provide the ability to auto remediate misconfigurations and compliance violations from the console without needing any additional tools/functions.

iii. The solution shall integrate with ticketing systems (e.g., Jira, ServiceNow, Slack) for alerting and remediation.

iv. The solution shall provide detailed remediation steps and automated remediation options for IAM permission and access alerts.

10. Agentless Workload Scanning

i. The solution shall provide option to scan hosts, containers, Kubernetes, and serverless workloads without deploying agents. Agentless scanning shall:

- Detect vulnerabilities in workloads and images.

- Detect configuration risks and compliance violations in workloads.

- Detect malware in workloads.

- Detect secrets hidden in plain sight within running and non-running workloads

ii. The solution shall scan workloads in runtime across multi-cloud environments (AWS, Azure, GCP, OCI).

iii. The solution shall scan virtual machines and host OS architectures (Linux, Windows).

iv. The solution shall scan container architectures (Docker, Kubernetes, OpenShift, Red Hat).

v. The solution shall scan Kubernetes architectures, including managed Kubernetes services (e.g., Amazon EKS, Google GKE, Azure Container Service).

vi. The solution shall scan container images before they're deployed inside container registry and CI/CD pipelines.

vii. The solution shall scan serverless architectures (Amazon Lambda, Azure Functions, Google Cloud Functions).

viii. The solution shall detect sensitive information that is improperly secured inside host and container images such as embedded passwords, login tokens, and other types of secrets.

11. Manage Cloud Identity, Permission and Access Entitlement Discovery

i. The solution shall discover both human and machine identities as well as entitlements across cloud providers.

ii. The solution should discover accurate net-effective cloud identity entitlements of machine and users to gain clear visibility and actionable insight for cloud identities across clouds through visualized graph and table views.

iii. Must provide the capability to visualize the relationship between roles and resources that access has been granted in either a graph or table view

iv. The solution should support integration with IdP services such as Okta, Azure AD etc to gain comprehensive and complete cloud identity visibility across multi-cloud environments.

12. Policy and Governance

i. The solution shall provide out-of-the-box policies to identify risky permissions and remove unwanted access.

ii. The solution must provide the ability to create customizable policies for specific IAM issues within an organization.

iii. The solution shall automatically Identify IAM policies that enable public data exposure, privilege escalation, and lateral movement.

iv. The solution shall identify workloads with permissions to create new users, roles, and groups.

v. The solution shall automatically detect identity threats such as account compromise, insider threats, and other malicious activity.

vi. The solution shall provide option to apply user and entity behavior analytics (UEBA) to detect anomalous behaviors.

CLOUD WORKLOAD PROTECTION (CWP) for Cloud Native Workload Security

1. General

i. The solution should be deployed as a minimal agent on the cloud workloads such as VMs, Containers and Serverless to provide asked security features to the workloads and should provide a unified workload protection framework to protect cloud native applications across different environments such as cloud managed Kubernetes platform, self-operated Kubernetes platform, OpenShift and etc

ii. The solution must provide a defense-in-depth approach to protect the host-VMs, Containers and Serverless functions across their lifecycle by using continuous vulnerability management, compliance checking, runtime defense and cloud native Web Application security

iii. Should generate a GUI based dynamically generated map showing all the inter VM, inter containers, serverless and inter process communication and function level interface with other services in the cloud environment.

iv. The solution must support workloads (hosts, containers and kubernetes) running either on public cloud like AWS, Azure, GCP, OCI and On-premise datacenter.

v. The solution should provide for grouping of the containers by Cluster and namespaces in the map

vi. Maps for VMs, Containers and Serverless should color-code the objects on the map to show vulnerability status, compliance status and runtime state such that the security posture of the application is instantly obtained

vii. The sensors should run only a single instance of the agent on each VM and Kubernetes/Dockers worker node without adding any files or binaries to the containers being protected

viii. The platform should display the security status of existing running containers and container hosts according to their risk level in a dashboard immediately after installation. This should include existing vulnerabilities and malware as well as the insecure container or container host configurations.

2. Vulnerability Management

i. The solution should provide flexibility to choose between agentless and agent-based security for cloud native workload (host, containers and Serverless) vulnerability and compliance management across AWS, Azure, GCP and Oracle Cloud.

ii. Should perform continuous vulnerability management across all types of workloads such as VM, Container and Serverless environment including the registry and repository for the same.

iii. The solution should support vulnerability detection across the OS layer, application framework and custom packages and The agent should be able to scan the host operating system on which the containers are running and provide details of all known vulnerabilities

iv. The solution should report the result of vulnerability scan done in CI/CD tools on the centralized console and must allow definition of policies to alert and block severe vulnerabilities from moving forward in the development pipeline

v. Should highlight risk factors introduced by each vulnerability and utilize behavioral metrics about current runtime environment to assign risk score to vulnerabilities such that vulnerabilities with highest risk can be identified

vi. Should be able to also take information from runtime environments and correlate vulnerability risk to them and provide risk score for top vulnerabilities in the production, UAT environment

vii. The solution should support vulnerability detection across the OS layer, application framework and custom packages and The agent should be able to scan the host operating system on which the containers are running and provide details of all known vulnerabilities

viii. Should provide layer by layer vulnerability analysis and pinpoints vulnerability data at each container image layer.

ix. Should allow definition of policies for admission control to stop images not matching the corporate vulnerability polices from being run in production environment

x. Should provide flexibility to apply different policies to different images based on container name, image name, host name and labels

xi. Should provide plugin and command-line interface for integrating with Jenkins and other CI/CD tools such that vulnerability scan can be performed during the build process.

xii. The solution should have pre-built templates for HIPAA, PCI, GDPR, and NIST SP 800-190, along with 300+ certified checks for the AWS, Dockers, Kubernetes, and Linux CIS Benchmarks

xiii. The solution should provide for at least 300 out of box checks for hardening and compliance checks of the cloud environment

xiv. The solution must support for custom compliance checks via OpenSCAP, XCCDF, and Bash scripts

xv. The solution should allow for creation of TRUST policy to allow, by policy, which registries, repositories, and images to trust, and stop images from running if they are deemed non-trusted

xvi. The solution must allow definition of policies to not just alert non-compliance but also enforce the recommendations of selected compliance checks

xvii. Granular policy controls prevent unauthorized images from progressing through the CICD pipeline

3. Runtime environment protection

i. The solution should be able to learn the behavior of each running container workloads and build runtime model automatically
ii. The solution should provide visibility in the terms of processes running, ports being listened, outbound connections made, domain names lookup by DNS and file system access
iii. The solution should update runtime model of workloads automatically for new application releases
iv. The solution should detect anomalies in running workloads based on automatically generated runtime models on processes, network activities and file system access
v. The solution must block suspicious activities based on runtime model learned, malware database and advanced threat protection feeds
vi. The solution must store forensic data as part of any security incident and displays the incident, kill chain, and data timeline for seamless incident response
vii. The solution should have host OS behavior modelling capabilities using the process and file system actions that understands the tasks that OS services need to do as a baseline.
viii. The solution must provide File Integrity monitoring Monitor files and directories against read, write, and metadata changes with alert and prevent capabilities.
ix. The solution must provide behavioral-based anomaly detection - host intrusion detection and protection for the underlying host OS.
x. The solution should provide host and container forensics capabilities to help after action analysis of host system behaviors to determine the sequence of events that lead to an incident.
xi. The solution should provide Incident forensics, logging with alert to simplify SOC Incident Response
xii. The platform should have the ability to fine-tune runtime policy to reduce noisy false positives and compatibility to enforce policy for Alert, Block and Kill.
xiii. The platform should have the ability to fine-tune runtime policy by adding threat-based active protection such as malware detection, crypto miners, reverse shell attacks, port scanning etc. to reduce noisy false positives and compatibility to enforce policy for Alert, Block and Kill.

4. **Network Security features**

i. The solution must perform zero-touch machine learning to automatically build network topology across hosts, containers, and serverless apps

ii. The solution must learn new communication patterns across workloads automatically for new application releases

iii. The solution must provide Layer 7: Application protection to protect workloads against known and unknown threats including but not limited to SQL injection, brute force attacks, click jacking, shellshock, information leakage and etc.

iv. The solution should discover API endpoints for granular visibility on deployed cloud assets and API Gateways.

v. The tool should perform API risk profiling to identify API risk factors, sources of risk, vulnerabilities and changes to prioritize remediation or protection.

vi. The solution should detect, alert & block Web and API attacks in real time on hosts, containers, kubernetes and serverless deployments to prevent breaches.

vii. The solution should detect, alert & block OWASP Top 10 Web Attacks in real time to prevent breaches

viii. The solution should have the ability to provide a risk assessment for API definitions to determine risky and insecure APIs.

5. **Quality Gate and Trusted Image enforcement for container going in to Production Clusters**

i. The tool must dynamically analyses the runtime behavior of image in on-prim sandbox environment before running them in your development and production environments.

ii. The Solution should prevent container being deployed on kubernetes cluster/worker Nodes, if container image does not meet the minimum defined vulnerability criteria without relying on CI-CD tools or on Kubernetes access control to prevent malicious containers to run on worker nodes.

iii. The Solution should prevent container being deployed on kubernetes cluster/worker Nodes, if container image has Compliance issue. Example:: Sensitive info is embedded in environment variables, Private keys stored in Image, Image is created with a root user. Etc. This should be achieved without relying on CI-CD tools or on Kubernetes access control.

iv. The Solution should have ability to prevent container being deployed on kubernetes cluster if container image is not prequalified as TRUSTED IMAGE. The tool should be able to create TRUSTED IMAGE policy based on (a) Trusted Repos (b) Trusted Base Images (c) Manually qualified images etc. And the tool should have ability to alert and/or block deployment when container don't meet the TRUSTED IMAGE policy without relying on CI-CD tools or on Kubernetes access control.

6. Container image sandbox analysis

i. The solution should dynamically scan container images in a sandbox to detect suspicious activities like malware and port scanning and provide a detailed runtime behavior profile to prevent malicious images from deployment into runtime

ii. Capability to scan and sandbox container images upon download from 3rd parties to analyze prior to developing apps on it.

- Malicious Behavior i.e. malware, crypto miners and outbound C2C.
- Understand behavior of container image i.e. process/file system calls

7. Architecture and Integration

i. The solution should be provided as a SaaS or on-premise software tool with support for VMs and Kubernetes/container in AWS, Azure, and GCP cloud environments. It should provide flexibility of securing cloud native software stacks on Openshift, Kubernetes, and Tanzu container environment.

ii. The solution should have extensive logging and telemetry capability

iii. The solution should have extensive API capability and should offer all the above features as and API

iv. The solution must have an intuitive UI to provide rapid forensics and investigative capabilities.

v. The solution must integrate with Active Directory, OpenLDAP, and SAML

vi. The solution must have Alerting integration with developer and operations tools like Jira, Slack, Pager duty, SOAR platforms

vii. The solution must provide for Open integration support for alert using Webhook.

Cloud Code Security

1. Infrastructure as code
   i. The solution must Identify misconfigurations in IAC files and present developer friendly suggestions and fixes via native IDE, VCS (Git) & CI/CD plugins to prevent misconfigured resources from deployment into runtime
   ii. Tool must have the capability to scan a wide array of IAC templates i.e. TFT (HCL format), CFT (JSON / YAML), ARM, Helm, Dockerfiles, Swagger, Kubernetes App manifest (JSON/YAML), BICEP and others and where possible automated remediation actions
   iii. Must be able to detect and scan existing IAC templates in Git repos i.e. GitHub, Gitlab, BitBucket, Azure Repos etc.
   iv. Must be able to detect and scan existing IAC mis-configurations in pull request/merge request
   v. Must be able to visualize the relationships between code elements i.e. IAC and Packages to determine relationships and dependencies
   vi. The tool must have the capability to integrate with DevOps tooling and workflows i.e. IDE, CI workflows and GitOps workflows
   vii. Platform supports scanning of secrets, detect secrets in IDEs, Git-based VCS, and CI/CD executions.
   viii. Must be able to natively report results within Developer workflow tools i.e. Git (Github, Gitlab etc.), IDE tools and CI tooling as well as ad hoc usage via the CMD.
   ix. Capability to define code custom policies in addition to out of the box policies that can be cloned.
2. Software Composition Analysis (SCA)
   i. The solution must detect and prevent critical open source vulnerabilities from being deployed in direct & transitive dependencies with clear, automated fixes and blocking via native IDE, VCS or CI/CD plugins.
   ii. Must have the capability to perform SCA for a wide range of package manager's i.e. Dockers, Go, Java (Maven/Gradle) Javascript (NPM, Yarn, Bower) Kotlin (Gradle) Python (Pip, Pipfile), Ruby and YAML
   iii. The solution support vulnerability scanning based on CVE's and return detailed information on each vulnerability i.e. CVE ID, CVSS score, Package Name, Version, Attack Vector, Public POC, Exploit in the Wild and whether a fix is available

iv. Must be able to provide the capability to bump fix packages.

v. Must list and map all packages and their dependencies, also visualize where possible as a supply chain with dependencies.

vi. Must provide scanning for licensing compliance violations and non-compliance

vii. Must be able to scan existing repos for code based vulnerability and compliance issues.

viii. Must be able to scan packages as changes and modifications are raised via Pull and Merge request.

ix. Ability to generate Software Bill of Materials (SBOM) and output in industry standard formats i.e. Cyclone DX XML and CSV

Location of Work

The successful bidder shall be required to work in close co-ordination with Bank's teams during entire life cycle of the project. The successful bidder may be required to work at locations prescribed by Bank such as Banks CHQ, DC/DR and other offices as per Banks requirement. All expenses (travelling/lodging, etc.) shall be borne by the successful bidder.

1. **J&K Bank Ltd.**
   Information Security Department / Security Operations Center,
   Corporate Headquarters, M A Road,
   Srinagar 190001, Kashmir (UT of Jammu & Kashmir)
   India

2. **Datacenter Noida**

   Jammu & Kashmir Bank Ltd.
   Facility Management, Noida
   J&K Bank, 5th & 7th Floor, SIFY Greenfort
   Data Centre, Plot No:B-7, Opposite
   Jaypee Hospital, Sector 132, Noida, U.P. India 201301

3. **DR Mumbai**

   Jammu & Kashmir Bank Ltd.
   Disaster Recovery Site,
   Plot. No GEN/72/1/A, TTC Industrial Area
   MIDC Mahape Navi Mumbai-400701

Invitation for Tender Offer

J&K Bank invites tenders for invite online bids from bidders fulfilling requisite eligibility criteria laid down in the RFP 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 **₹1,500** by way of NEFT, details of which are mentioned at clause 13.2.

1. 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.

2. Bidders are required to submit Bank guarantee drawn in favor of "J&K BANK LTD" payable at Srinagar, towards Earnest money Deposit (EMD). The Bank may accept Bank guarantee in lieu of EMD for an equivalent amount valid for 180 days 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.

3. 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 high level deliverables expected from the bidder are as mentioned below however low level deliverables will be finalized with successful bidder (refer to the scope mentioned in Scope of Work clause. (Service provider also need to provide milestone wise, role wise and application wise (if applicable) resource man-day projection along with their technical proposal):

Bidder needs to adhere to below mentioned project timeline for implementation of proposed EMM solution.

1	a. Project kick-off b. Submission of System Requirement Specification (SRS) study. c. Submission of High-level design document, Low-level design document and pre-requisites.	Completion of the activities within 2 weeks of issuance of Purchase Order
2	Installation, configuration and commissioning of the entire solution as per Bank's requirement.	OEM is required to do end-to-end installation, configuration and commissioning, license delivery within 4weeks from the date of issuance of Purchase Order.
3	Product Trainings (Certified Training Through the OEM Learning Process)	Within 4 week from the date of completion of installation, configuration and commissioning.

The bidder must strictly adhere to the timeline schedule, as specified in the purchase contract executed between the Parties for performance of the obligations, arising out of the purchase contract and any delay in completion of the obligations by the bidder will enable Bank to resort to any or all of the following provided that the bidder is first given a 30 days" written cure period to remedy the breach/delay:
a. Claiming Liquidated Damages
b. Termination of the purchase agreement fully or partly and claim liquidated damages.
c. Forfeiting of Earnest Money Deposit / Invoking EMD Bank Guarantee/Performance Guarantee.

However, Bank will have the absolute right to charge penalty and/or liquidated damages as per Tender /contract without giving any cure period, at its sole discretion besides taking any other appropriate action.

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 may extend the Bidder's time for performance against suitable extension of the performance guarantee for delivery.

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) besides taking appropriate action against the successful bidder including blacklisting such bidder from participating in future tenders.

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.

REVIEW:
The solution shall remain under review for a period of 2 months from the date of issuance 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 solution 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 endeavor 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. 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 160 marks or more out of 200 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 160 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 **160 out of 200** 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**. 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.

Stage 3-Evaluation of Commercial Bid

Scoring Methodology

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

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

Only those Bidders scoring at least **160 marks out of 200** 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 bank at its own discretion may undertake reverse auction.

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) Vendor Registration

b) Publish 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
j) Reverse Auction with Qualified Bidders
k) Contract Award

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

M/s. e-Procurement Technologies Limited

B-705, Wall Street- II, Opp. Orient Club, Ellis Bridge, Near Gujarat College,

Ahmedabad- 380006, Gujarat

Help Desk:

Sandhya Vekariya – 6352631968

Suraj Gupta – 6352632310

Ijlalaehmad Pathan – 6352631902

Imran Sodagar – 9328931942

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 Name:	**Tender Fee/ Cost Account**
16-digit Account No	**9931530300000001**
Bank Name	The J&K Bank Ltd
Branch Name	Corporate Headquarters MA Road Srinagar J&K - 190001
IFSC Code	JAKA0HRDCHQ
Amount	INR 1,500/=

UTR Number may be uploaded on E-tendering portal

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 INR 5, 00,000 (Rupees Five Lakhs only).The Bank may accept Bank guarantee in lieu of EMD for an equivalent amount valid for 180 days from the last date of bid submission and issued by any scheduled commercial Bank acceptable to the 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	INR 5,00,000/=

In case of a Bank Guarantee from foreign Bank operating in India, prior permission of the Bank is essential. The format of Bank Guarantee is enclosed in Annexure G.

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 (PBG) for 5% of the total project cost and valid for 42 months including claim period of 6 (six) months, validity starting from its date of issuance. 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 successful bidder will furnish an unconditional performance bank guarantee for **5%** of the total project cost. The format of the PBG is given as per Annexure H .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 Successful 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 favor 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 Successful 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 Successful Bidder for its failure to complete its obligations under the contract. The Bank shall also be entitled to make recoveries from the Successful 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 Successful Bidder under the contract.

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. Price quoted by the Bidder in Reverse auction shall remain valid for duration of 6 calendar months from the date of conclusion of RA.

iii. 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

Payment will be made as per the milestones defined below:

Sr. #	Project Milestones	Payment Terms
01	Delivery and installation of software components supporting licenses.	30% of First year License cost

02	Go-Live, UAT Signoff, user and administrative Training.	70% of First year License cost.
03	Year 2 & 3 license	100% of the Annual Cost Payment post activation of Licenses.

Payment to be made subject to submission of 5% of PBG of the total Project Cost.

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

1. The Company 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 directly or indirectly 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 Company,
   iii. Breach of confidentiality obligations by the Company,
   iv. Negligence (including but not limited to any acts or omissions of the Company, its officers, principals or employees) or misconduct attributable to the Company 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 company.
   vii. Non-compliance by the Company with applicable Laws/Governmental/Regulatory Requirements.

   Provided however,

i. BANK notifies the Company in writing immediately on being aware of such claim,
ii. The Company has sole control of its defense and all related settlement negotiations.

The Company 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 Agreement.

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. The progress regarding execution of the contract, made by the selected Bidder is found to be unsatisfactory.
d. 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 abide by the terms of the contract which results in the termination of the contract, the Bank shall be entitled to claim liquidated damage equivalent to as total cost of contract as on date of happening of event which gives right to the Bank to seek liquidated damages from the Vendor for any loss which may occur to the Bank on account of non-performance, breach of terms and conditions including but not limited to negligence.

Fixed Price

The Commercial Offer shall be on a fixed price basis, inclusive of all taxes and levies. 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 Company/Service Provider(including its sub-contractors).The Company shall be subject to annual audit by internal/ external Auditors appointed by the Bank / inspecting official from the RBI or the persons authorized by RBI 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 company is required to submit such certification by such Auditors to the Bank

Company shall allow the Bank and RBI or persons authorized by it to access Bank documents, records or transactions or any other information given to, stored or processed by Company within a reasonable time failing which Company will be liable to pay any charges/ penalty levied by the Bank without prejudice to the other rights of the Bank. 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."

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, 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 three 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.

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.

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).

Resolution of Disputes and Arbitration clause

The Bank and the Successful 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 Successful bidder. If designated Officer of the Bank and representative of Successful bidder 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 Successful 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 Successful 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 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.

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

The Successful Bidder shall have to execute service level agreement for deliverables and successful execution of the projects to meet Banks requirement to its satisfaction. The Bank would stipulate strict penalty clauses for nonperformance or any failure in the implementation/efficient performance of the project. The Bidder should execute the Agreement within 15 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 successful 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/service specified
b) Installation and commissioning charges, if any,
c) Packing, Forwarding and Transportation charges up to the sites to be inclusive.
d) All taxes and levies and for Destinations.

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, 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 Bidder and its personnel shall not carry any written material, layout, diagrams, floppy diskettes, 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 Bidder's personnel shall follow J&K Bank's information security policy and instructions in this regard.

c. The 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 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 Bidder to protect its own proprietary information. Bidder recognizes that the goodwill of J&K Bank depends, among other things, upon the Bidder keeping such proprietary information confidential and that unauthorized disclosure of the same by Bidder could damage J&K Bank. By reason of Bidder's duties and obligations hereunder, Bidder may come into possession of such proprietary information, even though the 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. Bidder shall use such information only for the purpose of performing the Service(s) under the Contract/Agreement.

d. 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 Bidder by J&K Bank, including any copies or reproductions, both hardcopy and electronic.

e. That the Company 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 Company's and its subsidiaries' businesses. Without

limiting the foregoing, the Company 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 Company's and its subsidiaries' businesses.

f. The Bidder shall certify that to the knowledge of the 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 Bidder or its subsidiaries or of any data of the 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 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 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 Bidder confirms the compliance with Banks Supplier Security Policy.

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

j. That the 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 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 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 Bidder will notify Customer of breaches in 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 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. 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 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 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 Bidder for its own information or the information of its customers of a similar nature.

p. That the 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, 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 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 Bidder's audit. If Bank chooses to conduct its own security audit, such audit shall be at its own expense. Bidder shall promptly correct any deficiency found in a security audit.

r. That after providing 30 days prior notice to 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 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 Bidder's auditors, or the successors to their role in the event of a corporate reorganization, at Bidder's cost.

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 payments 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 terms of this RFP, the information provided by Bank herein and all other information provided by BIDDER in connection with the services offered to be provided by the BIDDER pursuant to this RFP, are to be treated by BIDDER as strictly confidential and proprietary. Such materials are to be used solely for the purpose of responding to this request. Access shall not be granted to third parties except upon prior consent of Bank and upon the written agreement of the intended recipient to treat the same as confidential. Bank may request at any time that any of Bank's material be returned or destroyed.

Sub-Contracting

The services offered to be undertaken in response to this RFP shall be undertaken to be provided by the BIDDER/ directly employing their employees, and there shall not be any sub-contracting without prior written consent from the Bank. All the resources deployed by the bidder should be on the bidder's payroll.

Reverse Auction

In order to reduce the time involved in the procurement process, Bank shall be entitled to complete the entire procurement process through a single Reverse Auction or in multiple Reverse Auctions The Bank shall however, be entitled to cancel the Reverse Auction process, if in its view procurement or Reverse Auction process cannot be conducted in a fair manner and / or in the interest of the Bank.

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.

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 Bidder in writing. The time for completion of the work will be extended suitably to account for duration of the suspension

Annexure A: Confirmation of Terms and Conditions

To

Chief Information Security Officer,
Information Security Department.
Corporate Headquarters

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

190 001 J&K.

Dear Sir,

Sub: RFP No …… For RFP FOR CLOUD SECURITY POSTURE MANAGEMENT & WORKLOAD PROTECTION date ……

Further to our proposal dated ……, in response to the Request for Proposal for selection of vendor for providing services for RFQ FOR CLOUD SECURITY POSTURE MANAGEMENT & WORKLOAD PROTECTION (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.
Corporate Headquarters

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

190 001 J&K.

Dear Sir,

Sub: RFP no: _____ for RFP FOR CLOUD SECURITY POSTURE MANAGEMENT & WORKLOAD PROTECTION dated _____

Having examined the tender documents including all annexures the receipt of which is hereby duly acknowledged, we, the undersigned, offer services for RFQ FOR CLOUD SECURITY POSTURE MANAGEMENT & WORKLOAD PROTECTION 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 including the conditions applicable to reverse auction proposed to be followed by the Bank.

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
1	The Bidder must be registered with Registrar of Companies / a Govt Organization/ PSU / PSE/ LLP or Private/ Public Limited Company in India.	Certificate of incorporation or any other certificate of registration issued by competent authority from Government of India
2	The Bidder should have been in existence in India for the last three years as on 31.03.2025. (DPIIT recognized start-ups exempted)	Copy of Certificate of Incorporation / Certificate of commencement of business.
3	The Bidder should have a minimum annual turnover of Rs. 50 Crores (Rupees) in each of the last three financial years viz. 2022-23, 2023-24 and 2024-25. (Micro and Small enterprises - MSEs and DPIIT recognized start-ups are exempted from this clause).	Audited Financial statements for the financial years 2022-23, 2023-24 and 2024-25 with CA Certificate for the said period

4	The Bidder should have positive net worth in each of the last 3 financial Year's viz. 2022-23, 2023-24 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 revenue expenditure + other intangible assets)	Audited Financial statements for the financial years 2022-23, 2023-24 and 2024-25. CA Certificate for the said period. The CA certificate should be without any conditions.
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	Bidders shall be the Original Equipment Manufacturers (OEM) of Solution (OR) an authorized Security Service Provider.	If the applicant is an OEM, an Undertaking Letter has to be submitted in this effect. If the bidder is an Authorized Dealer/Distributor, an Authorization letter from their OEM to deal/market their product in India and it should be valid at the time of submission of the Bid
8	The Bidder should have its own Service Centre/Office/ in India	Relevant Credential letters.
9	The proposed solution must be deployed in at least 1 PSU Bank and/or Private Banks in India, during last 3 years, and should be currently running successfully.	The bidder shall provide the details of contract which are still valid. Work Orders & Reference Letters of satisfactory Performance from the Clients as per format provided has to be submitted along with documentary proof. Purchase Order along with Email from the client containing all the required information. Kindly note that that Client's Email should be from their official Email IDs only, containing their name, designation & Mobile no

10	The proposed solution should have been in existence for at least 3 years or more.	Bidder should provide the purchase order copy or reference letter from their customer for the same.
11	The OEM or Bidder/ should be in business of development / Manufacturing / Selling Information Security products for the immediate preceding three years in India as on 31.03.2025.	Bidder should provide the purchase order copy or reference letter from their customer for the same.
12	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.
13.	The bidder or OEM should have a fully functional Customer Service Centre with 24/7 accessibility. The centralized trouble-ticketing tool for call logging, monitoring and troubleshooting purpose should have 24/7 access via a published number and email ID	Certificate containing the details
14.	Bidder and OEM must be an ISO 27001: 2022 or higher certified company.	ISO 27001: 2022 or higher certificate

Annexure E: Technical Bid Form

Apart from Scope mentioned in the RFP, he bidder will provide inputs in the table below on the basis of functionality available in the solution.

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 CLOUD SECURITY POSTURE MANAGEMENT & WORKLOAD PROTECTION.**

S No.	Technical Specification Cloud Security Platform	Marks	Compliance (Y/N)
	Cloud Security Posture Management & Workload Protection		
1	**Platform Requirement**		
1.1	The solution should be a Cloud Security Posture Management & Workload Protection tool which can integrate over API with multiple accounts. and multiple regions of in public cloud environment such as Amazon Web Services (AWS), Azure, Google Cloud Platform (GCP) and Oracle Cloud Infrastructure (OCI) with a single centralized console and generate improper network, misconfiguration, and compliance related alerts	1	
1.2	The solution must have a centralized asset inventory and Configuration Management Database (CMDB) of all cloud assets across various cloud environments such as Amazon Web Services (AWS), Azure, Google Cloud Platform (GCP) and Oracle Cloud Infrastructure (OCI)	1	
1.2.2	The solution must support cloud security posture assessment i.e. misconfiguration detection, compliance without any dependency on snapshot based agentless scanning.	1	
1.3	The Solution shall continuously discover and automatically classify cloud resources as soon as they are deployed.	1	
1.4	The Solution shall maintain full history of configuration changes over time for each cloud asset, to simplify compliance auditing and forensics. Should provide a quick diff/delta view of configuration add/delete/change for each cloud asset along with the line view.	1	
1.5	The solution shall provide the choice of agentless or agent-based deployment based on use cases.	1	
1.6	The solution shall support major cloud service providers including AWS, Google Cloud, Azure, OCI, IBM, Alibaba Cloud, IBM Cloud, etc.	1	

1.7	The solution shall leverage generative artificial intelligence (AI) for end users to ask any question about their environment and automate repetitive tasks.	1	
1.8	The solution must Identify the riskiest infrastructure resources exposure to Internet by combining misconfiguration, vulnerability, internet exposure, threats, anomalies, excessive permission, web and api related risks, data security risks to prioritize remediation effort.	1	
2	**Enforce Policy Governance**		
2.1	The Solution Should continually monitor all cloud resources for misconfigurations.	1	
2.2	The Solution Should provide out-of-box policies to check for security best practices for Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) configuration.	1	
2.3	The Solution shall provide ability to clone, customize, and run an existing policy	1	
2.4	The Solution shall have ability to enforce policy governance guardrails that can automatically trigger alerts for misconfigurations and configuration drift.	1	
2.5	The Solution shall have the ability to provide guided remediation details for issues detected out-of-the-box	1	
2.6	The Solution shall have the ability to auto-remediate infrastructure changes based on a specific policy requirement, without needing any external tools and functions.	1	
3	**Detecting Risks and Incidents and generating Alerting**		
3.1	The Solution shall have ability to detect and Alert on Risky Configurations: Provide facility to View configuration alerts in Graphical User Interface (GUI) Console and utilize tool to investigate the user activities that led to the misconfiguration.	1	
3.2	The Solution shall have ability to detect and Alert on Network Security: Check for unencrypted traffic, assets directly connected to the internet, compromised services, and traffic to and from suspicious IPs.	1	
3.3	The Solution Should have ability to detect and Alert on Sensitive Audit Actions Check report on sensitive user activities such as asset creation/deletion, security group changes, Identity Access Management (IAM) role changes and more.	1	
3.4	The Solution shall have ability to detect and Alert on Anomalous User Activities: Identify anomalous activities and provides guidance on how to take actions to prevent further incident.	1	
4	**Cloud Compliance & Reporting**		
4.1	The Solution shall provide a customizable view of entire compliance posture in compliance dashboard for all Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) services.	1	
4.2	The solution shall have the ability to automatically generate on demand reports of specific sets of controls and/or compliance for all Public Cloud Accounts	1	

4.3	The solution have the ability to report on compliance status for cloud infrastructure services as per: minimum compliance reporting for PCI DSS, CIS (AWS, Azure, GCP), RBI Baseline Cyber Security and Resilience Requirements, SEBI - Consolidated Cybersecurity and Cyber Resilience Framework (CSCRF), SOC 2, PCI DSS, NIST 800-53 Rev5, HIPAA, GDPR, ISO 27001, NIST CSF, MiTRE ATT&CK. Also should have option & ability to create custom compliance templates based on business requirements.	1	
4.4	The solution shall have the ability to export reports to PDF. Also, shall have built-in ability to schedule daily, Monthly and Weekly emailing of compliance PDF report to the required stakeholders.	1	
5	**Investigation capabilities**		
5.1	The Solution shall provide ability to perform ad hoc investigation for reviewing active resources and resource changes across the Purchaser's multi-cloud environment.	1	
5.2	The Solution shall have ability to ingest Cloud Configuration and allow to run ad hoc query and investigation on them	1	
5.3	The Solution shall have ability to ingest Cloud audit logs of privilege user activity and allow to run ad hoc query and investigation on them. Also, shall provide user activity and a Geo location details based on user login activity.	1	
5.4	The Solution shall have ability to ingest cloud flow logs from the cloud providers and allow to run ad hoc query and investigation on them. Also shall provide graph visualization of network flows to create a point in time the traffic flow in the Purchaser's cloud VPC.	1	
5.5	The solution shall support granular queries across any IAM policies and events for investigations.	1	
5.6	The solution shall provide option to explore IAM permissions, relationships, and events with an intuitive graph.	1	
6	**Integrations**		
6.1	The solution shall have the ability to send alerts via integrations with 3rd party solutions like Security Information Event Management, Security Orchestration Automation Response and Helpdesk/Ticketing Platforms	1	
6.2	The solution shall have the ability to ingest and display 3rd party host vulnerability and threat data from Vulnerability Assessment platforms (like Tenable Nessus, Qualys, etc), Cloud platforms.	1	
6.3	The solution shall have the ability to integrate with NIC's Single Sign On (SSO) solution and demonstrate user access for a valid user and deny for an invalid user.	1	
6.4	The solution shall have the ability to provide a fully supported Rest API for programmatic access to the tool, so that teams can take advantage of automating various tasks and reporting.	1	
7	**Cloud Network Traffic Analysis & Network anomaly detection**		
7.1	The solution shall have the ability to generate a snapshot in time visualization of network activity including auto classification of Suspicious IPs	1	
7.2	The Purchaser shall be able to automate Weekly, Monthly compliance report	1	

7.3	The solution shall have out-of-the-box security policies purpose- built to address threat vectors targeting public cloud environments, including detection of cloud-specific threats like crpytojacking activities.	1	
7.4	The solution shall detect unusual server port activity or unusual protocol activity from a client within or outside the Purchaser's cloud environment to a server host within or outside the Purchaser's network, using a server port or an IP protocol that is not typical to the Purchaser's network traffic flows.	1	
7.5	Network reconnaissance— The solution shall detect port scan or port sweep activities that probe a server or host for open ports.	1	
7.6	The solution shall identify hosts within the Purchaser's cloud environment that may be compromised and sending out spam.	1	
7.7	Detect anomaly such as but not limited to: - backdoor activity - botnet activity - cryptominer activity - DDoS activity - downloader activity - dropper activity - exploit kit activity - file infector activity - hacking tool activity - infostealer activity - Linux malware activity - loader activity - network data exfiltration activity - port scan activity - port sweep activity - ransomware activity - remote access trojan activity - rootkit activity - spambot activity - unusual protocol activity - unusual server port activity - webshell activity - wiper activity - worm activity	1	
8	**IAM Monitoring & User Entity Behaviour Analysis**		
8.1	The solution shall have ability to do Privileged activity monitoring and alert on unusual user activity—Discover insider threat and an account compromise using advanced data science. This shall be aided with profiling of a user's activities on the console, as well as the usage of access keys based on the location and the type of cloud resources.	1	
8.2	The solution shall have ability to do User and Entity Behaviour Analytics (UEBA) and alert on Excessive login failures—Detect potential account hijacking attempts discovered by identifying brute force login attempts. Excessive login failure attempts shall be evaluated dynamically based on the models observed with continuous learning.	1	

8.3	The solution shall have ability to detect Account compromise, insider threat detection, and monitoring and alert on account hijacking attempts-Detect potential account hijacking attempts discovered by identifying unusual login activities. These shall be based on concurrent login attempts made in short duration from two different geographic locations or login from a previously unknown browser, operating system, or location.	1	
8.4	Detect suspicious activity originating from The Onion Router (TOR) anonymity network to access resources related to services such as below that could lead to potentially malicious activities from the user: - AI / ML services - Analytics services - Application Integration services - Compute services - Containers services - Database services - Dev Tools services - IoT services - Media services - Migration services - Monitoring / Management services - Networking services - Security services - Storage services - Web services	1	
9	**Remediation**		
9.1	The solution shall provide alerts with detailed context with suggested remediation steps.	1	
9.2	The solution shall provide the ability to auto remediate misconfigurations and compliance violations from the console without needing any additional tools/functions.	1	
9.3	The solution shall Integrate with ticketing systems (e.g., Jira, Service Now, Slack) for alerting and remediation.	1	
9.4	The solution shall provide detailed remediation steps and automated remediation options for IAM permission and access alerts.	1	
10	**Agentless Workload Scanning**		
10.1	The solution shall provide option to scan hosts, containers, Kubernetes, and serverless workloads without deploying agents. Agentless scanning shall: - Detect vulnerabilities in workloads and images. - Detect configuration risks and compliance violations in workloads. - Detect malware in workloads. - Detect secrets hidden in plain sight within running and non-running workloads	1	
10.2	The solution shall scan workloads in runtime across multicloud environments (AWS, Azure, GCP, OCI).	1	
10.3	The solution shall scan virtual machines and host OS architectures (Linux, Windows).	1	
10.4	The solution shall scan container architectures (Docker, Kubernetes, OpenShift, Red Hat).	1	

10.5	The shall scan Kubernetes architectures, including managed Kubernetes services (e.g., Amazon EKS, Google GKE, Azure Container Service).	1	
10.6	The solution shall scan container images before they're deployed inside container registry and CI/CD pipelines.	1	
10.7	The solution shall scan serverless architectures (Amazon Lambda, Azure Functions, Google Cloud Functions).	1	
10.8	The solution shall detect sensitive information that is improperly secured inside host and container images such as embedded passwords, login tokens, and other types of secrets.	1	
	Manage Cloud Identity, Permission and Access		
11	**Entitlement Discovery**		
11.1	The solution shall discover both human and machine identities as well as entitlements across cloud providers.	1	
11.2	The solution should discover accurate net-effective cloud identity entitlements of machine and users to gain clear visibility and actionable insight for cloud identities across clouds through visualized graph and table views.	1	
11.2	Must provide the capability to visualise the relationship between roles and resources that access has been granted in either a graph or table view	1	
11.3	The solution should support integration with IdP services such as Okta, Azure AD,etc to gain comprehensive and complete cloud identity visibility across multi-cloud environments.	1	
12	**Policy and Governance**		
12.1	The solution shall provide out-of-the-box policies to identify risky permissions and remove unwanted access.	1	
12.2	The solution must provide the ability to create customizable policies for specific IAM issues within an organization.	1	
12.3	The solution shall automatically Identify IAM policies that enable public data exposure, privilege escalation, and lateral movement.	1	
12.4	The solution shall identify workloads with permissions to create new users, roles, and groups.	1	
12.5	The solution shall automatically detect identity threats such as account compromise, insider threats, and other malicious activity.	1	
12.6	The solution shall provide option to apply user and entity behaviour analytics (UEBA) to detect anomalous behaviours.	1	
	CLOUD WORKLOAD PROTECTION (CWP) for Cloud Native Workload Security		
1	**General**		
1.1	The solution should be deployed as a minimal agent on the cloud workloads such as VMs, Containers and Serverless to provide asked security features to the workloads and should provide a unified workload protection framework to protect cloud native applications across different environments such as cloud managed Kubernetes platform, self-operated Kubernetes platform, OpenShift and etc	1	

1.2	The solution must provide a defence-in-depth approach to protect the host-VMs, Containers and Serverless functions across their lifecycle by using continuous vulnerability management, compliance checking, runtime defence and cloud native Web Application security	1	
1.3	Should generate a GUI based dynamically generated map showing all the inter VM, inter containers, serverless and inter process communication and function level interface with other services in the cloud environment.	1	
1.4	The solution must support workloads (hosts, containers and kubernetes) running either on public cloud like AWS, Azure, GCP, OCI and On-premise datacentre.	1	
1.5	The solution should provide for grouping of the containers by Cluster and namespaces in the map	1	
1.6	Maps for VMs, Containers and Serverless should color-coded the objects on the map to show vulnerability status, compliance status and runtime state such that the security posture of the application is instantly obtained	1	
1.7	The sensors should run only a single instance of the agent on each VM and Kubernetes/Dockers worker node without adding any files or binaries to the containers being protected	1	
1.8	The platform should display the security status of existing running containers and container hosts according to their risk level in a dashboard immediately after installation. This should include existing vulnerabilities and malware as well as the insecure container or container host configurations.	1	
1.9	The Bidder should have the OEM Certifications of the solution	3	
1.10	The Bidder should have the required professional experience of implementing the solution in various Banks	3	
1.11	Technical Presentation/Demo by the Bidder	12	
2	**Vulnerability Management**		
2.1	The solution should provide flexibility to choose between agentless and agent-based security for cloud native workload (host, containers and Serverless) vulnerability and compliance management across AWS, Azure, GCP and Oracle Cloud.	1	
2.2	Should perform continuous vulnerability management across all types of workloads such as VM, Container and Serverless environment including the registry and repository for the same.	1	
2.3	The solution should support vulnerability detection across the OS layer, application framework and custom packages and The agent should be able to scan the host operating system on which the containers are running and provide details of all known vulnerabilities	1	

2.4	The solution should report the result of vulnerability scan done in CI/CD tools on the centralized console and must allow definition of policies to alert and block severe vulnerabilities from moving forward in the development pipeline	1	
2.5	Should highlight risk factors introduced by each vulnerability and utilize behavioural metrics about current runtime environment to assign risk score to vulnerabilities such that vulnerabilities with highest risk can be identified	1	
2.6	Should be able to also take information from runtime environments and correlate vulnerability risk to them and provide risk score for top vulnerabilities in the production, UAT environment	1	
2.7	The solution should support vulnerability detection across the OS layer, application framework and custom packages and The agent should be able to scan the host operating system on which the containers are running and provide details of all known vulnerabilities	1	
2.8	Should Provide layer by layer vulnerability analysis and pinpoints vulnerability data at each container image layer.	1	
2.9	Should allow definition of policies for admission control to stop images not matching the corporate vulnerability polices from being run in production environment	1	
2.10	Should provide flexibility to apply different policies to different images based on container name, image name, host name and labels	1	
2.11	Should provide plugin and command-line interface for integrating with Jenkins and other CI/CD tools such that vulnerability scan can be performed during the build process	1	
2.12	The solution should have pre-built templates for HIPAA, PCI, GDPR, and NIST SP 800-190, along with 400+ certified checks for the AWS, Dockers, Kubernetes, and Linux CIS Benchmarks	1	
2.13	The solution should provide for at least 400 out of box checks for hardening and compliance checks of the cloud environment	1	
2.14	The solution must support for custom compliance checks via OpenSCAP, XCCDF, and Bash scripts	1	
2.15	The solution should allow for creation of TRUST policy to allow, by policy, which registries, repositories, and images to trust, and stop images from running if they are deemed non trusted	1	
2.16	The solution must allow definition of policies to not just alert non-compliance but also enforce the recommendations of selected compliance checks	1	
2.17	Granular policy controls prevent unauthorized images from progressing through the CICD pipeline	1	
3	**Runtime environment protection**		
3.1	The solution should be able to learn the behaviour of each running container workloads and build runtime model automatically	1	
3.2	The solution should provide visibility in the terms of processes running, ports being listened, outbound connections made, domain names lookup by DNS and file system access	1	
3.3	The solution should update runtime model of workloads automatically for new application releases	1	

3.4	The solution should detect anomalies in running workloads based on automatically generated runtime models on processes, network activities and file system access	1	
3.5	The solution must block suspicious activities based on runtime model learned, malware database and advanced threat protection feeds	1	
3.6	The solution must store forensic data as part of any security incident and displays the incident, kill chain, and data timeline for seamless incident response	1	
3.7	The solution must should have host OS behaviour modelling capabilities using the process and file system actions that understands the tasks that OS services need to do as a baseline.	1	
3.8	The solution must provide File Integrity monitoring Monitor files and directories against read, write, and metadata changes with alert and prevent capabilities.	1	
3.9	The solution must provide behavioural-based anomaly detection - host intrusion detection and protection for the underlying host OS.	1	
3.10	The solution should provide host and container forensics capabilities to help after action analysis of host system behaviours to determine the sequence of events that lead to an incident.	1	
3.11	The solution should provide Incident forensics, logging with alert to simplify SOC Incident Response	1	
3.12	The platform should have the ability to fine-tune runtime policy to reduce noisy false positives and compatibility to enforce policy for Alert, Block and Kill.	1	
3.13	The platform should have the ability to fine-tune runtime policy by adding threat-based active protection such as malware detection, crypto miners, reverse shell attacks, port scanning etc. to reduce noisy false positives and compatibility to enforce policy for Alert, Block and Kill.	1	
4	**Network Security features**		
4.1	The solution must perform zero-touch machine learning to automatically build network topology across hosts, containers, and serverless apps	1	
4.2	The solution must learn new communication patterns across workloads automatically for new application releases	1	
4.3	The solution must provide Layer 7: Application protection to protect workloads against known and unknown threats including but not limited to SQL injection, brute force attacks, click jacking, shellshock, information leakage and etc.	1	
4.4	The solution should discover API endpoints for granular visibility on deployed cloud assets and API Gateways.	1	
4.5	The tool should perform API risk profiling to identify API risk factors, sources of risk, vulnerabilities and changes to prioritize remediation or protection.	1	
4.6	The solution should detect, alert & block Web and API attacks in real time on hosts, containers, kubernetes and serverless deployments to prevent breaches.	1	
4.7	The solution should detect, alert & block OWASP Top 10 Web Attacks in real time to prevent breaches	1	

4.8	The solution should have the ability to provide a risk assessment for API definitions to determine risky and insecure APIs.	1	
5	**Quality Gate and Trusted Image enforcement for container going in to Production Clusters**		
5.1	The tool must dynamically analyse the runtime behaviour of image in an on-prim sandbox environment before running them in your development and production environments.	1	
5.2	The Solution should prevent container being deployed on kubernetes cluster/worker Nodes, if container image does not meet the minimum defined vulnerability criteria without relying on CI-CD tools or on Kubernetes access control to prevent malicious containers to run on worker nodes.	1	
5.3	The Solution should prevent container being deployed on kubernetes cluster/worker Nodes, if container image has Compliance issue. Example:: Sensitive info is embedded in environment variables, Private keys stored in Image, Image is created with a root user. Etc. This should be achieved without relying on CI-CD tools or on Kubernetes access control.	1	
5.4	The Solution should have ability to prevent container being deployed on kubernetes cluster if container image is not prequalified as TRUSTED IMAGE. The tool should be able to create TRUSTED IMAGE policy based on (a) Trusted Repos (b)Trusted Base Images (c)Manually qualified images etc. And the tool should have ability to alert and/or block deployment when container don't meet the TRUSTED IMAGE policy without relying on CI-CD tools or on Kubernetes access control.	1	
6	**Container image sandbox analysis**		
6.1	The solution should dynamically scan container images in a sandbox to detect suspicious activities like malware and port scanning and provide a detailed runtime behaviour profile to prevent malicious images from deployment into runtime	1	
6.2	Capability to scan and sandbox container images upon download from 3rd parties to analyse prior to developing apps on it. - Malicious Behaviour i.e. malware, crypto miners and outbound C2C. - Understand behaviour of container image i.e. process/file system calls	1	
7	**Architecture and Integration**		
7.1	The solution should be provided as a SaaS or on-premise software tool with support for VMs and Kubernetes/container in AWS, Azure, and GCP cloud environments. It should provide flexibility of securing cloud native software stacks on Openshift, Kubernetes, and Tanzu container environment.	1	
7.2	The solution should have extensive logging and telemetry capability	1	
7.3	The solution should have extensive API capability and should offer all the above features as and API	1	
7.4	The solution must have an intuitive UI to provide rapid forensics and investigative capabilities.	1	
7.5	The solution must integrate with Active Directory, OpenLDAP, and SAML	1	
7.6	The solution must have Alerting integration with developer and operations tools like Jira, Slack, Pager duty, SOAR platforms	1	
	Cloud Code Security		

1	**Infrastructure as code**		
1.1	The solution must Identify misconfigurations in IAC files and present developer friendly suggestions and fixes via native IDE, VCS (Git) & CI/CD plugins to prevent misconfigured resources from deployment into runtime	1	
1.2	Tool must have the capability to scan a wide array of IAC templates i.e. TFT (HCL format), CFT (JSON / YAML), ARM, Helm, Dockerfiles, Swagger, Kubernetes App manifest (JSON/YAML), BICEP and others and where possible automated remediation actions	1	
1.3	Must be able to detect and scan existing IAC templates in Git repos i.e. GitHub, Gitlab, BitBucket, Azure Repos etc.	1	
1.4	Must be able to detect and scan existing IAC mis-configurations in pull request/merge request	1	
1.5	Must be able to visualise the relationships between code elements i.e. IAC and Packages to determine relationships and dependencies	1	
1.6	The tool must have the capability to integrate with DevOps tooling and workflows i.e. IDE, CI workflows and GitOps workflows	1	
1.7	Platform supports scanning of secrets, detect secrets in IDEs, Git-based VCS, and CI/CD executions.	1	
1.8	Must be able to natively report results within Developer workflow tools i.e. Git (Github, Gitlab etc), IDE tools and CI tooling as well as ad hoc usage via the CMD.	1	
1.9	Capability to define code custom policies in addition to out of the box policies that can be cloned.	1	
2	**Software Composition Analysis (SCA)**		
2.1	The solution detect and prevent critical open source vulnerabilities from being deployed in direct & transitive dependencies with clear, automated fixes and blocking via native IDE, VCS or CI/CD plugins	1	
2.2	Must have the capability to perform SCA for a wide range of package managers i.e. Docker, Go, Java (Maven/Gradle) Javascript (NPM, Yarn, Bower) Kotlin (Gradle) Python (Pip, Pipfile), Ruby and YAML	1	
2.3	The solution support vulnerability scanning based on CVE's and return detailed information on each vulnerability i.e. CVE ID, CVSS score, Package Name, Version, Attack Vector, Public POC, Exploit in the Wild and whether a fix is available	1	
2.4	Must be able to provide the capability to bump fix packages	1	
2.5	Must list and map all packages and their dependencies, also visualise where possible as a supply chain with dependencies	1	
2.6	Must provide scanning for licensing compliance violations and non-compliance	1	
2.7	Must be able to scan existing repos for code based vulnerability and compliance issues.	1	
2.8	Must be able to scan packages as changes and modifications are raised via Pull and Merge request	1	
2.9	Ability to generate Software Bill of Materials (SBOM) and output in industry standard formats i.e. Cyclone DX XML and CSV	1	

	Total	160	

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

Part B

Sr. No.	**Evaluation category**	**Evaluation criteria**	**Scoring Logic**	**Criteria Weightage**
01	Solution Implementation and Service Experience in the BFSI or Technology Organization	A. Number of years' Experience in providing and successful implementation of the similar platform / solution to the clientele. B. Experience in terms of completed number of projects	a. 1 Years – 2 Marks 2 years -5 Marks >= 3 Years – 10 Marks 1 project- 5 marks 2 Projects – 10 Marks >=3 Projects -15 Marks	25 Marks
03	Resource Profile	No. of OEM Certified Engineers / Resources having 03 years or above of experience in implementing and transition support	1-2 Personnel – 5 Marks 3-5 Personnel – 10 Marks > 5 Personnel – 15 Marks	15 Marks

Total Marks including Part A and Part B	**200 Marks**

Signature and Seal of Company

Annexure F: Commercial Bid Format

1. 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.

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

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

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

S. No.	Item Details	Quantity	Unit Cost for Each	Year Cost (Rs)			Total Cost for 3 Years (Rs)	Method of Consumption
				First Year	Second Year	Third Year		
1	CSPM Solution bundled with License Cost, Implementation Cost and ATS (Annual Technical Support).	100						To be billed post activation

****Taxes shall be extra as applicable.**

Note:

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.

The license must be interchangeable between the Workloads, Containers, Serverless, LAMBDHA, FARGATE etc.

a. For each of the above items provided the bidder is required to provide the cost for every line item where the bidder has considered the cost in BOM.
b. 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.
c. 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.
d. All Deliverables to be supplied as per RFP requirements provided in the tender
e. The Service Charges need to include all services and other requirement as mentioned in the RFP

f. The bidder has to make sure all the arithmetical calculations are accurate. Bank will not be held responsible for any incorrect calculations however for the purpose of calculation Bank will take the corrected figures / cost.
g. All prices 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. The Bidder is expected to provide the GST amount and GST percentage in both the commercial and masked bids (without amounts being submitted in the technical response).
i. There will be no price escalation for during the contract period and any extension thereof. Bid submitted with an adjustable price quotation will be treated as non-responsive and will be rejected.
j. **Details to be provided for any commercial provided against "Any Other Charges". Bank have discretion to mark these line items as optional if Bank feels these items are not mandatory for the project. Cost of any other charges will be consider for TCO calculation purpose however Bank will place order for these items at Bank's discretion as per requirement.
k. If any of the milestone is part of the scope and not coved under commercial bid format then bidder have to provide the same in commercial bid format against any other charges as milestone wise separate line items.

l. 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.

m. Bidder is required to factor/provide Hardware / Software Infrastructure under this project.

Signature with Seal

Date:
Name:
Designation:

Annexure G: Bank Guarantee Format

Bank Guarantee No: _____
Dated:_____
Bank:_____

To

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

Chief Information Security Officer,

Information Security Department.
Corporate Headquarters

190 001 J&K.

WHEREAS..... (Company Name) registered under the Companies Act 1956 and having its Registered Office at..... India (hereinafter referred to as "the bidder") proposes to RFP and offer in response to RFP No. ....., dated .....for RFP for selection of vendor for..... (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 SI/OEM 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 bidder 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;

    i. our liability under this Guarantee shall not exceed Rs.....(Rupees.....only) ;
    ii. this Bank Guarantee shall be valid up to and including the date ..... ; 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.

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,

Chief Information Security Officer,
Information Security Department.
Corporate Headquarters

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 due 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)

Mutual Non-disclosure Agreement

THIS MUTUAL NONDISCLOSURE AGREEMENT (the "Agreement") is made and entered into as of (DD/MM/YYYY) by and between _____, a company incorporated under the laws of India , having its registered address at _____ (the "Company") and "The Jammu and Kashmir Bank Ltd, a Banking Company under 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 Licensee which unless the context requires include its successors in interests and permitted assigns). (the"Recipient").

1. Purpose J&K Bank has engaged or wishes to engage the company 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 is 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 "AS IS." Each 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.

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 for a period of from the date hereof.

10. Adherence. The content of the agreement is subject to adherence audit by J&K Bank. It shall be the responsibility of the Company 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.

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 for .... and designated representative of the Bidder. If designated Officer of the Bank for ....and representative of Bidder 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 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.

13. Miscellaneous. This Agreement shall bind and injure to 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".

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.

Annexure J: Service Level Agreement.

This Service Level agreement ("Agreement") is made at Srinagar (J&K) on this …….day of …….2020 ("effective date") between

i. "The Jammu and Kashmir Bank Ltd, a Banking Company under 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 Licensee 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 ……

COMPANY NAME	RECIPIENT
By:_____	By:_____
Name: _____	Name: _____
Title: _____	Title: _____
Address:_____	Address:_____
_____	_____
Company Seal	Company Seal

(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
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, 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

To be added here, once scope is finalized.

1. **Platform Requirement**
   i. The solution should be a Cloud Security Posture Management & Workload Protection tool which can integrate over API with multiple accounts. and multiple regions of in public cloud environment such as Amazon Web Services (AWS), Azure, Google Cloud Platform (GCP) and Oracle Cloud Infrastructure (OCI) with a single centralized console and generate improper network, misconfiguration, and compliance related alerts.
   ii. The solution must support cloud security posture assessment i.e. misconfiguration detection, compliance without any dependency on snapshot based agentless scanning.

iii. The solution must have a centralized asset inventory and Configuration Management Database (CMDB) of all cloud assets across various cloud environments such as Amazon Web Services (AWS), Azure, Google Cloud Platform (GCP) and Oracle Cloud Infrastructure (OCI)
iv. The Solution shall continuously discover and automatically classify cloud resources as soon as they are deployed.
v. The Solution shall maintain full history of configuration changes over time for each cloud asset, to simplify compliance auditing and forensics. Should provide a quick diff/delta view of configuration add/delete/change for each cloud asset along with the line view.
vi. The solution shall provide the choice of agentless or agent-based deployment based on use cases.
vii. The solution shall support major cloud service providers including AWS, Google Cloud, Azure, OCI, IBM, Alibaba Cloud, IBM Cloud, etc.
viii. The solution shall leverage generative artificial intelligence (AI) for end users to ask any question about their environment and automate repetitive tasks.
ix. The solution must identify the riskiest infrastructure resources exposure to Internet by combining misconfiguration, vulnerability, internet exposure, threats, anomalies, excessive permission, web and api related risks, data security risks to prioritize remediation effort.

2. Enforce Policy Governance

i. The Solution should continually monitor all cloud resources for misconfigurations.
ii. The Solution should provide out-of-box policies to check for security best practices for Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) configuration.
iii. The Solution shall provide ability to clone, customize, and run an existing policy
iv. The Solution shall have ability to enforce policy governance guardrails that can automatically trigger alerts for misconfigurations and configuration drift.
v. The Solution shall have the ability to provide guided remediation details for issues detected out-of-the-box
vi. The Solution shall have the ability to auto-remediate infrastructure changes based on a specific policy requirement, without needing any external tools and functions.

3. Detecting Risks and Incidents and generating Alerting

i. The Solution shall have ability to detect and Alert on Risky Configurations:
ii. Provide facility to View configuration alerts in Graphical User Interface (GUI) Console and utilize tool to investigate the user activities that led to the misconfiguration.
iii. The Solution shall have ability to detect and Alert on Network Security:
iv. Check for unencrypted traffic, assets directly connected to the internet, compromised services, and traffic to and from suspicious IPs.
v. The Solution Should have ability to detect and Alert on Sensitive Audit Actions

vi. Check report on sensitive user activities such as asset creation/deletion, security group changes, Identity Access Management (IAM) role changes and more.
vii. The Solution shall have ability to detect and Alert on Anomalous User Activities:
viii. Identify anomalous activities and provides guidance on how to take actions to prevent further incident.

4. **Cloud Compliance & Reporting**
   i. The Solution shall provide a customizable view of entire compliance posture in compliance dashboard for all Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) services.
   ii. The solution shall have the ability to automatically generate on demand reports of specific sets of controls and/or compliance for all Public Cloud Accounts
   iii. The solution have the ability to report on compliance status for cloud infrastructure services as per: minimum compliance reporting for PCI DSS, CIS (AWS, Azure, GCP), RBI Baseline Cyber Security and Resilience Requirements, SEBI - Consolidated Cybersecurity and Cyber Resilience Framework (CSCRF), SOC 2, PCI DSS, NIST 800-53 Rev5, HIPAA, GDPR, ISO 27001, NIST CSF, MiTRE ATT&CK. Also should have option & ability to create custom compliance templates based on business requirements.
   iv. The solution shall have the ability to export reports to PDF. Also, shall have built-in ability to schedule daily, Monthly and weekly emailing of compliance PDF report to the required stakeholders.

5. Investigation capabilities
   i. The Solution shall provide ability to perform ad hoc investigation for reviewing active resources and resource changes across the Purchaser's multi-cloud environment.
   ii. The Solution shall have ability to ingest Cloud Configuration and allow to run ad hoc query and investigation on them
   iii. The Solution shall have ability to ingest Cloud audit logs of privilege user activity and allow to run ad hoc query and investigation on them. Also, shall provide user activity and a Geolocation details based on user login activity.
   iv. The Solution shall have ability to ingest cloud flow logs from the cloud providers and allow to run ad hoc query and investigation on them. Also shall provide graph visualization of network flows to create a point in time the traffic flow in the Purchaser's cloud VPC.
   v. The solution shall support granular queries across any IAM policies and events for investigations.
   vi. The solution shall provide option to explore IAM permissions, relationships, and events with an intuitive graph.

6. **Integrations**

i. The solution shall have the ability to send alerts via integrations with 3rd party solutions like Security Information Event Management, Security Orchestration Automation Response and Helpdesk/Ticketing Platforms
ii. The solution shall have the ability to ingest and display 3rd party host vulnerability and threat data from Vulnerability Assessment platforms (like Tenable Nessus, Qualys,etc), Cloud platforms.
iii. The solution shall have the ability to integrate with NIC's Single Sign On (SSO) solution and demonstrate user access for a valid user and deny for an invalid user.
iv. The solution shall have the ability to provide a fully supported Rest API for programmatic access to the tool, so that teams can take advantage of automating various tasks and reporting.

7. Cloud Network Traffic Analysis & Network anomaly detection

i. The solution shall have the ability to generate a snapshot in time visualization of network activity including auto classification of Suspicious IPs
ii. The Purchaser shall be able to automate Weekly, Monthly compliance report
iii. The solution shall have out-of-the-box security policies purpose- built to address threat vectors targeting public cloud environments, including detection of cloud-specific threats like crpytojacking activities.
iv. The solution shall detect unusual server port activity or unusual protocol activity from a client within or outside the Purchaser's cloud environment to a server host within or outside the Purchaser's network, using a server port or an IP protocol that is not typical to the Purchaser's network traffic flows.
v. Network reconnaissance - The solution shall detect port scan or port sweep activities that probe a server or host for open ports.
vi. The solution shall identify hosts within the Purchaser's cloud environment that may be compromised and sending out spam.
vii. Detect anomaly such as but not limited to:

- backdoor activity
- botnet activity
- cryptominer activity
- DDoS activity
- downloader activity
- dropper activity
- exploit kit activity
- file infector activity
- hacking tool activity

- infostealer activity
- Linux malware activity
- loader activity
- network data exfiltration activity
- port scan activity
- port sweep activity
- ransomware activity
- remote access trojan activity
- rootkit activity
- spambot activity
- unusual protocol activity
- unusual server port activity
- webshell activity
- wiper activity
- worm activity

8. IAM Monitoring & User Entity Behavior Analysis

i. The solution shall have ability to do Privileged activity monitoring and alert on unusual user activity—Discover insider threat and an account compromise using advanced data science. This shall be aided with profiling of a user's activities on the console, as well as the usage of access keys based on the location and the type of cloud resources.

ii. The solution shall have ability to do User and Entity Behavior Analytics (UEBA) and alert on Excessive login failures—Detect potential account hijacking attempts discovered by identifying brute force login attempts. Excessive login failure attempts shall be evaluated dynamically based on the models observed with continuous learning.

iii. The solution shall have ability to detect Account compromise, insider threat detection, and monitoring and alert on account hijacking attempts-Detect potential account hijacking attempts discovered by identifying unusual login activities. These shall be based on concurrent login attempts made in short duration from two different geographic locations or login from a previously unknown browser, operating system, or location.

iv. Detect suspicious activity originating from The Onion Router (TOR) anonymity network to access resources related to services such as below that could lead to potentially malicious activities from the user:

- AI / ML services

- Analytics services
- Application Integration services
- Compute services
- Containers services
- Database services
- Dev Tools services
- IoT services
- Media services
- Migration services
- Monitoring / Management services
- Networking services
- Security services
- Storage services
- Web services

9. Remediation

i. The solution shall provide alerts with detailed context with suggested remediation steps.

ii. The solution shall provide the ability to auto remediate misconfigurations and compliance violations from the console without needing any additional tools/functions.

iii. The solution shall integrate with ticketing systems (e.g., Jira, ServiceNow, Slack) for alerting and remediation.

iv. The solution shall provide detailed remediation steps and automated remediation options for IAM permission and access alerts.

10. Agentless Workload Scanning

i. The solution shall provide option to scan hosts, containers, Kubernetes, and serverless workloads without deploying agents. Agentless scanning shall:

- Detect vulnerabilities in workloads and images.
- Detect configuration risks and compliance violations in workloads.
- Detect malware in workloads.
- Detect secrets hidden in plain sight within running and non-running workloads

ii. The solution shall scan workloads in runtime across multicloud environments (AWS, Azure, GCP, OCI).
iii. The solution shall scan virtual machines and host OS architectures (Linux, Windows).
iv. The solution shall scan container architectures (Docker, Kubernetes, OpenShift, Red Hat).
v. The solution shall scan Kubernetes architectures, including managed Kubernetes services (e.g., Amazon EKS, Google GKE, Azure Container Service).
vi. The solution shall scan container images before they're deployed inside container registry and CI/CD pipelines.
vii. The solution shall scan serverless architectures (Amazon Lambda, Azure Functions, Google Cloud Functions).
viii. The solution shall detect sensitive information that is improperly secured inside host and container images such as embedded passwords, login tokens, and other types of secrets.

11. Manage Cloud Identity, Permission and Access Entitlement Discovery

i. The solution shall discover both human and machine identities as well as entitlements across cloud providers.
ii. The solution should discover accurate net-effective cloud identity entitlements of machine and users to gain clear visibility and actionable insight for cloud identities across clouds through visualized graph and table views.
iii. Must provide the capability to visualize the relationship between roles and resources that access has been granted in either a graph or table view
iv. The solution should support integration with IdP services such as Okta, Azure AD,etc to gain comprehensive and complete cloud identity visibility across multi-cloud environments.

12. Policy and Governance

i. The solution shall provide out-of-the-box policies to identify risky permissions and remove unwanted access.
ii. The solution must provide the ability to create customizable policies for specific IAM issues within an organization.
iii. The solution shall automatically Identify IAM policies that enable public data exposure, privilege escalation, and lateral movement.
iv. The solution shall identify workloads with permissions to create new users, roles, and groups.
v. The solution shall automatically detect identity threats such as account compromise, insider threats, and other malicious activity.
vi. The solution shall provide option to apply user and entity behavior analytics (UEBA) to detect anomalous behaviors.

CLOUD WORKLOAD PROTECTION (CWP) for Cloud Native Workload Security

8. General

i. The solution should be deployed as a minimal agent on the cloud workloads such as VMs, Containers and Serverless to provide asked security features to the workloads and should provide a unified workload protection framework to protect cloud native applications across different environments such as cloud managed Kubernetes platform, self-operated Kubernetes platform, OpenShift and etc

ii. The solution must provide a defense-in-depth approach to protect the host-VMs, Containers and Serverless functions across their lifecycle by using continuous vulnerability management, compliance checking, runtime defense and cloud native Web Application security

iii. Should generate a GUI based dynamically generated map showing all the inter VM, inter containers, serverless and inter process communication and function level interface with other services in the cloud environment..

iv. The solution must support workloads (hosts, containers and kubernetes) running either on public cloud like AWS, Azure, GCP, OCI and On-premise datacenter.

v. The solution should provide for grouping of the containers by Cluster and namespaces in the map

vi. Maps for VMs, Containers and Serverless should color-code the objects on the map to show vulnerability status, compliance status and runtime state such that the security posture of the application is instantly obtained

vii. The sensors should run only a single instance of the agent on each VM and Kubernetes/Dockers worker node without adding any files or binaries to the containers being protected

viii. The platform should display the security status of existing running containers and container hosts according to their risk level in a dashboard immediately after installation. This should include existing vulnerabilities and malware as well as the insecure container or container host configurations.

9. Vulnerability Management

i. The solution should provide flexibility to choose between agentless and agent-based security for cloud native workload (host, containers and Serverless) vulnerability and compliance management across AWS, Azure, GCP and Oracle Cloud.

ii. Should perform continuous vulnerability management across all types of workloads such as VM, Container and Serverless environment including the registry and repository for the same.

iii. The solution should support vulnerability detection across the OS layer, application framework and custom packages and The agent should be able to scan the host operating system on which the containers are running and provide details of all known vulnerabilities

iv. The solution should report the result of vulnerability scan done in CI/CD tools on the centralized console and must allow definition of policies to alert and block severe vulnerabilities from moving forward in the development pipeline

v. Should highlight risk factors introduced by each vulnerability and utilize behavioral metrics about current runtime environment to assign risk score to vulnerabilities such that vulnerabilities with highest risk can be identified
vi. Should be able to also take information from runtime environments and correlate vulnerability risk to them and provide risk score for top vulnerabilities in the production, UAT environment
vii. The solution should support vulnerability detection across the OS layer, application framework and custom packages and The agent should be able to scan the host operating system on which the containers are running and provide details of all known vulnerabilities
viii. Should provide layer by layer vulnerability analysis and pinpoints vulnerability data at each container image layer.
ix. Should allow definition of policies for admission control to stop images not matching the corporate vulnerability polices from being run in production environment
x. Should provide flexibility to apply different policies to different images based on container name, image name, host name and labels
xi. Should provide plugin and command-line interface for integrating with Jenkins and other CI/CD tools such that vulnerability scan can be performed during the build process.
xii. The solution should have pre-built templates for HIPAA, PCI, GDPR, and NIST SP 800-190, along with 400+ certified checks for the AWS, Dockers, Kubernetes, and Linux CIS Benchmarks
xiii. The solution should provide for at least 400 out of box checks for hardening and compliance checks of the cloud environment
xiv. The solution must support for custom compliance checks via OpenSCAP, XCCDF, and Bash scripts
xv. The solution should allow for creation of TRUST policy to allow, by policy, which registries, repositories, and images to trust, and stop images from running if they are deemed non trusted
xvi. The solution must allow definition of policies to not just alert non-compliance but also enforce the recommendations of selected compliance checks
xvii. Granular policy controls prevent unauthorized images from progressing through the CICD pipeline

10. Runtime environment protection

i. The solution should be able to learn the behavior of each running container workloads and build runtime model automatically
ii. The solution should provide visibility in the terms of processes running, ports being listened, outbound connections made, domain names lookup by DNS and file system access
iii. The solution should update runtime model of workloads automatically for new application releases

iv. The solution should detect anomalies in running workloads based on automatically generated runtime models on processes, network activities and file system access
v. The solution must block suspicious activities based on runtime model learned, malware database and advanced threat protection feeds
vi. The solution must store forensic data as part of any security incident and displays the incident, kill chain, and data timeline for seamless incident response
vii. The solution must should have host OS behavior modelling capabilities using the process and file system actions that understands the tasks that OS services need to do as a baseline.
viii. The solution must provide File Integrity monitoring Monitor files and directories against read, write, and metadata changes with alert and prevent capabilities.
ix. The solution must provide behavioral-based anomaly detection - host intrusion detection and protection for the underlying host OS.
x. The solution should provide host and container forensics capabilities to help after action analysis of host system behaviors to determine the sequence of events that lead to an incident.
xi. The solution should provide Incident forensics, logging with alert to simplify SOC Incident Response
xii. The platform should have the ability to fine-tune runtime policy to reduce noisy false positives and compatibility to enforce policy for Alert, Block and Kill.
xiii. The platform should have the ability to fine-tune runtime policy by adding threat-based active protection such as malware detection, crypto miners, reverse shell attacks, port scanning etc. to reduce noisy false positives and compatibility to enforce policy for Alert, Block and Kill.

11. Network Security features

i. The solution must perform zero-touch machine learning to automatically build network topology across hosts, containers, and serverless apps
ii. The solution must learn new communication patterns across workloads automatically for new application releases
iii. The solution must provide Layer 7: Application protection to protect workloads against known and unknown threats including but not limited to SQL injection, brute force attacks, click jacking, shellshock, information leakage and etc.
iv. The solution should discover API endpoints for granular visibility on deployed cloud assets and API Gateways.
v. The tool should perform API risk profiling to identify API risk factors, sources of risk, vulnerabilities and changes to prioritize remediation or protection.
vi. The solution should detect, alert & block Web and API attacks in real time on hosts, containers, kubernetes and serverless deployments to prevent breaches.
vii. The solution should detect, alert & block OWASP Top 10 Web Attacks in real time to prevent breaches
viii. The solution should have the ability to provide a risk assessment for API definitions to determine risky and insecure APIs.

12. **Quality Gate and Trusted Image enforcement for container going in to Production Clusters**

i. The tool must dynamically analyses the runtime behavior of image in on-prim sandbox environment before running them in your development and production environments.

ii. The Solution should prevent container being deployed on kubernetes cluster/worker Nodes, if container image does not meet the minimum defined vulnerability criteria without relying on CI-CD tools or on Kubernetes access control to prevent malicious containers to run on worker nodes.

iii. The Solution should prevent container being deployed on kubernetes cluster/worker Nodes, if container image has Compliance issue. Example:: Sensitive info is embedded in environment variables, Private keys stored in Image, Image is created with a root user. Etc. This should be achieved without relying on CI-CD tools or on Kubernetes access control.

iv. The Solution should have ability to prevent container being deployed on kubernetes cluster if container image is not prequalified as TRUSTED IMAGE. The tool should be able to create TRUSTED IMAGE policy based on (a) Trusted Repos (b)Trusted Base Images (c)Manually qualified images etc. And the tool should have ability to alert and/or block deployment when container don't meet the TRUSTED IMAGE policy without relying on CI-CD tools or on Kubernetes access control.

13. **Container image sandbox analysis**

i. The solution should dynamically scan container images in a sandbox to detect suspicious activities like malware and port scanning and provide a detailed runtime behavior profile to prevent malicious images from deployment into runtime

ii. Capability to scan and sandbox container images upon download from 3rd parties to analyses prior to developing apps on it.
- Malicious Behavior i.e. malware, crypto miners and outbound C2C.
- Understand behavior of container image i.e. process/file system calls

14. **Architecture and Integration**

i. The solution should be provided as a SaaS or on-premise software tool with support for VMs and Kubernetes/container in AWS, Azure, and GCP cloud environments. It should provide flexibility of securing cloud native software stacks on Openshift, Kubernetes, and Tanzu container environment.

ii. The solution should have extensive logging and telemetry capability

iii. The solution should have extensive API capability and should offer all the above features as and API

iv. The solution must have an intuitive UI to provide rapid forensics and investigative capabilities.

v. The solution must integrate with Active Directory, OpenLDAP, and SAML

vi. The solution must have Alerting integration with developer and operations tools like Jira, Slack, Pager duty, SOAR platforms

vii. The solution must provide for Open integration support for alert using Webhook.

Cloud Code Security

1. Infrastructure as code
   i. The solution must Identify misconfigurations in IAC files and present developer friendly suggestions and fixes via native IDE, VCS (Git) & CI/CD plugins to prevent misconfigured resources from deployment into runtime
   ii. Tool must have the capability to scan a wide array of IAC templates i.e. TFT (HCL format), CFT (JSON / YAML), ARM, Helm, Dockerfiles, Swagger, Kubernetes App manifest (JSON/YAML), BICEP and others and where possible automated remediation actions
   iii. Must be able to detect and scan existing IAC templates in Git repos i.e. GitHub, Gitlab, BitBucket, Azure Repos etc.
   iv. Must be able to detect and scan existing IAC mis-configurations in pull request/merge request
   v. Must be able to visualize the relationships between code elements i.e. IAC and Packages to determine relationships and dependencies
   vi. The tool must have the capability to integrate with DevOps tooling and workflows i.e. IDE, CI workflows and GitOps workflows
   vii. Platform supports scanning of secrets, detect secrets in IDEs, Git-based VCS, and CI/CD executions.
   viii. Must be able to natively report results within Developer workflow tools i.e. Git (Github, Gitlab etc.), IDE tools and CI tooling as well as ad hoc usage via the CMD.
   ix. Capability to define code custom policies in addition to out of the box policies that can be cloned.
2. Software Composition Analysis (SCA)
   i. The solution must detect and prevent critical open source vulnerabilities from being deployed in direct & transitive dependencies with clear, automated fixes and blocking via native IDE, VCS or CI/CD plugins.
   ii. Must have the capability to perform SCA for a wide range of package manager's i.e. Dockers, Go, Java (Maven/Gradle) Javascript (NPM, Yarn, Bower) Kotlin (Gradle) Python (Pip, Pipfile), Ruby and YAML
   iii. The solution support vulnerability scanning based on CVE's and return detailed information on each vulnerability i.e. CVE ID, CVSS score, Package Name, Version, Attack Vector, Public POC, Exploit in the Wild and whether a fix is available
   iv. Must be able to provide the capability to bump fix packages.
   v. Must list and map all packages and their dependencies, also visualize where possible as a supply chain with dependencies.
   vi. Must provide scanning for licensing compliance violations and non-compliance
   vii. Must be able to scan existing repos for code based vulnerability and compliance issues.

viii. Must be able to scan packages as changes and modifications are raised via Pull and Merge request.

ix. Ability to generate Software Bill of Materials (SBOM) and output in industry standard formats i.e. Cyclone DX XML and CSV

Contract Uptime

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 24x7x365 an uptime of 99.90% during warranty 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.

The "**Downtime**" is the time between the Time of Report by the Bank and Time of Restoration/Rectification within the contracted hours. "**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.

The percentage uptime is calculated on quarterly basis as follows:

(Total hours in a quarter - downtime hours within the quarter)

---------- * 100

Total hours in a quarter

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

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/AMC period Cost for every 4 hrs. of delay in restoration	15 days of Warranty period Cost for every 1 day of delay in
Severity-2	10 days of Warranty/AMC period Cost for every 12hrs of delay in restoration	10 days of Warranty period Cost for every 2 days of delay in
Severity-3	5 days of Warranty/AMC period Cost for every 24 days delay in restoration	5 days of Warranty period Cost for every 3 days of delay in

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.

Term and Termination.

This SLA shall become effective on the Effective Date and shall continue in full force and effect unless or until terminated by either party in accordance with the terms of this SLA.

This SLA and/or any Service Attachment may be terminated as follows:

i. if a party makes an assignment for the benefit of creditors, file a petition in bankruptcy, commences any proceeding relating to it under any bankruptcy or similar statute, or there is commenced against such party any proceeding which shall be not dismissed in 30 calendar days, the non-assigning or non-filing party may terminate immediately upon giving notice to the other party.

ii. By the non-breaching party, for material breach of this SLA and/or any Service Attachment and failure of the breaching party to cure such breach within 30 calendar days after receiving written notice of such breach from the non-breaching party;

iii. By agreement between the parties.

Payment Terms

The Bidder must accept the payment terms proposed by the Bank as proposed in this section. The commercial bid submitted by the bidders must be in conformity with the payment terms proposed by the Bank. Any deviation from the proposed payment terms would not be accepted. The Bank shall have the right to withhold any payment due to the bidder, in case of delays or defaults on the part of the bidder. Such withholding of payment shall not amount to a default on the part of the Bank. If any of the items / activities as mentioned in the price bid is not taken up by the bank during the course of the assignment, the bank will not pay the cost of such items and professional fees quoted by the bidder in the price bid against such activity / item.

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:

Payment will be made as per the milestones defined below:

Sr. #	Project Milestones	Payment Terms
01	Delivery and installation of software components supporting licenses.	30% of First year License cost
02	Go-Live, UAT Signoff, user and administrative Training.	70% of First year License cost.
03	Year 2 & 3 license	100% of the Annual Cost Payment post activation of Licenses.

Payment to be made subject to submission of 5% of PBG of the total Project Cost.

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.

Dispute Resolution

Any dispute controversy or claims arising out of or relating to this Master Agreement or any Service Attachment thereto shall be resolved amicably, by parties through negotiation. If the parties are unable to settle such dispute by negotiation within 15 days from date of receipt of notice by the affected party, parties shall opt for settlement by arbitration in accordance with the provisions of the Arbitration and Conciliation Act, 1996 and the rules made there under, as amended from time to time. The Arbitral tribunal shall comprise of three arbitrators, one arbitrator to be appointed by each party, and the third arbitrator shall be appointed by such arbitrators.

The cost of appointing the respective arbitrators shall be borne by the respective party, however the cost of appointing the third arbitrator shall be borne by the parties equally by both the parties.

The place of arbitration shall be _____ and the arbitration proceedings shall be conducted in English language."

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 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.

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

iii. 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.

Termination of Contract

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 three months prior notice.

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.

Indemnity

a. The Company 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 directly or indirectly 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 Company,
   iii. Breach of confidentiality obligations by the Company,
   iv. Negligence (including but not limited to any acts or omissions of the Company, its

officers, principals or employees) or misconduct attributable to the Company 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 company;
vii. Non-compliance by the Company with applicable Laws / Governmental /Regulatory Requirements. Provided however,

a) BANK notifies the Company in writing immediately on being aware of such claim,
b) The Company has sole control of its defense and all related settlement negotiations.

The Company 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 Agreement.

b. Notwithstanding anything to the contrary contained in this agreement the company shall indemnify and hold the Bank harmless from and against any claims, losses, damages, liabilities or expenses (including legal fees of solicitor(s)/advocate(s)), up to the extent of actual loss suffered by the Bank, resulting from any of the acts or omissions of the Company, its officers, principals or employees in connection with provision of the services under this agreement or breach of any of the obligations of the Company under this agreement.

Right to Audit

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

The Selected Bidder (Bidder) 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 Bidder 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, 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 three 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.

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.
"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.
"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.
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.
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 .... and designated representative of the Company. If designated Officer of the Bank for ....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
Corporate Headquarters. 190001

The Jammu & Kashmir Bank MA Road, Srinagar

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	Agreed and signed on behalf of
Company's Authorized Signatory	J&K Bank Limited
Name……	Name……
Designation……	Designation……
Place……	Place……

Date.....	Date .....
Witness (1):	Witness (1):
Name..... Designation..... Place..... Date.....	Name..... Designation..... Place..... Date .....
Witness (2):	Witness (2):
Name..... Designation..... Place..... Date.....	Name..... Designation..... Place..... Date .....

Annexure K: Undertaking

To

Chief Information Security Officer,
Information Security Department.
Corporate Headquarters

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

190 001 J&K.
Dear Sir,

Sub: RFP no: _____ for RFQ FOR CLOUD SECURITY POSTURE MANAGEMENT & WORKLOAD PROTECTION

Having examined the tender documents including all annexures the receipt of which is hereby duly acknowledged, we, the undersigned, offer to provide SELECTION OF VENDOR FOR RFQ FOR CLOUD SECURITY POSTURE MANAGEMENT & WORKLOAD PROTECTION 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 including the conditions applicable to reverse auction proposed to be followed by the Bank.

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 State 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 L: Know Your Employee (KYE) Clause

To

Chief Information Security Officer,
Information Security Department.
Corporate Headquarters

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

190 001 J&K.

Dear Sir,

1. 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._____ _____ (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.

2. 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.

3. 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

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

Annexure M: Compliance Requirements

1. 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.

2. 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.

3. 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.

4. 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.

5. 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.

6. 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.

7. 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.

8. 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.

9. 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.

10. 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.

11. 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.

12. The Service Provider must provide the Bank secure control for managing its identities (Including Identity Creation and Deletion / Modification & Termination).

13. The Service Provider shall ensure Authentication, Authorization, Accounting, Access control and logging (Format, retention and Access) meet the Bank's regulatory and legal requirements.

14. 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.

15. The Service Provider shall have the information readily available on Location and time of access of the Service Provider Team.

16. 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.

17. 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.

18. 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

19. The bidder shall ensure to adopt and is in compliance with Change Management and Incident Response Procedures as specified in (ITIL).

20. The Service Provider shall share its DR plan with Bank so as to ensure it matches the Bank's BCP requirements.

21. The Service Provider has the ability to retrieve and restore data following data loss incidents.

22. 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.

23. 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.

24. 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.

25. 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).

26. 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.

27. 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.

28. 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.

29. 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.

30. 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.

31. 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.

32. 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.

33. 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.

34. 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.

35. 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.

36. 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.

37. 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.

38. The Service Provider shall grant unrestricted and effective access to data related to the outsourced activities.

39. 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.

40. 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.

41. Bidder shall not propose any solution/components which is near to end of life or end of support during the tenure of the contract.