Request for Proposal (RFP)

for

Implementation, Support and Maintenance of Dynamic Application Security Testing (DAST) Tool

EBID-: IT-26-27-267
Date : 23rd Nov 2026

This Document is the property of Multi Commodity Exchange of India Ltd (MCX). It may not be copied, distributed, or recorded on any medium, electronic, or otherwise, without MCX written permission. Use of contents given in this document, even by the authorized personnel/agencies for any other purpose other than the purpose specified herein, is strictly prohibited as it shall amount to copyright violation and thus shall be punishable under the Indian law

Public

Table of Contents

Section 1 – Introduction 3
1.1 MCX India Limited Background 3
1.2 Background 3
Section 2 – Contact Details and Submission Process 3
2.1 Submission of Proposal 4
2.2 Terms & Conditions: 4
2.3 Payment Terms: 5
Section 3 – Submission of Bids 5
Section 4 – Bid Evaluation Process 5
4.1 Bidder 60 5
4.2 Techno-Commercial evaluation 5
Section 5 - Terms & Conditions 6
Section 6 – Implementation Requirements 8
6.1 Resource Allocation 8
6.2 Solution Services and Frequency of Delivery to be ensured by the Bidder / OEM: 8
6.3 Project Timelines 9
6.4 Support and Maintenance 9
Annexure - A: Technical Specification and Scope of Work 10
Annexure - B: Inventory 15
Annexure – C: Bidder's Organization Profile 15
Annexure – D: Compliance for Eligibility Criteria 16
Annexure – E: SLA & Penalties 17
Penalty for Delayed Delivery: 18
Penalty for Delayed Implementation: 18
Annexure - F: Commercial Bid 19
Annexure–G: Notification, Confidentiality, Termination Clause 22
Notification: 22
Confidentiality: 23
Termination Clause: 23
Annexure–H: Bank Guarantee (Procurement Team) 23
Annexure – I: IT Act & Free from Malware/Backdoor Certificate 23

Public

Section 1 – Introduction

1.1 MCX India Limited Background

Multi Commodity Exchange of India Limited (MCX), India's first listed exchange, is a state-of-the-art, commodity derivatives exchange that facilitates online trading of commodity derivatives transactions, thereby providing a platform for price discovery and risk management. The Exchange, which started operations in November 2003, operates under the regulatory framework of Securities and Exchange Board of India (SEBI).

Considering regulatory requirements in India (SEBI, CERT-In, NCIIPC, etc.) and increasing innovative cyber risk threats, malwares and threats emanating from emerging technologies like AI/ML, bots, dark-webs, social engineering, cloud etc., MCX wants to enhance their cyber security strategies to be aligned with changing needs of new working world. From predicting cyber-attacks (internal and external) to managing Endpoint protection, MCX wants to accelerate risk reduction across their entire technology landscape.

The purpose of MCX behind this RFP is to seek a detailed technical and commercial proposal for procurement of the Software/ Solutions Services desired in this RFP. The proposed Products, Hardware, Software, Services must integrate with MCX's existing infrastructure seamlessly.

Bidder shall mean any entity (i.e., juristic person) who meets the eligibility criteria given in this RFP and is willing to provide the Software Solutions/ Products/ services as required in this RFP. The interested Bidders who agree to all the terms and conditions contained in this RFP may submit their Bids with the information desired in this RFP. Consortium bidding is not permitted under this RFP.

Interested Bidders are advised to go through the entire RFP before submission of Bids to avoid any chance of elimination. The eligible Bidders desirous of taking up the project for supply of proposed Products, Software, Solution, services for MCX are invited to submit their technical and commercial proposal in response to this RFP. The criteria and the actual process of evaluation of the responses to this RFP and subsequent selection of the successful Bidder will be entirely at MCX's discretion. This RFP seeks proposals from Bidders who have the necessary experience, capability & expertise to provide MCX with the proposed Products, Software Solutions, and services adhering to MCX's requirements outlined in this RFP.

1.2 Background

This RFP is to invite tender for installation, commissioning, and maintenance of an On-Premises Breach and Attack Simulation (BAS) Tool (covering Security Control Validation [SCV], Adversarial Exposure Validation / Attack Path Validation [AEV/APV], and Automated Red Teaming).

Section 2 – Contact Details and Submission Process

Contact Details and Submission Process

Submission of Proposal

The proposal with the relevant information / documents/ acceptance of all terms and conditions as described in this RFP document will be submitted online. Contact details for RFP submission.

Mr. Prakash Komu –- prakash.komu@mcxindia.com **– 9920381998**

Public

List of the Annexures to be submitted online as mentioned below.

S/N	Particulars	Annexure	To be submitted with
1	Technical Specification and Scope of Work	**Annexure-A**	Technical Bid
2	Inventory	**Annexure-B**	Technical Bid
3	Bidders Organization Profile & capability Presentation to support the scope of work as per RFP and post implementation support. Along with earlier similar projects	**Annexure-C**	Technical Bid
4	Eligibility Criteria	**Annexure-D**	Technical Bid
5	Service Level Agreement	**Annexure-E**	Technical Bid
6	Commercial Bid	**Annexure-F**	Commercial Bid
7	Penalty, Notification, Confidentiality, Termination Clause	**Annexure-G**	Technical Bid
8	Bank Guaranty	**Annexure-H**	Technical Bid
9	Tender Document duly signed		Technical Bid
11	Power of Attorney (signing authority letter from Company)	**Annexure-I**	Commercial Bid
10	IT Act & Free from Malware/Backdoors Certificate	**Annexure-J**	Technical Bid

2.1 Terms & Conditions:

2.1.1 Tenders should strictly confirm the specifications. Tenders not conforming to the specifications will be rejected summarily.

2.1.2 Any incomplete or ambiguous terms/ conditions/quotes will disqualify the offer.

2.1.3 MCX reserves the right to accept in part or in full or reject the entire quotation and cancel the entire tender, without assigning any reason there for at any stage where any terms and conditions from the Vendors are not acceptable to MCX.

2.1.4 MCX reserves the right to impose and recover penalties from the vendors who violate the terms & conditions of the tender including refusal to execute the order placed on them for any reasons.

2.1.5 The Bidder must submit Integrity Pact and NDA wherever and whenever (as applicable).

2.1.6 Notwithstanding the approximate quantity mentioned in the Tender the quantities are liable to alteration by omission, deduction or addition, payment shall be regulated on the actual work done at the accepted rates and payment schedule.

2.1.7 The qualified Bidder rates finalized discovered will be valid for 24 months and the qualified Bidder vendor is bound to execute the orders placed at qualified Bidder rates during the duration of the contract. The validity period may be extended at the discretion of MCX, which will be binding on the vendors.

2.1.8 The prices quoted for Solution & Services should be for a period of three years and in INR. MCX has the right to dismiss the contract any time with the notice of 01 Month, if found guilty or deemed unfit for effective operation The prices should be exclusive of all taxes, the vendor should arrange for obtaining permits wherever applicable excluding taxes.

2.1.9 The Vendor should attach all the related product literature, data sheets, handouts, evaluation reports etc., pertaining to the solutions for which the Vendor has quoted. Subjective validation of the submitted bids will be validated and scrutinized internally.

2.1.10 MCX may change the bid evaluation criteria at its own discretion after receipt of bids from competent bidder. MCX also reserves the right to remove components from Commercial bid for evaluation purpose and for releasing the work order for partial scope.

2.1.11 MCX will notify the successful Bidder in writing by way of issuance of purchase order through letter or email that its Bid has been accepted. The selected Bidder must acknowledge by return email/letter in token of acceptance.

2.1.12 The bidder must sign the Bank guaranty and other contracts as per the points stated in the RFP / annexure.

Public

2.2 Payment Terms:

2.2.1 **For Supply/Delivery of Hardware/Appliances, Licenses, Installation of Licenses: -**

90% after successfully delivery & Installation post sign off, 5% after 6 months from installation and 5% after 12 months after installation.

2.2.2 **For Implementation of Solution (DC, DR): -**

90% after successful implementation post sign off, 10% 6 months after successful implementation and implementation/configuration review and certification by OEM with final signoff by MCX.

2.2.3 For AMC/ATS, on half yearly basis (In advance) within 45days subject to satisfactory service delivery and SLA compliance

Section 3 – Submission of Bids

Post confirmation from bidder and receipt of expression of interest, the MCX team will evaluate the responses received. The eligible bidder will receive the details about participating in e-bidding process, through MCX authorized e-bidder. Two (2) separate proposals: Technical and commercial to be submitted separately. Technical proposal will contain Configuration, Technical details, Eligibility criteria feedback, etc. Commercial proposals contain commercials, payment terms, other charges, Delivery, etc. and should be password protected and password to be shared when requested from MCX procurement team only.

Section 4 – Bid Evaluation Process

4.1 Bidder Eligibility Criteria

4.1.1 Bidder Profile and experience in the industry.
4.1.2 Bidder capability to support the RFP scope and based on the presentation.
4.1.3 Bidder support facilities / proactive support/Profile/ Previous experience.
4.1.4 OEM post sale support and experience.
4.1.5 MCX will evaluate the technical and functional specifications of all the equipment quoted by the Bidder.
4.1.6 During evaluation and comparison of bids, MCX may, at its discretion, ask the bidders for clarification of its bid. The request for clarification shall be in writing and no change in prices or the substance of the bid shall be sought, offered, or permitted. No post bid clarification at the initiative of the bidder shall be entertained.
4.1.7 MCX reserves the right to evaluate the bids on technical, functional, and subjective parameters including factory visit, client site visit and witness demos of the system and verify functionalities, response times, public documents, Market Share, OEM establishment blogs, Group Company experience with product etc.
4.1.8 Also please refer Annexure – D for details

4.2 Techno-Commercial evaluation

4.2.1 Technical bids will be examined by the Technical Committee of MCX which may call for clarifications / additional information from the Vendors which must be furnished to the Technical Committee in the time stipulated by the Technical Committee. E.g., Presentation, Demo or POC of the product.
4.2.2 Technical bids will be opened for eligibility criteria and technical evaluation.
4.2.3 Bids that are not substantially responsive are liable to be disqualified at MCX.'s discretion.
4.2.4 Technical evaluation will include technical information submitted as per technical Bid format, demonstration/POC of proposed solution, reference calls and site visits, wherever required.
4.2.5 The Bidder may highlight the noteworthy / superior features of their Services. Proposed solution features, guaranteed uptime, integration, underlying components' etc.
4.2.6 Scalability / Capability of the proposed solution to meet future requirements not outlined in the RFP with around 20% yearly growth.

Public

4.2.7 The Bidder will demonstrate/substantiate all claims made in the technical Bid to the satisfaction of the Company, the capability of the Services to support all the required functionalities at their Price in their lab or those at other organizations where similar Services is in use or during POC.

4.2.8 The detailed scope of work will be included in the Request for Proposal (RFP) document which shall be issued to all the qualified bidders. Technical evaluation of the submitted bids with respect to the RFP will then be evaluated. Technically qualified bidders will be selected under qualified Bidder criterion. Financial bid will be evaluated only for the technically qualified bidders.

Section 5 - Terms & Conditions

5.1 Submission of bid for RFP is evidence of a Bidder's consent to comply with the terms and condition of Request for RFP process and subsequent bidding process. If a Bidder fails to comply with any of the terms, its bid may be summarily rejected.

5.2 Willful misrepresentation of any fact in the RFP will lead to the disqualification of the Bidder without prejudice against other actions that MCX may take. The RFP and the accompanying documents will become property of MCX.

5.3 The Bidders shall be deemed to license, and grant all rights to MCX, to reproduce the whole or any portion of their product/solution for the purpose of evaluation, to disclose the contents of submission to other Bidders and to disclose and / or use the contents of submission as the basis for RFP process.

5.4 MCX reserves the right to accept or reject any or all RFPs received without assigning any reason whatsoever and MCX's decision in this regard will be final.

5.5 MCX reserves the right to inspect/Audit the facilities of the bidder at any time during the evaluation stage to verify the genuineness and to ensure the conformity with the proposal submitted.

5.6 Successful Bidder to comply with SEBI/NCIIPC/CERT-In cyber security framework requirements and all guidelines issues time to time including Cloud adoption guidelines

5.7 The bidder is required to submit its full profile giving details about organization, experience, technical personnel in the organization, competence, and adequate evidence of its financial standing etc. in the enclosed form which will be kept confidential.

5.8 No contractual obligation whatsoever shall arise from the RFP process.

5.9 Any effort on the part of Bidder to influence evaluation process may result in rejection of the RFP.

5.10 MCX is not responsible for non-receipt of RFPs within the specified date and time due to any reason including postal delays or holidays in between.

5.11 MCX reserves the right to verify the validity of information provided in the RFPs and to reject any bid where the contents appear to be incorrect, inaccurate, or inappropriate at any time during the process of RFP.

5.12 MCX wants that implementation to be done by the bidder along with OEM engineers. Post implementation the partner / bidder should have the capability to manage, maintain and support the product (with or without OEM's support)

Public

5.13 The Bidder should perform efficacy tests periodically at least on quarterly basis to ensure the standards are maintained aligning compliance and industry best standards.

5.14 Bidders shall be deemed to have,

a. Examined the Request for RFP document and its subsequent changes, if any for the purpose of responding to it.
b. Examined all circumstances and contingencies, influencing their RFP application and which is obtainable by the making of reasonable enquiries.
c. Satisfied themselves as to the correctness and sufficiency of their RFP applications and if any discrepancy, error, or omission is noticed in the RFP, the Bidder shall notify MCX in writing on or before the end date/time.
d. The bidder shall bear all costs associated with submission of RFP, presentation/POC desired by MCX.
e. MCX will not be responsible or liable for any cost thereof, regardless of the conduct or outcome of the process.
f. Bidders must advise MCX immediately in writing of any material change to the information contained in the RFP application, including any substantial change in their ownership or their financial or technical capacity. Copies of relevant documents must be submitted with their advice.
g. Shortlisted Bidders must not advertise/publicize in any form (without prior written permission from MCX) about their unit having been shortlisted by MCX.
h. The detailed scope of the work will be included in the Request for Proposal (RFP) document which shall be issued to all the qualified bidders. Technical evaluation of the submitted bids with respect to the RFP will then be evaluated. Technically qualified bidders will be selected under qualified Bidder criterion. Financial bid will be evaluated only for the technically qualified bidders.
i. MCX may re-visit any of the conditions of this RFP, before the deadline for submission.
j. A weightage of 70:30 % respectively shall be considered for technical and commercial bid (inclusive of functional, subjective, efficacy evaluation).
k. The threshold limit for minimum technical score will be 55% out of 70 to qualify for further bidding process

5.15 MCX have the right to cancel the tendering process at any time, without thereby incurring any liabilities to the affected Bidders. Reasons for cancellation, as determined by MCX in its sole discretion include but are not limited to, the following:

a. Services contemplated are no longer required.
b. Scope of work is not adequately or clearly defined due to unforeseen circumstances and/or factors and/or new developments.
c. The project is not in the best interest of MCX.
d. Any other reason.

5.16 **Documents**: Bidder shall provide following documents as part of implementation signoff: (As applicable)

a. Technical architecture document
b. HLD & LLD
c. Test cases document
d. Functional specification document
e. User Manual
f. Installation and Operations manual
g. SOPs for day-to-day activities
h. All other relevant documents are required for the project.

Public

5.17 **Acceptance: -**The solution shall be considered accepted based on following points:

a. All applicable criteria to determine conformity of any Deliverable with the agreed Specifications based on which MCX may accept the relevant Deliverable.

b. MCX shall review and conduct acceptance testing prior to its acceptance of the Software/hardware Deliverables. The Bidder will aid and support in installation as per the Documentation and installation guidelines provided by Bidder, and the MCX's review and acceptance testing as described in the relevant Statement of Work or in an Acceptance Test plan agreed between the Parties. MCX shall promptly begin its review and, if appropriate, test each Software Deliverable to determine whether it conforms to the Specifications or other mutually agreed acceptance criteria. If the MCX reasonably determines that the Software Deliverable has not met the Acceptance Criteria, MCX shall notify the Bidder in writing of any such non-conformity within the specified period. MCX shall provide written acceptance of Software Deliverable if MCX has not found any non-conformity of the Software Deliverable with the Acceptance Criteria during the review.

5.18 **Training:** Bidder shall provide the training to the MCX personal as describe below

Bidder should provide OEM training and certification (2 days or more classroom training) to MCX team (Around 15 people). The training should be technical with lab setup including architecture, software components, policy installation, and troubleshooting, operations, reporting and other aspects of solution.

Post Implementation, the bidder should provide operational training every year to officials of the MCX.

Section 6 – Implementation Requirements

6.1 Resource Allocation

- Resource allocation for implementation will be mutually decided in agreement with MCX and Bidder. The Resources allocated for implementation must fulfill the industry standards and the competency in OEM certified with OEM tool implementation experience.
- End to end implementation of solution, agent deployment, troubleshooting and configuration of databases and clusters as per deployment requirement to be taken care by Bidder.
- MCX has the authority to examine the resources for competency and can request change of resource – anytime to the bidder, if found unfit or for any other valid reasons.

6.2 Solution Services and Frequency of Delivery to be ensured by the Bidder / OEM:

Device Management	
Activity Detail	**Frequency of Delivery**
System Hardening	As and when required
Update/Upgrade/Patching/ Vulnerability remediation	As and when required
Backup/Restore	As per the policy defined by MCX
Configuration Management	As and when required
Configuration Review and Performance Tuning	Quarterly or as and when required
Change Management	As and when required
Access Management	Continuous
Solution Manual /SOP Preparation and Review	During Implementation of the solution (Baseline

Public

	Manual), Half Yearly Review.
Device Problem Management	As and when required
DR Drill of the Solution	As and when requested
License & AMC Management	Continuous
OEM/SI Liaising for technical support	As and when required
Use-cases configuration, automated incident response, reports, dashboards, etc.	As and when required
Integration with IT / IS infrastructure for automated response (Existing/Future)	As and when required
Custom Reports	As and when required
OEM/SI Coordination for Support	As and when required

6.3 Project Timelines

Bidders are requested to furnish the following timelines regarding the implementation of the proposed solution:

6.3.1 Defining Implementation Plan, Architecture, Complete installation, configuration, and deployment of BAS Solution at DC and DR in standalone deployment. The complete solution implementation along with business defined use-cases should be completed within 08 weeks or less from issuance of the purchase order. This also includes DC DR cutover and cutback, integration of security tools and other required.

6.3.2 Product warranty and AMC will start after successful implementation of the proposed solution.

6.3.3 Bidders are requested to add phase wise timeline / Milestones and present it during the presentation.

Phase	**Timelines**								
	W0	W1	W2	W3	W4	W5	W6	W7	W8
Planning									
Design									
Installation, Configuration & Deployment									
Integration of security tools and technologies									
Use-cases creation and automated incident response									
Testing & *Optimization									
Deployment Validation & Sign-off from MCX									

6.4 Support and Maintenance

6.4.1 Support and maintenance services for the entire contract period including 24x7 online support, telephonic support, and onsite visits (DC/DR) for issue resolutions, without any extra cost to MCX.

6.4.2 All support during Implementation by bidder/OEM must be provided onsite & no Remote access will be allowed through any remote desktop sharing applications.

6.4.3 System Maintenance and Support services also includes:

a The maintenance support should be (24x7 365days) including product (major or minor) upgrades and updates. The support should be for unlimited requests. It may be provided on Email / Telephone /Onsite.

b Direct OEM Service and support should be covered under with dedicated TAM (Technical Account Manager) and onsite support, as and when required.

Public

c The proposed product (hardware, software, etc.) should not be under "End of Sale", "End of Support", "End of License" for the next five years and the proposed product should not be under "End of Shelf Life" (EOSL) in the next five years.

d If product goes EOSL/EOL within contract period of five years, support, and upgrade to new versions of hardware/software shall be provided by the bidder to MCX without any additional cost.

e If MCX selects the proposed product and even after the contract period is over, the bidder should provide support for the period as decided by the MCX at mutually agreed rates.

6.5.5 Bidder should create SOPs to carry out system administration tasks including regular backup of system, restoration, installation, health check, VAPT activity and closure of VAPT findings within MCX defined timelines. Bidder should also support any faults in the proposed solution by troubleshooting and coordinating with the OEM. The bidder should support such activities any time that is required during the contract period.

6.5.6 Bidder should support for any internal or external security preparedness drills (including SEBI / NCIIPC / CERT-In cyber drills) and carry out activities for setting up monitoring and response systems required for the drills and participate in all stages of such drills as and when required.

6.5.7 Bidder to comply with SEBI Cyber security framework & Cloud adoption requirements and advisories/circulars issued time to time by SEBI, NCIIPC and CERT-In.

6.5.7 Bidder should design architecture for DC – DR cutover and cutback and the same must be implemented along with go-live implementation.

Annexure - A: Technical Specification and Scope of Work

Compliance: C – Fully compliant, P – Partially Compliant, N – Not compliant

The key requirements of Breach and Attack Simulation (BAS) solution are as follows.

The scope of work under this RFP includes, but is not limited to, the following:

- Supply and licensing of the proposed on-premises BAS Platform, sized for the specified user count, asset volume, and data retention requirements, including production and UAT environments.
- Installation, configuration, and commissioning of the Solution on infrastructure provided by the MCX.
- Configuration of asset inventory, vulnerability management, risk management, assessment management, exception management, workflow, dashboard, and reporting modules as per requirements.
- Integration with the existing security tools.
- User Acceptance Testing (UAT) support, defect resolution, and Go-Live support.
- Training of administrators, end users, and approvers on the use and administration of the Solution.
- Post-implementation Hyper Care support for a defined period following Go-Live.
- Ongoing Annual Maintenance Contract (AMC) support, including patches, upgrades, and helpdesk support, for the contract period specified in this RFP.
- Provision of complete technical, administrator, and user documentation.

Any activity reasonably necessary to achieve the successful implementation and operation of the Solution, even if not explicitly listed above, shall be deemed to be within the scope of this RFP unless expressly excluded.

Public

Scope of Work

The primary objective of this RFP is to implement an on-premises Dynamic Application Security Testing (DAST) solution covering Automated Web & API Vulnerability Scanning (AWVS) and Authenticated Business Logic & Runtime Exploit Validation (ABLV), centered on continuous application security testing, compliance, and DevSecOps posture enhancement, where scan policies and attack payloads can be customized as per MCX internal security policies and regulatory requirements.

Automated Web & API Vulnerability Scanning (AWVS) ensures the security resilience of external and internal web applications, portals, microservices, and APIs (REST, SOAP, GraphQL) by continuously testing running applications in staging and production environments against real-world attack vectors mapped to OWASP Top 10, OWASP API Security Top 10, CWE/SANS Top 25, and regulatory standards. By proactively identifying runtime vulnerabilities and misconfigurations, the solution provides evidence-based proof of exploitability and prescriptive developer remediation guidance.

Authenticated Business Logic & Runtime Exploit Validation (ABLV) provides continuous, deep-crawl validation of complex, modern web architectures (Single Page Applications, JavaScript-heavy frameworks, and multi-step authenticated workflows) to uncover authentication bypasses, session management flaws, broken access controls (IDOR/BOLA), and injection vulnerabilities. By combining intelligent crawling with safe, automated exploit verification, ABLV proves which application flaws are truly exploitable, eliminates false positives, and verifies vulnerability closure upon patching.

Detailed SoW

Automated Web & API Vulnerability Scanning (AWVS)

- Ensure Continuous Regulatory Compliance: Automatically and continuously assess web applications and APIs against regulatory frameworks and industry standards (e.g., SEBI CSCRF, NCIIPC, CERT-In, ISO 27001, PCI-DSS, NIST, OWASP Top 10, OWASP API Top 10) to produce audit-ready compliance reports at any time, with the ability to customize or create new scan policies as per MCX security guidelines.
- Achieve Comprehensive Application & API Coverage: Enforce application-layer defense-in-depth by discovering and testing public-facing portals, internal web applications, legacy platforms, and APIs (importing OpenAPI/Swagger, Postman collections, WSDL, and GraphQL schemas) against runtime threats without requiring access to underlying source code.
- Enable Proof-Based Vulnerability Validation: Proactively identify and safely verify exploitable runtime flaws—such as SQL Injection (SQLi), Cross-Site Scripting (XSS), Server-Side Request Forgery (SSRF), Remote Code Execution (RCE), and security misconfigurations—delivering concrete HTTP request/response evidence to minimize false positives.
- Automate Auditing and Developer Reporting: Improve the efficiency and accuracy of IT, regulatory, and VAPT audits by providing centralized dashboards and detailed technical reports featuring root-cause analysis, CVSS scoring, and actionable remediation guidance tailored to specific tech stacks.
- Provide Centralized Visibility and Risk Prioritization: Consolidate scan findings across diverse environments (UAT, staging, pre-production, and production) into a single on-premises management console, offering a risk-prioritized view of MCX's

Public

application attack surface and trend analytics.

Authenticated Business Logic & Runtime Exploit Validation (ABLV) Requirements

- Deep Crawling & Complex Authentication Handling: Safely navigate and scan modern Single Page Applications (SPAs) and complex multi-step workflows using recorded login sequences, macro playback, and automated handling of SSO, OAuth 2.0, JWT, SAML, and Multi-Factor Authentication (MFA) tokens.
- CI/CD & Enterprise Ecosystem Integration: Embed automated security gates directly into MCX's DevSecOps pipelines (Jenkins, GitLab, Azure DevOps, etc.) and integrate seamlessly with existing MCX SIEM, WAF (for virtual patching rule generation), vulnerability management, and ticketing/bug-tracking tools (Jira, ServiceNow) for automated ticket creation and closure verification.
- Incremental & Non-Disruptive Scanning: Execute scheduled, incremental, or delta scans targeting newly deployed code changes with granular rate-limiting and traffic-throttling controls to ensure zero degradation or disruption to live production applications.
- Asset Scope: Validation must extend across all MCX on-premises hosted web applications, customer/member portals, internal administrative interfaces, web services, and REST/SOAP/GraphQL APIs deployed across physical, virtual, and containerized environments without requiring cloud connectivity or external data egress.

Risk Management Requirements

Requirements governing dynamic risk scoring, risk acceptance, risk registers, and enterprise risk reporting.

Sr. No.	Requirement Description	Compliance (Yes/No/Partial)	Bidder Remarks
1	The proposed solution shall calculate a dynamic, composite risk score for each vulnerability and asset by combining CVSS base score, EPSS score, exploit maturity, asset criticality, internet exposure, business impact, and compensating controls.		
2	The proposed solution shall allow risk administrators to configure and adjust the weightage of each risk-scoring factor without vendor dependency.		
3	The proposed solution shall provide a formal risk acceptance workflow with mandatory business justification, defined approval hierarchy, and expiry/review date.		
4	The proposed solution shall require re-justification and re-approval of accepted risks upon expiry, with automatic reminders to risk owners in advance of expiry.		
5	The proposed solution shall maintain a consolidated risk register aggregating accepted risks, exceptions, and waivers across the organization, with reporting by business unit, asset, and severity.		
6	The proposed solution shall support configurable risk appetite thresholds, with automated flagging of risks exceeding defined risk appetite.		
7	The proposed solution shall provide a risk heat map visualizing residual risk by business unit, asset group, and severity category.		

Public

Sr. No.	Requirement Description	Compliance (Yes/No/Partial)	Bidder Remarks
8	The proposed solution shall maintain full audit history of all risk acceptance, waiver, and exception decisions, including approver identity, timestamp, and justification.		
9	The proposed solution shall allow risk owners to view a consolidated risk exposure summary for assets and applications under their ownership.		
10	The proposed solution shall support recalculation of risk scores based on asset criticality, exposure, or threat intelligence.		
11	The proposed solution shall provide drill-down capability from an aggregate risk score to the underlying contributing vulnerabilities and assets.		
12	The proposed solution shall support configurable risk waiver workflows distinct from permanent risk acceptance, including defined validity periods.		
13	The proposed solution shall generate Key Risk Indicator (KRI) reports suitable for presentation to senior management and the Board, on a scheduled or on-demand basis.		
14	The proposed solution shall maintain segregation of duties between the requester, approver, and reviewer roles in all risk acceptance and waiver workflows.		
15	The proposed solution shall support automated notification to designated risk owners when new critical or high vulnerabilities materially change their risk exposure.		
16	The proposed solution shall provide historical trend reporting of aggregate risk over time, by business unit and enterprise-wide.		
17	The proposed solution shall provide role-based restrictions such that only designated risk owners or above can approve risk acceptance beyond a configurable severity threshold.		
18	The proposed solution shall enrich vulnerability records with CISA Known Exploited Vulnerabilities (KEV) catalogue status and equivalent exploited-in-the-wild intelligence, with the enrichment mechanism fully supported in an on-premise deployment.		
19	The proposed solution shall compute and display both inherent risk and residual risk (post compensating controls and exceptions) at vulnerability, asset and application level.		

Assessment Management Requirements

Requirements governing the planning, execution, tracking, and sign-off of security assessments.

Sr. No.	Requirement Description	Compliance (Yes/No/Partial)	Bidder Remarks
1	The proposed solution shall support end-to-end management of security assessments, including planning, scheduling, execution tracking, and sign-off.		
2	The proposed solution shall support multiple assessment types including application security assessments (grey/black box) & infrastructure/Cloud assessments.		
3	The proposed solution shall allow raising of assessment requests		

Public

Sr. No.	Requirement Description	Compliance (Yes/No/Partial)	Bidder Remarks
	through a structured request-for-assessment workflow with mandatory business and technical justification.		
4	The proposed solution shall maintain an assessment calendar providing visibility of planned, in-progress, and completed assessments across the organization.		
5	The proposed solution shall support assignment of internal or external testers/assessors to specific assessments with defined scope and timelines.		
6	The proposed solution shall maintain assessment status tracking (Assigned, In Progress, Pending Validation, Completed) with configurable stage definitions.		
7	The proposed solution shall support formal sign-off workflows for application golive, requiring approval from designated application/business owners.		
8	The proposed solution shall maintain a consolidated assessment summary view showing assigned and actual start/end dates, tester, status, and residual risk.		
9	The proposed solution shall support linking of assessment findings directly to the vulnerability management module for unified tracking and closure.		
10	The proposed solution shall provide re-assessment and retest tracking to validate remediation of previously identified findings.		
11	The proposed solution shall support configurable assessment frequency (one-time, periodic, ad hoc) per application or asset, with automated reminders for due reassessments.		
12	The proposed solution shall generate assessment-level synopsis reports suitable for stakeholder circulation, summarizing scope, findings, and residual risk.		
13	The proposed solution shall maintain a complete assessment history per application, including all historical assessment cycles and outcomes.		
14	The proposed solution shall allow filtering and reporting of assessments by application, tester, assessment type, business unit, and completion status.		
15	The proposed solution shall support export of assessment summary and detailed findings reports in PDF and Excel formats, with optional password protection.		
16	The proposed solution shall support linking of multiple assessments to a single application to track security posture evolution over time.		
17	The proposed solution shall provide role-based visibility such that application owners can view only assessments relevant to their applications.		
18	The proposed solution shall maintain assessment coordinator and stakeholder notification lists configurable per assessment.		
19	The proposed solution shall provide dashboards summarizing assessment coverage across the application portfolio, identifying applications overdue for assessment.		

Public

Sr. No.	Requirement Description	Compliance (Yes/No/Partial)	Bidder Remarks
20	The proposed solution shall support planning, tracking, and management of at minimum the following assessment types as distinct, individually reportable categories: Web Application, Mobile Application, API, Infrastructure Vulnerability Assessment, Internal Penetration Testing, External Penetration Testing, Database Assessment, Cloud Security Assessment / CSPM, Configuration Audit, Firewall / Network Device Rule Review, Thick Client and Thin Client Assessment, Wireless (Wi-Fi) Assessment, Secure Code Review (SCR), Software Composition Analysis (SCA), Red Team Assessment, and Third-party / Vendor Assessment.		
21	The proposed solution shall support tracking of the Application Security Life Cycle (ASLC) status of each application, including security clearance status prior to go-live and reassessment triggers upon major change.		
22	The proposed solution shall support concurrent assessments of different types on the same application or asset without data conflict.		

Exception Management Requirements

Requirements governing policy exceptions, generic exceptions, scenario-based exceptions, and risk waivers, including approval workflows.

Sr. No.	Requirement Description	Compliance (Yes/No/Partial)	Bidder Remarks
1	The proposed solution shall support multiple categories of exceptions including Vulnerability Exceptions , Risk exception, Hardening policy exceptions, generic risk exceptions and Third party / legacy risk waivers each with independently configurable workflows.		
2	The proposed solution shall require a mandatory description, business justification, and defined validity period ('exception till date') for every exception raised.		
3	The proposed solution shall support configurable multi-level, sequential approval hierarchies (Level 1, Level 2, Level n) where each subsequent approver may act only after the preceding level has approved.		
4	The proposed solution shall allow designation of coordinators who are notified of exception requests without possessing approval or processing authority.		
5	The proposed solution shall require a mandatory comment on every approval or rejection action, retained as part of the permanent audit trail.		
6	The proposed solution shall automatically route an exception request to the next approval level upon approval at the current level, without manual intervention.		
7	The proposed solution shall provide administrators the ability to add, modify, or retire exception categories, subject to a maker-checker (dual control) approval process.		
8	The proposed solution shall automatically flag and update the status of exceptions that pass their expiry date, and prevent further processing of expired exceptions without re-initiation.		
10	The proposed solution shall maintain a complete audit history for		

Public

Sr. No.	Requirement Description	Compliance (Yes/No/Partial)	Bidder Remarks
	every exception, including all approval/rejection actions, comments, and timestamps.		
11	The proposed solution shall allow attachment of supporting documents (e.g., compensating control evidence) to an exception request, subject to file type and size restrictions.		
12	The proposed solution shall support cancellation or withdrawal of a pending exception request by the requester, subject to an audit trail entry.		
13	The proposed solution shall provide a dashboard summarizing exceptions by status (Open, Approved, Expired, Pending Re-evaluation) across the organization.		
14	The proposed solution shall support bulk reporting and export of exception records, including linked vulnerability or asset references, for audit purposes.		
15	The proposed solution shall send automated reminder notifications to approvers and requesters in advance of exception expiry.		
16	The proposed solution shall restrict the ability to raise, approve, or configure exceptions strictly according to role-based permissions.		
17	The proposed solution shall support linkage of an exception record to one or more specific vulnerabilities, assets, or applications for full traceability.		
18	The proposed solution shall provide a re-evaluation workflow requiring justification and fresh approval when an exception is extended beyond its original expiry.		
19	The proposed solution shall maintain segregation between the requester and approver roles such that a requester cannot approve their own exception request.		
20	The proposed solution shall support configurable notification distribution lists (requester, coordinator, approvers) triggered at each stage of the exception lifecycle.		
21	The proposed solution shall allow download of a complete exception report, including audit history and all submitted details, in a standard document format.		
22	The proposed solution shall provide filtering of exception records by category, status, requester, approver, expiry date, and linked asset/application.		
25	The proposed solution shall support configurable escalation of exception approvals pending beyond a defined threshold period.		
26	The proposed solution shall track exception ageing and exception-ownership ageing as reportable metrics, with dashboards and reports of exceptions by configurable age bucket, owner and business unit.		

Workflow Requirements

Requirements governing configurability, governance, and automation of business workflows across all modules.

Public

Sr. No.	Requirement Description	Compliance (Yes/No/Partial)	Bidder Remarks
1	The proposed solution shall provide a configurable workflow engine allowing to define approval chains, escalation paths, and status transitions without vendor code changes.		
2	The proposed solution shall support conditional workflow routing based on asset criticality, vulnerability severity, business unit, or exception category.		
3	The proposed solution shall enforce segregation of duties within workflows such that maker and checker roles cannot be held by the same individual for a given transaction.		
4	The proposed solution shall provide a visual workflow designer or equivalent configuration interface for administrators to define and modify workflows.		
5	The proposed solution shall allow delegation of workflow approval authority to a designated alternate during periods of unavailability, with full audit logging.		
6	The proposed solution shall provide a consolidated task/inbox view for each user showing all pending workflow actions across modules		
7	The proposed solution shall maintain complete audit trails of every workflow action, including actor, action, timestamp, and comments.		
8	The proposed solution shall support bulk approval/rejection actions within workflows, subject to role-based permission and mandatory comments.		
9	The proposed solution shall provide configurable notification triggers at each workflow stage (initiation, approval, rejection, escalation, expiry).		
10	The proposed solution shall allow reassignment of pending workflow tasks by an administrator in the event of staff transition, with audit trail.		
11	The proposed solution shall support integration of workflow status with external ITSM/ticketing tools for unified tracking.		

Notification Requirements

Requirements governing automated alerts, reminders, and escalation notifications across the Solution.

Sr. No.	Requirement Description	Compliance (Yes/No/Partial)	Bidder Remarks
1	The proposed solution shall send automated email and/or in-application notifications for key events including initiation, approval, rejection, expiry, and escalation.		
2	The proposed solution shall provide configurable notification frequency (real-time, daily digest, weekly digest) per user or role.		
3	The proposed solution shall support integration with SMTP infrastructure for outbound email notifications, including support for TLS-secured relay.		
4	The proposed solution shall provide in-application notification badges/counters reflecting pending actions specific to the logged-in user.		
5	The proposed solution shall support SLA breach notifications		

Public

Dashboard Requirements

Requirements governing role-based, real-time visual representation of security and risk posture.

Sr. No.	Requirement Description	Compliance (Yes/No/Partial)	Bidder Remarks
1	The proposed solution shall provide role-based dashboards presenting relevant metrics to each user category		
2	The proposed solution shall provide a consolidated executive dashboard summarizing overall risk posture, open vulnerabilities by severity, SLA compliance, and exception volumes.		
3	The proposed solution shall provide real-time visualization of asset inventory composition, including assets with and without open vulnerabilities.		
4	The proposed solution shall provide drill-down navigation from any dashboard widget to the underlying detailed record set.		
5	The proposed solution shall provide trend charts for vulnerability discovery and closure rates over configurable time periods.		
6	The proposed solution shall display top vulnerabilities, top affected applications, and top affected assets by count and severity on a summary view.		
7	The proposed solution shall provide a risk score matrix/heat map view combining asset criticality and vulnerability severity.		
8	The proposed solution shall support dashboard filtering by business unit, asset group, application, and date range.		

Reporting Requirements

Requirements governing the Solution's standard and custom reporting capabilities.

Sr. No.	Requirement Description	Compliance (Yes/No/Partial)	Bidder Remarks
1	The proposed solution shall provide a library of standard reports including Executive Reports, Board Reports, CISO Dashboard Reports, Compliance Reports, Risk Reports, and Asset Reports.		
2	The proposed solution shall support ageing reports categorizing open vulnerabilities by configurable age buckets		
3	The proposed solution shall generate standard Key Risk Indicator (KRI) and Key Performance Indicator (KPI) reports suitable for regulatory and Board submission with minimal manual effort.		
4	The proposed solution shall support export of all reports in Excel and PDF formats, with optional password protection for sensitive reports.		

Basic Requirements:

Sr No	Technical Requirements	Compliance (YES / NO)	Bidders Remark
Deployment Requirements			

Public

1	Must operate completely within the organization's on-premise data centre.		
2	No reliance on external cloud services for scanning, storage, or updates.		
3	Support offline/air-gapped update mechanisms.		
4	Provide high availability, scalability, and on-prem backup/DR options.		
5	The solution should be able to integrate with SOAR, SIEM, Incident Management Tool, Change Management Tool, Ticketing Tool, GRC tool, Network Monitoring Solutions, Proxy, NAC, Email Gateways, ASE, Sandbox etc.		
6	Solution should support custom integrations through REST APIs, SOAP APIs, Utility Based integrations i.e. SSH, WEBHOOKS etc		
7	The solution must support backup and restore. Backup must contain at least: solution configuration, alerts, databases, classification policies, exception policies, notifications, etc. Restore operation should be user friendly, less complicated.		
8	Solution must support multiple OS platforms such Windows, Linux, MacOS, Virtualization platforms such as Hyper-V, Esxi, KVM, Nutanix etc.		
5	Must integrate with on-prem AD/LDAP/SAML for authentication and group mapping.		
6	Must maintain complete, on-prem audit logging of all user activities.		
Note: The Bidder may provide the additional features and functionalities of their proposed solution			

Public

Annexure - B: Inventory

List of Inventories will be shared to Successful bidder.

Annexure – C: Bidder's Organization Profile:

S/N	Particulars	Bidders Comment
1	Name of Bidders Company	
2	Registered Office Address	
3	Date of Incorporation	
4	Contact Person Phone and Email	
5	Director, MD & CEO Name, and contacts	
6	Total Employee count PAN India	
7	Brief description of the Bidder including details of its main line of Business	
8	Company /firms website URL	
9	Authorized Signatory of the Bidder (Name, Designation, address, contact no., email)	
10	Income Tax. No. (GST/PAN/GIR). Please enclose photocopy of latest income tax clearance certificate	
11	Bidders support office presence at Mumbai. In addition in Ahmedabad will be preferred	
12	Total No. of clients in India for the bidder for similar implementation SCR & Other endpoint Security Solutions	
13	Total number of clients in for similar services (Data Privacy exercise, assessment, implementation)	
14	Turnover and Net Profit of the company (Rs. In Crores)	

Public

Annexure – D: Compliance for Eligibility Criteria

#	Eligibility Criteria	Compliance (Compliant /Not Compliant)	Supporting Evidence
1.	The bidder should be a current legal entity with a minimum 3 years' experience of SCR solution implementation/support in India.	Y/N	Certificate of Incorporation or Appropriate Supporting Document, past PO not more than 5 years old
2.	The bidder should have performed implementation/support for at least three clients during the last 3 financial years, with at least one of which should be a large private. Kindly furnish details of the same in the Technical Proposal.	Y/N	Customer references to be provided & Copies of Purchase Orders
3.	The bidder must submit an undertaking that no Government / undertaking organizations have blacklisted the bidder for any reason. Past/present litigations, disputes, if any (Adverse litigations could result in disqualification, at the sole discretion of the Company)	Y/N	Undertaking by Bidder.
4.	Financial statements i.e., Audited Balance sheet and Profit & Loss accounts for last three years (FY2022-23 and FY2023- 24, FY2024- 25)	Y/N	Financial / Profit Loss statements certified by auditor

Annexure – E: SLA & Penalties:

The successful Bidder shall enter into a Service Level Agreement (SLA) with the MCX, containing all the Terms and Conditions of this RFP, including confidentiality, non-disclosure, Personal Data Privacy, Right to Audit, Penalty clauses, and any other clause relevant to the services offered.

Delivery of services should be completed as per MCX Group requirement of acceptance of Purchase Order. Extensions and delayed delivery will attract penalties.

Delivery for the in-scope activities is deemed to be complete only when all the items specified in the Purchase Order are completely delivered and date of delivery is the date on which the last service / activity is delivered.
If the delivery schedule is not maintained as stated or to such extended period as per stated in this RFP, a penalty of half percent (0.5%) of the item cost, for each week or part thereof of the delay subject to a maximum of 5% will be levied from the expiry date of delivery. The penalty for delayed delivery shall be computed scope area-wise, and the maximum penalty shall be 5% of the item cost.
Vendors need to strictly adhere to Service Level Agreements (SLA) computed on parameters as per industry's best practice. Services delivered by vendor should comply with the SLA

Public

mentioned in the table below. SLA will be calculated as below.

Sr No	Incident/Outage Type	Response SLA	Resolution SLA	TAC Support
1	Critical (P1)	10 Mins	2 hours	2 hours
2	High (P2)	30 Mins	4 hours	8 hours
3	Medium (P3)	60 Mins	24 hours	36 hours
4	Low/Info (P4)	180 Mins	36 hours	48 hours

SLA violation of the above table linked with service area mentioned below will attract penalties as below.

Sr No	**Service Area**	**Accepted Service Level**	**Penalty**
1	**UP Time of solution or any component there of: -** (Hardware, software, appliances, etc. supplied by selected Bidder). Impact on Production, demanding immediate attention. Leading to the complete disruption of the objective performed by the said solution.	99.995% and above	NA
		99.99% to 97.92%	1%
		97.91% to 95.83%	5%
		Less than 95.82%	10%
2	**Degradation of Solution** - Slowing down the operations of any component or solution thereof resulting in delayed alerts, responses, report generations, etc. resulting in business impact	Response and resolution time of 24 hours after reporting to SI/OEM support.	1% every four hours after the passage of Resolution time of 24 hours. The cap will be **10% of AMC.**
3	**Maintenance** Management – Version / Release/Upgrades / Patches	Bidder to inform MCX team and ensure that all components of Solution – firmware, software, middleware, etc. are updated with latest firmware, patches, upgrades, release, version, etc. as per the MCX policy(N-1).	Penalty of 2% for every fortnight for **not informing** the MCX of latest versions / release/upgrades/ patch for NAC solution upon its release. • Penalty of 2% for every week for **not informing** of critical security patches of NAC solution. • Penalty of 2% for every week of delayed updating/patching **beyond mutually agreed** upon. time schedule for any component of NAC once notified by the MCX. **Cap of 10% of AMC**

Public

1. Penalty for Delayed Delivery:

a Bidder / Vendor must provide hardware appliance (if required) for implementing solution. If the solution is VM based MCX shall provide VMs are desired for by the solution requirements projected by the bidder.

b Delivery / installation of Solution as a Software or Hardware based at MCX's DC & DR locations should be completed as per MCX requirement of acceptance of Purchase Order. Extensions and delayed delivery will attract penalties.

c Delivery / installation for the above purpose is deemed to be complete only when all the items specified in Purchase Order are completely delivered (Location wise) and date of delivery is the date on which the last item is delivered.

d If the delivery schedule is not maintained as stated or to such extended period as per stated in this RFP, a penalty of half percent (0.5%) of the item cost, for each week or part thereof of the delay subject to a maximum of 5% will be levied from the expiry of due date of delivery. The penalty for delayed delivery shall be computed location wise and maximum penalty shall be 5% of the item cost.

2. Penalty for Delayed Implementation:

a The Successful bidder (SB) is expected to complete the installation, implementation & operationalization of the solution as per the scope of work mentioned in this RFP within 08 weeks from date of date of issuance of PO. Along with at DC/DR fail-over and fail-back. Any delay / deviation from the above said shall attract penalties as follows.

b A penalty of half (0.5%) percent of total order value (PO Value) for each week or part thereof with a maximum cap of 5 % will be levied and deducted from the amount payable to Bidder.

c In case the delivery, installation & implementation of the solution is not completed within a maximum of 08 weeks from the date of acceptance of the Purchase order, MCX may at its discretion provide an opportunity to the service provider to submit reason if any for such delay. MCX shall evaluate such submission and its applicability and MCX decision in this regard shall be final and binding.

d Failure of the successful bidder to comply with the above installation schedule, as stipulated, shall constitute sufficient grounds for the annulment of the award of contract and invocation of bank guarantee (delivery). In such an event MCX will call for fresh bids and MCX shall have the right to blacklist the bidder for a period of one year.

Public

Annexure - F: Commercial Bid

1. DAST Tool:

TABLE I – COST OF HARDWARE/SOFTWARE:

Sl. No	Description	Qty (a)	Unit Price (Rs.) (b)	Total price (Rs.) (a*b)
1	Cost of software for 3-year with implementation for the following options: (Bidder should provide break-up of cost)	**for 3 year`s)**		
	Total cost			
	TAXES			

Sr. No	Commercial	Vendor Comments (Yes/No/Remark)
1	Please confirm that serial no 1 is considered for the commercial	
2	Please confirm that Software and licenses cost includes	
3	Support for 3 years: After sign-off one+ month of KT, handholding and training and then after online support (phone, email, virtual) and onsite as and when required	
4	Comprehensive warranty will start after 3 years with same product/ licenses/ features & services	
5	Confirm License type (perpetual/subscription based)	
6	Payment Terms: 1. For supply of Hardware/Appliance, licenses & implementation MCX will pay 90% after successful installation/implementation post sign off within 45days, 5% after 6 months from installation within 45days and 5% after 12 months from installation within 45days - for 1st year	
7	2) From 2nd year onwards for licenses/services payment will be yearly within 45 days	
8	Confirm the commercial you shared includes licenses cost for base software + user licenses.	
9	Mention the support type you will be providing	

Public

10	Bidders required to sign Agreement/Legal document with the Exchange. Until unless Agreement is not signed, payment will not be processed.	
11	Any deviations in Payment Terms, bidder should inform MCX in advance.	
12	Two references where the same solution is deployed by your company as a SI - Name, contact number, company name and designation - preferably exchange or banks	
13	There should not be any license restriction for the MCX user.	
14	How many simulators will be provided with the package	
15	No restriction in user creation in the application for MCX	
16	On demand activity to be performed related to the product apart from specified frequency mentioned by OEM/Partner	

TABLE II – COST OF IMPLEMENTATION:

Sl.No	Description	Total Cost (Rs.)
1	Total Cost of one-time installation and Implementation of solution at DC and DR (As mentioned in Table I)	
2	**Total Implementation Cost**	
3	**Taxes**	

Sr. No	**Commercials**	**Vendor Comments (Yes/No/Remark)**
1	Delivery / installation of Solution as a Software or Hardware based at MCX's DC & DR locations should be completed as per MCX requirement	
2	All support during Implementation by bidder/OEM must be provided onsite	
3	Resource allocation for implementation will be mutually decided.	
4	End to end implementation of solution, agent deployment, troubleshooting and configuration of databases and clusters	

Public

5	MCX has the authority to examine the resources for competency and mention the number of resources present during installation.	

TABLE III-AMC &ATS FOR SOLUTION

Sr	Description	Unit Price (Rs) A	Qty B	Total Price (Rs.) C=A*B
1.a	4th year AMC & ATS for SCR solution (DC&DR) after comprehensive warranty			
1.b	5th year AMC & ATS for SCR solution (DC&DR) after comprehensive warranty			
2	**Total Cost**			

Sr. No	Commercials	Vendor Comments(Yes/No/Remark)
1	Above mentioned conditions and request will be applicable for 4th & 5th year as well, in-case we plan for the continuation	
2	Online support (phone, email, virtual) and onsite as and when required for 4th & 5th Year	
3	Comprehensive warranty will start after the initial 3 years	
4	Payment terms for 4th year & 5th year for licenses/services payment will be yearly within 45days subject to satisfactory service delivery and SLA compliance.	

TABLE IV– TOTAL COST OF OWNERSHIP (TCO) For Source Code Review Capabilities:

Sl.No	Description	TABLE	Total Price (Rs.)
A	**Total amount**	**TABLE I**	
B	**Total amount**	**TABLE II**	
C	**Total amount**	**TABLE III**	
D	**GRAND TOTAL**		
E	**Taxes**		

Note:

Public

a. For Table I – bidders shall submit Bill of Materials (Quantity, Make and Model) and break up of cost of each component.

b. MCX may plan to purchase components in phased manner as per requirement.

c. If solution is appliance based, bidder to include cost accordingly. If it is VM based, MCX will provide the VM Infra.

d. All software supplied under this bid shall be of enterprise class with OEM support.

e. If the cost for any line item is indicated as zero, then it will be assumed by the MCX that the said item is provided to MCX without any cost.

f. The prices quoted above shall be considered for all the deliverables stated in this RFP document. No extra costs other than those quoted above shall accrue to the MCX.

g. The prices quoted by the bidder shall be exclusive of taxes (GST) and inclusive of all duties, levies, entry tax (wherever applicable).

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

i. Solution Warranty will commence only after successful implementation only after signoff from MCX IS team. All AMC/ATS will be applicable based on implementation signoff.

j. The license provided should include all functionalities and capabilities of the solution mentioned in the technical specifications, RFP requirements and scope of work. No separate costs are allowed.

Payment Terms:

1. For supply of Hardware/Appliance, licenses & implementation MCX will pay 90% after successful installation/implementation post sign off, 5% after 6 months from installation and 5% after 12 months from installation.
2. Bidders required to sign Agreement/Legal document with the Exchange. Until unless Agreement is not signed, payment will not be processed.
3. Any deviations in Payment Terms, bidder should inform MCX in advance.

Annexure–G: Notification, Confidentiality, Termination Clause

Notification:

MCX Group may in its absolute discretion apply selection criteria specified in the document for evaluation of proposals for short listing / selecting the eligible Bidder. MCX Group is not obliged to provide any reasons for such acceptance or rejection as evaluation process entirely internal.

The Exchange reserves the right to amend or modify the contents of RFP at any time before the date of bids submission. The decision of the Management Committee of MCX Group shall be final Submission of proposal notifies deemed acceptance of terms as mentioned in this RFP by Bidder**.**

Confidentiality:

The RFP document is strictly confidential and is not to be disclosed, reproduced, published in any manner, transmitted, or otherwise made available by the Recipient to any other party. MCX Group may update or revise the RFP document or any part of it at its sole discretion. The Recipient acknowledges that any such revised or amended document received by it shall be subject to the same terms and conditions as this original and subject to the same confidentiality

Public

undertaking. All Information pertaining to the Exchange obtained by the Service Provider because of participation in this RFP / project is confidential and must not be disclosed without prior written authorization from the Exchange**.**

Termination Clause

If the product / solution / services are not found to be satisfactory or if there is any non-compliance in product / service with respect to RFP or breach of delivery terms, SLA, uptime then MCX Group reserves the right to terminate the contract / Purchase Order (PO) giving notice to the bidder. The bidder should refund the payment made by MCX Group, if any.

If delivery and services are not completed within as per project timelines, MCX Group reserves the right to terminate the PO. The bidder should refund the payment made by MCX Group if there is any.

Annexure–H: Bank Guarantee (Procurement Team) if Applicable

Bidder to provide performance Bank Guarantee till warranty period if applicable.

Annexure – I: IT Act & Free from Malware/Backdoor Certificate (If applicable):

Information Technology Act Clause – Free of Malware/Backdoor/Harmful code

The Vendor understands and acknowledges that certain systems/computer resources/equipment/setups of MCX are identified as a Critical Information Infrastructure ("CII"). Therefore, All the Laws/ rules/ regulations and guidelines applicable to CII's and Protected Systems including the *"Information Technology Act, 2000"* and *"Information Security Practices and Procedures for Protected Systems",* set out in Gazette notification dated 22nd May 2018, shall be applicable to MCX.

The Vendor represents and warrants that: (1) the Vendor and/or its personnels shall always comply with the required laws, regulations and guidelines, applicable to the them, to ensure safety and security of MCX's CII's and Protected Systems; (2) the Vendor and/or its personnels shall not damage/harm MCX's systems/computer resources/equipment/setups; (3) the Vendor and/or its personnels shall not try to obtain unauthorized access to MCX's systems/computer resources/equipment/setups; (4) Vendor and/or its personnels shall not plant or place any harmful code, virus, self-propagating program, Trojan horse, trap door, backdoors or any other kind of harmful code or program in MCX's systems/computer resources/equipment/setups; (5) The Vendor and its personnel shall not leak and/or misuse the information stored and available on MCX's systems/computer resources/equipment/setups. Furthermore, the Vendor agrees to indemnify and keep indemnified, hold harmless and defend MCX against any/all loss, claims damage and penalty, that may be incurred by MCX, due to breach of Vendor's representations and warranties, as mentioned in this provision. In addition to the above the Vendor may also be liable for the punishment and/or penalty prescribed under the applicable laws (including the Information Technology Act, 2000).

Public

Information Security Requirements for RFPs (Technology - Products & Services)

1. Product/Service should have security certifications (Common Criteria EAL 3 and above or equivalent for products and SOC2/ISO 27001:2022 or equivalent assurance certificates for services) and submit reports/evidence.
2. Product/service should undergo security testing (VAPT, SAST, DAST etc)/audit before go-live and post go-live by CERT-In empaneled auditor and must close the identified security vulnerabilities within timelines without any cost implication to MCX.
3. In case of software, Bidder/OEM must provide full details of Software Bill of Material (SBoM) with libraries, open-source components etc. and certify no vulnerable component/libraries or used. Should ensure support for security patches and upgrades as and when required.
4. Bidder must have BCP setup and participate/support in cyber drills/exercises conducted by MCX from their product/service perspective.
5. Product/service must have support for integration with C-SOC tools (SIEM, EDR/XDR, SOAR, WAF, PAM etc.) through Syslog/API/CEF for security log monitoring and incident response at no additional cost to MCX.
6. Bidder must submit "Software/appliance are Free from malware/Backdoor" certificate. Clauses related to data security and privacy as per IT Act/ DPDP Act requirements must be part of NDA/agreements.
7. Right to audit/access to bidder environment or location if required by MCX, third party auditor appointed by MCX and/or regulatory body.
8. Selected bidder to demonstrate the security features in POC.

Bidder shall adhere to the relevant regulatory requirements (Existing or as and when received) of SEBI, NCIIPC, Cert-In and other regulators

Public

Public