INDIA INTERNATIONAL BULLION EXCHANGE IFSC LTD

Unit No. 1302A, Brigade International Financial Centre,

13th Floor, Building No. 14A, Block 14, Zone 1, GIFT SEZ, GIFT CITY, Gandhinagar, 382 050, Gujarat

Phone: +91 79 6969 7100

Email: info@iibx.co.in

REQUEST FOR PROPOSAL (RFP)

Hybrid Security Operations Centre

Issue Date
01-Sep-2025

CONTENTS

1. ABOUT INDIA INTERNATIONAL BULLION EXCHANGE IFSC LTD

India International Bullion Exchange IFSC Limited is India's first international bullion trading platform, inaugurated by Hon'ble Prime Minister Shri Narendra Modi on **July 29, 2022**, at GIFT City in Gandhinagar, Gujarat. It operates under the regulatory framework of International Financial Services Centres Authority (IFSCA) and is promoted by key national market infrastructure institutions viz., NSE, MCX, NSDL, CDSL and BSE (through India INX and India ICC) whereby these MIIs have equal stake in the holding company, India International Bullion Holding IFSC Ltd (IIBH) and in turn IIBH holds 100% stake in IIBX.

Key Points about IIBX

- **Spot Market Platform & BDRs**

IIBX offers T+0 trading in the form of Bullion Depository Receipts (BDRs) for Gold & Silver stored in Vaults registered with IFSCA and empanelled by India International Depository IFSC Ltd. (IIDI).

- **Launch of Futures Contracts (USD-denominated)**

Futures Trading in Gold and Silver was launched on IIBX in June 2024 and August 2025 respectively with comparable international pricing, offering Indian stakeholders an onshore hedge against price volatility.

- **Direct Import Access for Qualified Jewellers & TRQ Holders**

Qualified Jewellers and TRQ holders under the India–UAE CEPA can directly import bullion using IIBX.

- **Clearing & Settlement Infrastructure**

IFSCA-regulated IFSC Banking Units (IBUs) act as Clearing Banks, facilitating trade settlement in U.S. Dollars.

- **Regulatory Improvements**

With the introduction of the IFSCA (Bullion Market) Regulations, 2025, the Exchange expanded trading hours and relaxed net worth criteria for many categories of participants to foster broader access to its products and services.

- **Transparent Price Discovery & Quality Assurance**

  IIBX ensures transparent access to live bullion prices and quality-assured supplies & elevating market integrity.

- **Hedging in U.S. Dollars**

  With futures trading in USD, participants gain the ability to hedge bullion exposure onshore—avoiding reliance on overseas Exchanges.

✅ **In Summary**

IIBX represents a significant leap forward in India's bullion ecosystem—offering a transparent, efficient, and well-regulated marketplace for gold and silver. By combining onshore price discovery, direct import access, extended trading hours, and USD-settled Futures, the platform empowers domestic jewellers, bullion traders, refiners, and international suppliers to manage risk, enhance liquidity, and participate in an emerging global bullion hub centred in GIFT City.

2. EXECUTIVE SUMMARY

IIBX is emerging as a focal point for import of Bullion in India. IIBX also provides products for hedging the price risk in bullion. IIBX endeavours to provide best in class technology to gain the competitive edge in the market.

IIBX would like to setup a Security Operations Centre (SOC) at its own Data Centre at GIFT City Gandhinagar and inviting the proposals from the Technology partners / Original Equipment Manufacturers (OEM) of the Security Products for setting up and managing the SOC for IIBX.

3. TECHNICAL SPECIFICATIONS (SCHEDULE 1)

A. SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

1. Architecture & Scalability

- Must support 150 devices and 4500 EPS from Day 1, scalable up to 1,00,000 EPS or 500 devices/servers.
- Provide scale-out distributed architecture with collectors (virtual or physical appliances) that can cache logs if the storage/correlation tier is unavailable, compress logs before sending, and limit bandwidth usage.
- Storage and correlation tier (SIEM Cluster) must support both virtual and physical appliances, with no license limit based on storage size.
- Support 10:1 log compression, HA at all layers (collectors, database, leader nodes), and automatic failover with DR Support.
- Multi-tenant by default for departmental data segregation and analytics.
- Must support big-data storage and long-term historical data retention (at least 6 months online + 24 months offline).
- Support policy-based data archiving and restoration via GUI.
- No additional license fees for extra collection/processing nodes or HA.

2. Log Collection & Data Handling

- Collect logs via agent-based and agentless methods (syslog, JDBC, API, WMI, FTP/SFTP/SCP, SNMP, MQ, etc.).
- Collect additional context from devices via protocols like SNMP, WMI, SSH, Telnet, JDBC, OPSEC, JMX, and PowerShell.
- Support collection of flow data (S-Flow, J-Flow, NetFlow) and correlate all fields.
- Allow real-time event filtering at collectors without license impact.
- Collect and store raw, parsed, and enriched data in a tamper proof manner.
- Build parsers automatically; custom parsers editable in GUI without CLI.
- Must ingest logs from any source without prior parser creation.
- Support local log caching, encrypted transfer, and multiple destinations for log forwarding.
- Enrich logs with business context at collection layer.

- Support monitoring of Windows/Linux devices, network configurations, file integrity, registry changes, certificate status, and application/process lists.
- Provide built-in forensic investigation tools (OSQUERY, remote queries, baseline comparisons).

3. Analytics & Search

- Unified analytics interface for logs and performance data, with nested queries and real-time search before data is stored.
- Support searches combining CMDB and event data (e.g., non-reporting critical servers).
- Provide 3000+ reports and 2000+ correlation rules with content updates independent of software releases.
- Detect anomalies, algorithmically generated domains, and unusual spikes in activity.
- Support UEBA (User & Entity Behaviour Analytics) with baselining, anomaly detection, off-network log collection, USB monitoring, data exfiltration alerts, and application detection (e.g., TOR, gaming, uncommon VPNs).

4. Threat Intelligence & AI

- Include native OEM threat intelligence feed (CTA member) and integrate external TI feeds (REST API, CSV, domains, hashes, URLs, malware process names from organizations like NCIIPC, CERT-IN, NIST).
- Correlate TI data in real-time and historically with event data.
- Provide Python-based framework for custom TI integrations.
- Integrate with Generative AI (e.g., OpenAI/ChatGPT 4.0) for:
    - SOC health queries
    - Risk predictions
    - Report creation from aggregation/raw queries
    - Case analysis and enrichment
    - Incident response guidance based on threat category
- Support custom Machine Learning (ML) model creation, training, and automated rule triggering.

5. Incident, Case & Response Management

- Provide built-in case/ticketing system or integrate with tools like ServiceNow, Service Desk Plus (Manage Engine), ConnectWise, Remedy.
- Support escalation policies, SLA monitoring, PDF/PNG attachments, assignments, timelines, MTTR metrics.
- Provide automated case creation/assignment, SLA violation detection, and case dashboards (health, KPI, handling metrics).
- Enable automated/manual incident response and remediation via integrated playbooks or SOAR integration.
- Support false positive detection (CVE-based IPS analysis, IOC validation) and automated incident resolution recommendations via ML.
- Integrate with EDR tools without dependency on EDR agents for log collection.

6. Compliance, Dashboards & Reporting

- Provide dashboards for PCI status, MITRE ATT&CK mapping, SLA breaches, risk scoring (based on severity, criticality, rarity, frequency, vulnerabilities), and entity ranking.
- Out-of-the-box compliance reports at no extra cost.
- Support configurable watch lists for critical violators, location/user-IP mapping, and event enrichment without user context.
- The proposed solution shall allow setting SLA's for different milestones within each incident investigation and response action.
- There shall be a live timer on the dashboard that shows SLA time remaining for each milestone for the analyst to keep a track of live incidents.

7. Security, Access & Integration

- Role-based access control for data and GUI, with authentication via RADIUS/Microsoft AD.
- Maintain full audit logs of all administrative and system activities.
- Integrate with Phone/SMS/email gateways for alert notifications.
- Send alerts via SMTP, syslog, Kafka (producer/consumer).
- Support integration with on-prem and cloud devices, and with both log and flow data in a single interface.

B. SECURITY ORCHESTRATION, AUTOMATION & RESPONSE (SOAR)

1. General Solution Requirements

- Must be an on-premises solution, scalable in use cases and performance to ensure quick response to attacks.
- HA and automatic failover with DR Support
- Accept security alerts from all data sources in any format, supporting unlimited alerts/incidents and unlimited action executions without license limits.
- Integrate across platforms for event triage, case management, ticketing, and security actions (e.g., firewall blocking, DNS updates, Windows/Linux tasks, application geo-location scripts).
- Provide an intuitive GUI and wizard for incident creation via manual entry, API, web URL, or SIEM.
- Support LDAP authentication and creation of users/groups with role-based access.
- Allow storage of incident-related files (malware, logs, screenshots, etc.).
- Licensed for at least two users from day one.
- SOAR Solution should be proposed with both options, and IIBX will decide which option to adopt. [Mandatory to propose both options]

  Option 1 (Subset Model) – SOAR deployed as a subset of the Managed Service Provider platform under a Master Controller at MSSP's premise, integrated with MSSP services.
  Option 2 (Dedicated Instance) – SOAR deployed as a dedicated tenant on the IIBX environment. If IIBX opts for this option, no connectivity except remote access for configuration will be provided to the MSSP cloud.

2. Playbook Features

- Visual playbook builder supporting manual actions, decision steps, nested playbooks, loops, conditions, Python scripting, rich-text emails, tagging, and troubleshooting.
- Enable remediation and system actions (e.g., block user, disable account, update ticket, request approvals).
- Store playbooks in a structured manner with version control, rollback, cloning, and ability to mark public/private.

- Execute playbooks manually, on schedule, on data update, or via API triggers.
- Support concurrent playbook execution with scalability via additional nodes/licenses.
- Include built-in debugging tools, error-handling options, mock outputs, and step alignment.
- Allow bulk editing of steps (delete/copy across playbooks) and categorization (e.g., data ingestion vs. others).
- Resume execution from a failed step and export playbooks (single or linked) with all saved versions.
- Enable approval before automated actions and track playbook runs per incident.

3. Connectors & Integrations

- Provide at least 500+ vendor-validated connectors on day one with related documentation.
- Support custom connector development via SDK, with health monitoring dashboards and RBAC controls for actions.
- Include in-life connector updates without requiring full system upgrades.
- Offer user-friendly data ingestion wizards and remote SOAR agents for segmented networks with auto-upgrade capability.

4. Indicators & Threat Intelligence

- Maintain a central "Indicators" database with correlation across multiple alerts.
- Bulk import, update, and export indicators, assign reputations (manual or via threat intel feeds), and tag by event, campaign, attacker, and vector.
- Link indicators to Cyber Kill Chain phases and retrospectively check new IOCs against historical alerts.
- Include a vendor-neutral Threat Intelligence Platform (TIP) with one native OEM feed (CTA member) and support for multiple sources/formats (JSON, XML, STIX, free text) with TAXII export.
- Support custom tagging/scoring of indicators and native integration for running multiple custom playbooks from TIP.

5. Audit Trails & Logging

- Maintain granular audit trails for incidents (manual and automated actions) and system events (logins, updates, configuration changes) with details like category, user, IP, and timestamp.
- Present incident audit trails in clear timelines showing action sequences.
- Support log forwarding to syslog/SIEM (Fortinet, Splunk, Microsoft, QRadar, etc.) and ingestion from multiple SIEM sources.

6. Dashboards & Reporting

- Provide multiple configurable role-based dashboards (e.g., analyst, SOC manager) showing alerts, tasks, SLA breaches, ROI, KPIs, and SOC metrics (MTTD, MTTC, etc.).
- Include integration health and connector status dashboards, plus a framework for building/importing custom widgets (HTML/JSON/JS).
- Support custom dashboards without extra cost.

7. Incident & Alert Management

- Automatically group duplicate alerts into single incidents and prioritize based on environmental context.
- Support manual/automated evidence collection, war-room collaboration, and correlation of incidents across IOCs and artifacts with timeline visualization.
- Provide false-positive detection mechanisms and visualization of incident resolution progress.
- Maintain central web-based incident administration.

8. Security, Compliance & Authentication

- Out-of-the-box DPDP compliance module for SOC operations.
- RBAC enforcement for connectors, dashboards, and system actions.

9. AI & Automation Features

- Include bots for automated threat investigation.
- ML-based risk scoring for incident prioritization.
- Generative AI to provide contextual responses on schedules, expressions, procedures, etc.

C. THREAT INTELLIGENCE PLATFORM (TIP)

1. Deployment & Infrastructure

- Must be an on-premises solution with details of required hardware infrastructure and storage provided.
- No limitation on number of user accounts or devices to which threat feeds can be sent.

2. **Threat Feed Capabilities**

- Provide threat feeds for ransomware, malware, phishing, and hash values at a minimum.
- Include risk scoring with threat feeds.
- Support multiple data formats for exporting feeds to destinations.
- TIP should provide automation and workflow capability, including a threat library or database, which allows for easy searching, manipulation and enrichment of data.
- TIP should be able to consume intel from multiple structured data format like JSON, XML, STIX, free text and any other text data. It should support export of data through TAXII.

3. Integration & Data Sharing

- Support bi-directional integration with platforms such as SIEM, next-gen firewalls, and other security systems to send and store matched values.
- Allow querying and reporting on data correlated with threat feeds.

4. Detection & Asset Reporting

- Report internal assets/devices communicating with entities in threat feeds.
- Provide a geographical attack view to visualize threat origin and spread.

5. Dashboards & Reporting

- Offer a single centralized dashboard showing the latest indicators of compromise (IOCs) and enable customized reporting.

D. REQUIREMENTS FOR IMPLEMENTATION & MAINTENANCE

1. SOC Deployment & Project Management

- MSSP to assign a dedicated project team to plan, install, configure, conduct UAT, and move SOC technologies to production.
- Engage with IIBX SPOC to define execution approach, develop a project plan, identify prerequisites, schedule activities, and define sign-off criteria.
- Conduct regular governance meetings, provide progress reports, and share installation/integration/configuration documentation.
- Develop SOC blueprint design and architecture/SOP documentation for approval before implementation.
- Interface with technology leads for log source integration and custom parser development if required.
- Configure initial threat detection rules, reports, and dashboards based on infrastructure.

2. SIEM & SOAR Setup and Customization

- Set up and configure SIEM and SOAR platforms. Integration with all IIBX Infra devices.
- Unlimited custom log parser development for any proprietary or legacy format.
- Integration of non-standard log sources (text files, custom APIs).
- Create custom connectors for unsupported tools.
- Configure SLA parameters in SOAR and share SLA reports (daily/weekly/monthly).
- Develop and tune SOAR playbooks as per environment and agreed workflows, including automated case logging, enrichment, and response.
- Support playbook chaining, nested logic, and custom automation scripts (Python/Bash).
- Manage SIEM use case lifecycle, rule creation, and enhancements.

3. Threat Monitoring, Detection & Hunting

- Provide 24x7x365 monitoring for SIEM/SOAR alerts, incidents, and forensic investigations.

- Advanced threat hunting mapped to MITRE ATT&CK, using UEBA behaviour modelling for insider threat detection.
- High-fidelity alert tuning with weekly fine-tuning and duplicate alert suppression strategies.
- Threat feed integration, including CERT-In, with real-time alert enrichment from external feeds.
- Monthly threat landscape analysis and briefs.

4. Incident Response & Forensics

- Real-time alert validation, enrichment with environmental/historical data, and notification to IIBX post-triage.
- Provide incident response workflows within SOAR, with custom workflows for IR.
- Automated audit log extraction for compliance reviews (IFSCA, SEBI, RBI,ISO).
- Perform digital forensics and support investigation activities.
- Facilitate DR & BCP tabletop exercises.

5. Reporting & Dashboards

- Bespoke dashboard and reporting customization for stakeholders.
- Role-based dashboards showing real-time incidents, alerts, and status of actions.
- Analytical reporting on daily, weekly, monthly, and on-demand basis.

6. Compliance & Audit Support

- Full audit support for compliance frameworks (ISO, IFSCA, SEBI, RBI).
- Correlate threat feeds with events and document threat detection frameworks.
- Maintain and regularly review SOC process/procedure documentation.

7. Resource Management

- Provide remote L1, L2, L3 SOC analysts, SOC manager, and platform administrators for 24x7x365 operations.
- Ensure no resource replacement without prior IIBX approval; replacements must have equal or better experience. Maintain at least a one-month transition/handover period for resource changes.
- Conduct background verification for all SOC resources.

4. DETAILS OF IIBX FOR SOLUTION SIZING

A. SPECIFIC REQUIREMENTS FOR SOLUTION SIZING

Component	Current Requirement	Scalability Requirement	Notes
SIEM – EPS Capacity	4500 EPS from Day 1	Scalable up to 1,00,000 EPS	EPS = Events Per Second
SIEM – Device Count	150 devices from Day 1	Scalable up to 500 network devices/servers	Includes on-prem and cloud devices
SOAR – Playbook Execution	Support multiple concurrent playbooks	Scalable with additional nodes	Must support high-volume automation
SIEM – Storage Retention (Online)	6 months (raw + normalized logs)	Expandable as per retention policy	Online data must be fast-searchable
SIEM – Storage Retention (Offline)	24 months (raw logs should be compressed format)	Expandable as per retention policy	Offline data must be searchable /restorable
SOAR – User Licensing	Minimum 2 concurrent users in shift from Day 1.	Scalable without functionality limits	RBAC must be supported
SIEM – Flow Data Handling	Support S-Flow, J-Flow, NetFlow	Scalable with infrastructure growth	Full field correlation required
SOAR – Integrations	At least 500+ vendor integrations on Day 1	Expandable without license limits	Includes connectors for SIEM and security tools
SIEM/SOAR – HA & DR	HA & DR from Day 1 for collectors, database, and leader nodes	DR capability as per SLA	Must ensure zero data loss during failover

B. INFRASTRUCTURE DETAILS TO BE SUPPORTED

Device Type	Make
Routers & Switches	Cisco ISR 4400, Cisco Switch-Nexus & Catalyst 9000, Cisco Smart Business Switches 350
Firewall	Checkpoint 6600 / 6700, Checkpoint Smart Console GAIA OS, Fortinet 100F
WAF	F5 Cloud Firewall
XDR	Trend Micro Vision One (Apex One)
Database	Microsoft SQL 2019 &2022, MySQL 8.0, Mongo DB 6.0,
Operating Systems	Microsoft Windows Server 2019 & 2022, Microsoft Windows 11, RedHat Linux
Storage	Power Max 2000 Storage, Cisco MDS SAN Switch 9000
Servers	DELL Servers, Dell Open Manager/SCG
Email / Office	Office 365 Suite
Application/Web Server	IIS, Tomcat, In-House Application, PAM

5. ELIGIBILITY CRITERIA

Only those Bidders who fulfill the following criteria are eligible to respond to the RFP document. Offers received from the bidders who do not fulfill following criteria are considered as ineligible bidder.

No	Eligibility Criteria	Documents Required
1	Bidder must be legally registered entity i.e. Registered Firm / Limited Liability Partnership / Registered Domestic Company	Registration certificate issued by Registrar of Firms / Ministry of Corporate Affairs etc. Also Shop & Establishment License issued by local authority
2	Valid / Active Shop & Establishment, PAN and GST registration numbers	Self-certified S&E Certificate, PAN and GST copies
3	Bidder must be CERT-In empanelled.	Confirmation letter from CERT-In with valid expiry date.
4	Work Experience: - The bidder / supplier should have a minimum of Five year of experience in supply of SIEM Solutions to any organization like Banks, Govt. Organizations, PSU, Pvt. Ltd. Organization etc.	Copies of purchase orders from the organizations shall be submitted.
5	The bidder / suppliers should not have been blacklisted by any Company in the past or services terminated due to poor performance	An undertaking stating that the Company / Firm have not been blacklisted should be submitted.

6. SELECTION CRITERIA

1. The bidder would be evaluated based on scores obtained by them on Technical and Financial Parameters mentioned in Annexure 1 and Annexure 2 respectively.
2. The Financial bids would be invited only from the bidders scoring more than 70 marks out of 100 on Technical Parameters mentioned in Annexure 1.
3. The Financial bids received from the successful technical bidders would be given scores based on Financial Parameters mentioned in Annexure 2.
4. The Financial bids would be compared against the lowest financial bid (L1) to arrive at the score of the bidder.
5. The final score of the bidder would be calculated by assigning 70% weightage to the Technical Scores & 30% weightage to the Financial Score of the bidder.
6. The bidder having the highest technical score (H1), may be asked to match the bid with the Lowest (L1) bidder. If the H1 bidder matches bid with the L1 bidder, it may be considered for the award of contract, else the bidder scoring highest based on 70:30 ratio would be considered for the award of contract.

7. TECHNICAL BID & SCORING FORMAT (ANNEXURE 1)

Sr. No	Parameter	Select the Option Applicable						Total
1	Compliance to Solution Requirements (SIEM, SOAR, TIP) – Refer Schedule 1	Above 80 (50)	76-80 (45)	71-75 (40)	66-70 (35)	61-65 (30)	56-60 (25)	50
2	Compliance to MSSP Requirements (Implementation and Maintenance) – Refer Schedule 1	Above 30 (15)		26-30 (10)		20-25 (5)		15
3	Total number of similar Solutions implemented by the Bidder by BFSI	More than 50 (10)		26 to 50 (8)		10 to 25 (5)		10
4	Total Staff Strength of Bidder	More than 100 (10)		50 to 100 (8)		25 to 50 (5)		10
5	Technical Proposal & Bidder Presentation	Score would be given by the Committee						15
Total								**100**

Note:

1. The Technical Requirements (Chapter 3) for SIEM, SOAR, TIP, Implementation and Maintenance are provided in Excel format as Schedule 1. Click on below icon to download the Technical Requirements in Excel format file. (Schedule 1)

Schedule 1-Technical Requirei

2. The bidders are required to submit their compliances against each of the Technical Requirements mentioned in the Excel File.
3. The Parameter No. 1 i.e. compliance to Solution requirements is given a total weightage of 50 marks out of 100. The score would be allotted to each bidder out of 50 based on the compliances confirmed as "Y" by the bidder for the SIEM, SOAR and TIP sheets in Schedule 1. The applicable scores are mentioned for each option in the table.
4. The Parameter No. 2 i.e. compliance to MSSP requirements is given a total weightage of 15 marks out of 100. The score would be allotted to each bidder out of 15 based on the compliances confirmed as "Y" by the bidder for the MSSP sheet in Schedule 1. The applicable scores are mentioned for each option in the table.

5. The scores would be assigned for Parameter No. 3 & 4 based on the response of the bidder against these parameters. The applicable scores are mentioned for each option in the table.

8. FINANCIAL BID FORMAT (ANNEXURE 2)

This commercial bid provides pricing details for the perpetual licensing of SIEM, SOAR, UEBA, TIP solutions, and associated OEM support as per the RFP requirements. All prices are exclusive of applicable taxes.

Sr. No.	Description	Cost	Quantity	Price (INR)
1	Security Information and Event Management (SIEM – 150 Devices & 4500 EPS*)	Perpetual License		
2	Security Orchestration, Automation & Response (SOAR – 2 Concurrent Users) – **Sub-Set Model**	2 Year Price **[Sub-Set Model]**		
		Extended 1 Year Price **[Sub-Set Model]**		
3	Security Orchestration, Automation & Response (SOAR – 2 Concurrent Users) – **Dedicated Instance**	2 Year Price **[Dedicated Instance]**		
		Extended 1 Year Price **[Dedicated Instance]**		
4	User & Entity Behaviour Analytics (UEBA)	Perpetual License		
5	Threat Intelligence Platform (TIP)	2 Year Price		
		Extended 1 Year Price		
6	OEM Support (SIEM, SOAR, UEBA, TIP)	Annual Support & Subscription for 2 Years		
		Extended Annual Support & Subscription for 1 Years		
7	SOC Services by MSSP	Annual Charges for 2 Years		
		Extended Annual Charges for 1 Years		
8	SIEM - Pro-rate charges for 100 EPS**	Perpetual License		
9	SIEM - Pro-rate charges for 10 Devices	Perpetual License		
Total				

The bidders considering data Ingestion per day instead of EPS can consider:

* 375 GB per day (against 4500 EPS) for quoting the price.
** 8 GB per day (against 100 EPS) for quoting the price.

Note:

1. Prices should be quoted in Indian Rupees (INR) and should be exclusive of applicable taxes.
2. Please provide year wise price breakup in a separate table with complete details.
3. OEM support includes updates, patches, and technical assistance during the subscription period.
4. Quantity and final pricing to be filled as per project sizing and tender requirements.

9. ASSUMPTIONS AND CONSTRAINTS

1. There should be regular review and follow-up meetings, and the selected bidder shall provide the status of implementation. The same may be held through video conferencing.
2. All costs and expenses shall be incorporated into the project proposal and the Exchange shall not be liable for any expenses above and beyond the quoted project costs.
3. All software and hardware required by the project team shall be discussed and finalized before the award of project.
4. Timely delivery of the project is of utmost importance and any delay in the project shall be financially penalized based on mutually agreed upon criteria.
5. This assignment is non-transferable and the obligations and rights under this assignment, including the delivery of services, are not transferable or assignable to any other party without the express written consent of IIBX. Any attempt to transfer or assign the rights and obligations hereunder without such written consent shall be null and void.
6. No party will disclose any of the Confidential Information to any person except those of their employees, consultants, contractors and advisors having a need to know whole or part of such information in order to accomplish the purpose and will require each employee(s), consultants, contractors and advisors before he or she receives direct or indirect access to the Confidential Information to acknowledge the confidential and proprietary nature of the Confidential Information and agree to be bound by the obligations of the Client and/or the Bidder, as the case may be, under this Agreement.

10. TERMS AND CONDITIONS

1. This RFP does not commit to award a contract or to pay any costs incurred in the preparations or submission of proposals, or costs incurred in making necessary studies for the preparation thereof or to procure or contract for services or supplies.
2. Notwithstanding anything contained in this Request for proposal, IIBX reserves the right to accept or reject any Proposal and to annul the process and reject all Proposals, at any time without any liability or any obligation for such acceptance, rejection or annulment, and without assigning any reasons thereof.
3. At any time, prior to the deadline for submission of Bids, IIBX, for any reason, suo-moto or in response to clarifications requested by a prospective bidder may modify the Request for proposal by issuing amendment (s). IIBX may, at its discretion, extend the last date for the receipt of Bids.
4. IIBX makes no commitments, explicit or implicit, that the process under this Request for proposal will result in an engagement of the bidder. Further, this Request for proposal does not constitute an offer by IIBX.
5. The Proposals must be signed by a duly authorized person of the firm.
6. Bidders must provide all requisite information as required under this RFP and clearly and concisely respond to all points listed out in this RFP. Any proposal, which does not fully and comprehensively address this RFP, may be rejected.
7. Bidders must adhere strictly to all requirements of this RFP. No changes, substitutions, or other alterations to the requirement as stipulated in this RFP document will be accepted unless approved in writing by the Exchange.
8. IIBX reserves the right to negotiate with any of the bidders or other firms in any manner deemed to be in the best interest of the Exchange.
9. The solution should support 99.99% uptime to ensure the reliability and compliance of the service levels to the users.
10. The system should be highly available and automatically use failover servers/components in case of failure of any hardware or software component.
11. The system should be easily scalable with the introduction of additional hardware components or software components.

12. The bidder should be able to demonstrate that the system is fault tolerant and has resilient architecture and that there is no single point of failure.
13. The bidder must present implementation time for the project under consideration.
14. The bidder should also provide a framework on its support services and further development post implementation of the project.
15. The bidder should provide details on Service Level standards for implementation till go live and for continuous support while system is being used in production.
16. The Bidder will be required to submit the Performance Bank Guarantee (PBG) after the award of contract. The initial PBG would be towards the delivery performance and subsequent PBG would be towards the performance during the Maintenance Period. The PBG amount would be decided based on the contract value.
17. The bidder should provide detailed cost breakup containing the year wise breakup.
18. Any disputes of claims would be subject to the exclusive jurisdiction of Courts in Ahmedabad and governed by laws of India.

11. CONFIDENTIALITY STATEMENT

This document and any attachments thereto, is intended only for use by the recipient (as addressed above) and may contain legally and/or confidential, copyrighted, trademarked, patented or otherwise restricted information viewable by the intended recipient only. If you are not the intended recipient of this document (or the person responsible for delivering this document to the intended recipient), you are hereby notified that any dissemination, distribution, printing or copying of this document, and any attachment thereto, is strictly prohibited and violation of this condition may infringe upon copyright, trademark, patent, or other laws protecting proprietary and, or, intellectual property.

If you have received this document in error, please respond to the originator of this message or email him/her at the address below and permanently delete and/or shred the original and any copies and any electronic form this document, and any attachments thereto and do not disseminate further.

12. SUBMISSION DETAILS

All interested bidders are requested to respond to Request for Proposal based on the details sought under various sections of these documents. The following are the tentative timelines for the various stages of RFP.

Sr. No.	Milestone	Date
1.	Floating of Request for Proposal	01-Sep-2025
2.	Submission of queries by the bidders	09-Sep-2025
3.	Meeting to answer the queries raised by the bidders	11-Sep-2025
4.	Publishing the replies of the queries raised by the bidders	12-Sep-2025
5.	**Last date for Submission of Technical Bids in specified format**	18-Sep-2025
6.	Technical Presentation by the bidders	19-Sep-2025
7.	Evaluation of Technical Bids by IIBX	24-Sep-2025
8.	Intimation to the Technically qualified bidders for submission of Financial Bids in specified format	25-Sep-2025
9.	**Submission of Financial Bids in specified format by qualified bidders in a Password-Protected file***	29-Sep-2025
10.	Communication of Password of Financial Bid by the bidder	30-Sep-2025
10.	Opening of Password-Protected Financial bids in presence of bidders	30-Sep-2025
11.	Declaration of the selected bidder	Will intimate through email.

All queries and proposals may be emailed to ProcurementcommitteeIIBX@iibx.co.in.