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) - AMENDED

Privileged Access Management

Issue Date
12-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.

As part of our ongoing security strategy, IIBX aims to strengthen its identity and access management posture by implementing a PAM solution that provides:

- Centralized privileged credential management
- Multi-Factor Authentication (MFA)
- Session monitoring and recording
- Automated password rotation
- Zero-Trust enforcement for privileged accounts

3. SCOPE OF WORK

- A PAM solution that fulfils the technical requirements listed in Section 4 Technical Specifications (Schedule 1)
- Supply, Implementation, Configuration, and integration services
- Required licenses from day one
- Documentation, training, and post-deployment support
- AMC & Support for Privileged Access Management (PAM) solution

4. TECHNICAL SPECIFICATIONS (SCHEDULE 1)

The PAM solution must meet or exceed the following minimum technical specifications:

4.1 Deployment Architecture

- On-prem deployment
- Setup high availability in the Primary data centre with a backup at disaster recovery in case the main site goes down.
- Lightweight agent or agentless architecture support

4.2 Discovery & Onboarding

- Automatic discovery of privileged accounts (local, domain, cloud)
- Onboarding workflow for systems, accounts and applications.
- Asset discovery for non-integrated devices.

4.3 Authentication & Access Control

- Support MFA for local PAM users and remote SAML, RADIUS, and LDAP users
- Zero-Trust principles with posture checking and MFA integration
- User IP-based access control, schedule-based access control, and ZTNA device-tag-based access control.
- Role-based access (least privilege enforcement)
- FIDO password-less authentication via SAML SSO from day one
- IP / MAC address control for PAM User Login
- Just in time access provisioning / Time based access.
- Time based restrictions
- Application based restrictions – Windows / Linux
- User based copy / paste restrictions.
- Screen sharing for device access through PAM should be possible using various remote tools, such as Microsoft Teams.

4.4 Credential Management

- Automated password rotation based on policy
- Credential vault for resources, eliminating the need for users to know passwords
- Scheduled credential changes (LDAPS, Samba, SSH, SSH key)
- Auto passwords change after check-in
- Approval-based asset access (via email and web interface)
- Maker Checker for Admin activity

4.5 Session Management & Monitoring

- Privileged session recording (full video and SSH logs)
- Proxy mode to prevent sensitive data delivery to endpoints
- Blocking dangerous SSH commands with filtering profiles
- Audit tracking for all privileged account usage
- Session watermarking and tamper-proof logs

4.6 Connectivity & Protocol Support

- Native access for PuTTY, RDP, REALVNC
- Support for Windows, Linux, and MacOS (including MacOS screen sharing over RDP)
- Gateway option for assets behind firewalls
- Support for high-strength SSH encryption and advanced RDP authentication (Cred SSP, TLS)
- Agentless connection options
- Support Hybrid Infrastructure – Cloud, On-Prem, Legacy

4.7 Security & Compliance

- Built-in DLP and antivirus scanning (or integration with 3rd-party solutions)
- Anti-virus scanning for file transfers (Web SFTP, Web SAMBA, SCP)
- Policy-based access enforcement
- TPM support for private key protection
- Built-in packet capture for troubleshooting

- Mapping to Standards: ISO 27001, NIST, CIS etc.

4.8 Integration & Platform Requirements

- Native integration with Active Directory, AAA, 2FA, endpoint security, and ZTNA solutions
- Single endpoint agent compatible with Firewall SSL VPN
- Integration with SIEM, SOAR, EDR and IAM
- Integration with Ticketing System – ServiceNow, JIRA, ServiceDesk (Manage Engine)
- Integration with Thin Client (SSMS, Checkpoint Smart Console)
- Ability to create separate zero-trust policies for on-network and internet access

4.9 User Experience and Accessibility

- Web based access for Admin / User PAM portal
- Self Service access request workflows

4.10 Audit, Logging and Reporting

- Immutable audit logs of all activities
- Real-time alerting for suspicious behaviour
- Alert on PAM Bypass Devices
- Pre-built compliance reports (e.g., SOX, PCI, HIPAA)
- Customized Dashboard
- Custom report builder and scheduled reports
- Log session start/end times for Live and recorded video, duration, user identity, and access method
- Content search in recorded and live videos

4.11 Password Retrieval in case of emergency purpose or Break Glass Scenario.

- PAM Recovery Scenarios
    - PAM Database Corruption (e.g., due to hardware failure)
    - PAM Application Crash or Outage
    - Network Segmentation or Isolation Event
    - Cyber Attack /Ransomware affecting PAM

    - Disaster Recovery site activation

- Regularly export encrypted credential vault backups.
- Store in multiple secure offline locations (primary DC, DR site, and secure offsite).
- Backups must be encrypted with AES-256 or stronger.

5. DETAILS OF IIBX FOR SOLUTION SIZING

A. SPECIFIC REQUIREMENTS FOR SOLUTION SIZING

Parameter	Initial Phase	Scalability Requirement over 3 years
PAM Users	100	150
Concurrent Sessions for each user	10	15
Number of Devices	200	300

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, SIEM & SOAR

6. ELIGIBILITY CRITERIA

Only those Bidders who fulfil the following criteria are eligible to respond to the RFP document. Offers received from the bidders who do not fulfil 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	Work Experience: - The bidder / supplier should have a minimum of 2 year of experience in supply of PAM Solutions to any organization like Banks, Govt. Organizations, PSU, Pvt. Ltd. Organization etc.	Copies of purchase orders from the organizations shall be submitted.
4	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.

7. 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.

8. TECHNICAL BID & SCORING FORMAT (ANNEXURE 1)

Sr. No	Parameter	Select the Option Applicable			Total
1	Compliance to Solution Requirements – Refer Schedule 1	Above 55 (50)	51-55 (40)	45-50 (30)	50
2	Implementation methodology and timeline	Less than 1 Month (15)	1 Month to 2 Months (10)	2 Month to 3 Month (5)	15
3	Bidder/OEM experience and references in BFSI	More than 50 (10)	26 to 50 (8)	10 to 25 (5)	15
4	Technical Proposal & Bidder Presentation	Score would be given by the Committee			20
Total					**100**

Note:

1. The Technical Requirements 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 Requirer

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 requirements mentioned in Schedule 1. The applicable scores are mentioned for each option in the table.
4. The scores would be assigned for Parameter No. 2 & 3 based on the response of the bidder against these parameters. The applicable scores are mentioned for each option in the table.
5. The Technical Proposal & Bidder Presentation should cover the following:

- Detailed technical compliance matrix (indicating full/partial compliance for each requirement)
- Proposed architecture diagram
- Implementation methodology and project timeline
- Licensing model and total cost of ownership (TCO) for 3–5 years
- Customer references for similar deployments
- Support model and SLAs

9. FINANCIAL BID FORMAT (ANNEXURE 2)

This commercial bid provides pricing details for the licensing of PAM 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	PAM Solution subscriptions for 150 administrative users and 300 devices, including high availability (HA) in the Data Center (DC) and Disaster Recovery (DR) site.	Subscription cost for 3 years		
2	Installation of PAM Solutions as per IIBX standards.	One time		
3	AMC / Support charges of PAM Solutions.	AMC / Support for 3 years		
4	Cost per additional 5 users / 10 Devices	Subscription cost for 3 years		
Total				

Note:

1. Prices should be quoted in Indian Rupees (INR) and should be exclusive of applicable taxes.
2. OEM support includes updates, patches, and technical assistance during the subscription period.
3. Quantity and final pricing to be filled as per project sizing and tender requirements.
4. Please provide a year-wise breakup of *Subscription* and *Support* costs separately, in a separate sheet, with complete details.
5. In case the proposed solution is software based, the indicative infrastructure hardware cost & configuration for implementing the solution needs to be specified by bidder in a separate sheet. IIBX will provide the required hardware.

10. 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.

11. 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.

12. 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.

13. 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. (Presentation Dates would be communicated over email to respective bidders)	19-Sep-2025 to 23-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.

14. RESPONSE TO QUERIES RECEIVED AGAINST INITIAL RFP

RESPONSE TO QUERY SET – 1

Sr No	Section No	Clause	Clause Details	Queries	IIBX Response
1	4.3	Authentication & Access Control	Zero-Trust principles with posture checking and MFA integration	Pls help us understand requirement of posture check.	The PAM solution must enforce Zero Trust principles by validating both user identity and device health before granting access. Device posture checks must include OS version and patch level, security agent presence (AV/EDR/DLP), TPM and secure boot status, encryption status, and compliance with corporate security policies. Non-compliant devices must either be blocked or granted restricted access, and posture check results must be logged and integrated with SOC and SIEM systems for real-time monitoring and audit readiness
2			User IP-based access control, schedule-based access control, and ZTNA device-tag-based access control.	Pls help us understand requirement of ZTNA device-tag-based access control.	The PAM solution must integrate with the organization's ZTNA framework to enforce device-tag-based access control. The system should dynamically evaluate user identity, device compliance (OS patches, antivirus, MDM enrolment, disk encryption), and risk posture before granting privileged access. Access should be allowed only from

Sr No	Section No	Clause	Clause Details	Queries	IIBX Response
					managed, trusted devices.
3	4.5	Session Management & Monitoring	Session watermarking and tamper-proof logs	Pls help us understand requirement of Session watermarking.	The PAM solution must support dynamic session watermarking to overlay session-specific identifiers such as username, session ID, source IP, and timestamp on all privileged sessions (RDP, SSH, and Web). The watermark must appear both during live sessions and on session recordings to ensure traceability and deter data leakage.
4	4.6	Connectivity & Protocol Support	Native access for PuTTY, RDP, REALVNC, and browsers (Chrome, Firefox, Edge)	Pls help us understand requirement of Native Access for browsers.	Kindly read as Native Access for PuTTY, RDP, REALVNC. The Native access for Browsers shall be removed in modified RFP.
5	4.7	Security & Compliance	Built-in DLP and antivirus scanning	Pls help us understand requirement in detail.	The solution should be able to integrate with Antivirus (AV) and Data Loss Prevention (DLP) solutions for file scanning purposes
6			Anti-virus scanning for file transfers	Pls help us understand requirement in detail.	The solution should be able to integrate with Antivirus (AV) and Data Loss Prevention (DLP) solutions for file scanning purposes
7			TPM support for private key protection	Pls help us understand requirement in detail.	This is a generic requirement.

RESPONSE TO QUERY SET – 2

Sr No	Bidder Queries	IIBX Response
1	Do we need to consider a ZTNA solution with PAM Solution? Should this be considered in the next phase?	No
2	Regarding Point No. 23 – More details are required about the maker-checker activity.	Admin activity can't be performed with single admin user
3	For Points No. 40, 52, and 54 – In terms of mapping standards/compliance, can we integrate this with your SIEM solution? Do we need to consider any additional components or licensing for that?	The PAM Solution should independently generate compliance reports.
4	Regarding Point No. 60, is it acceptable to consider the backup as encrypted without explicitly mentioning a specific algorithm, such as AES-256?	AES-256 is the minimum encryption required.
5	Regarding Point No. 50, do you currently have an existing SIEM or SOAR solution in place? If yes, can this requirement be addressed through that platform?	The PAM Solution should independently generate compliance reports.

RESPONSE TO QUERY SET – 3

Sr No.	Bidder's Query	IIBX Response
1	What is the total no of users to be considered to be 150 and 300 are unique IP's?	The no. of devices mentioned can be considered as no. of unique IP's. The no. of users are not same as unique IP's.
2	What number of roles to be considered on every unique IP?	The no. of roles shall be general and not bound to IP's
3	What will be the total count number of devices that needs to be onboarded in PAM?	Please refer section 5A
4	Who will provide the Hardware, Operating System and CALS?	IIBX
5	What is the line item for FINANCIAL BID FORMAT (ANNEXURE 2) AMC / Support or Subscription cost for 3 years ? Pricing should be AMC base or Subscription base ?	The pricing should combine the subscription cost as well as AMC. The year wise break up for subscription fees & AMC can be provided in separate sheet
6	What will be the Architecture requirement for PAM is it Active-Passive or Active-Active?	Active-Passive
7	Implementation timeline ?	1 Month
8	100% payment for PAM Licenses at the start of implementation process?	The payment will be linked to delivery & Implementation Milestones
9	PAM Implementation location will be Onsite or Remote?	Onsite.
10	Post Go live and implementation, who will manage PAM L1/L2 BAU Support?	IIBX
11	Support / Implementation Location for IIBX will be Remote or Onsite ?	Either
12	Support Window - Business Hours or 24*7 End to End Support	OEM Support required
13	Pls specify standard Penalty charges if any ?	It will be decided post selection of Bidder.
14	Sample SLA?	Critical issue to be resolved in 30 minutes. Non- critical issue to be resolved in 4 hours.

RESPONSE TO QUERY SET – 4

Sr No.	AREA	TECHNICAL SPECIFICATIONS	QUERIES	IIBX Response
1	Deployment Architecture	Setup high availability in the Primary data centre with a backup at disaster recovery in case the main site goes down.	Could you please confirm if the requirement is for two active nodes in the Data Center and one passive node at the Disaster Recovery (DR) site, with DR to be activated only in the event of a complete DC failure?	Yes
2	Discovery & Onboarding	Asset discovery for non-integrated devices.	Is this feature considered mandatory, given that only a known and limited set of devices (maximum 300) will be onboarded?	Yes
3	Authentication & Access Control	Support MFA for local PAM users and remote SAML, RADIUS, and LDAP users	Would you require the PAM solution to include its own MFA capability, or is integration with your existing MFA solution preferred?	The PAM solution should include its own MFA capability.
4	Authentication & Access Control	Zero-Trust principles with posture checking and MFA integration	Could you clarify which specific parameters or security attributes are expected to be validated as part of device posture checks?	The PAM solution must enforce Zero Trust principles by validating both user identity and device health before granting access. Device posture checks must include OS version and patch level, security agent presence (AV/EDR/DLP), TPM and secure boot status, encryption status, and compliance with corporate security policies. Non-compliant devices

Sr No.	AREA	TECHNICAL SPECIFICATIONS	QUERIES	IIBX Response
				must either be blocked or granted restricted access, and posture check results must be logged and integrated with SOC and SIEM systems for real-time monitoring and audit readiness
5	Authentication & Access Control	FIDO password-less authentication via SAML SSO from day one	Do you currently use FIDO-compliant devices, and is the intention to leverage them for multi-factor authentication within the PAM solution?	No, currently IIBX does not use FIDO-compliant devices, but the features for FIDO passwordless via SAML SSO is required to be available in Solution from Day one.
6	Authentication & Access Control	Time based restrictions	Could you please elaborate on the type of time-based restrictions you are referring to? Are these related to access windows, session durations, or other criteria?	It is related to Access Window (for example between 9.00 am to 7.00 pm) as well as Session Duration (maximum 60 minutes)
7	Connectivity & Protocol Support	Gateway option for assets behind firewalls	Will an additional access gateway/component be required, or will users connect via VPN first and then access resources through PAM?	External users connect via VPN first and then access resources through PAM
8	Security & Compliance	Built-in DLP and antivirus scanning (or integration with 3rd-party solutions)	Is there a requirement for integration with Antivirus (AV) and Data Loss Prevention (DLP) solutions via ICAP for file scanning purposes?	Yes
9	Security & Compliance	Policy-based access enforcement	Could you please provide more details or a use case for the following feature	The PAM solution must provide policy-based access enforcement

Sr No.	AREA	TECHNICAL SPECIFICATIONS	QUERIES	IIBX Response
			mentioned in the RFP	capabilities, allowing administrators to define and enforce dynamic rules for privileged access based on contextual attributes such as user role, authentication strength, device posture, IP location, time of access, and risk score. The policy engine must support automated workflows for allow/deny decisions, just-in-time privilege elevation, manager approvals, and real-time session controls to ensure compliance with cybersecurity guidelines.
10	Security & Compliance	TPM support for private key protection	Could you please provide more details or a use case for the following feature mentioned in the RFP	This is a generic requirement.
11	Integration & Platform Requirements	Native integration with Active Directory, AAA, 2FA, endpoint security, and ZTNA solutions	Could you please share the specific use cases or workflows envisioned for integration with Endpoint Security and Zero Trust Network Access (ZTNA) platforms?	The PAM solution must integrate natively with leading endpoint security platforms and ZTNA solutions to enforce Zero Trust principles.
12	Integration & Platform Requirements	Integration with Ticketing System – ServiceNow, JIRA, ServiceDesk (Manage Engine)	Could you specify the name and type of the ticketing system currently in use (e.g., ServiceNow, BMC	Currently IIBX is using Service Desk (Manage Engine.) However it should have flexible for

Sr No.	AREA	TECHNICAL SPECIFICATIONS	QUERIES	IIBX Response
			Remedy), to ensure compatibility for integration?	integrate with other ticketing tool as well.
13	Integration & Platform Requirements	Ability to create separate zero-trust policies for on-network and internet access	Could you please provide more details or a use case for the following feature mentioned in the RFP	The PAM solution must support defining and enforcing separate Zero Trust policies for internal on-network access and external access.
14	Audit, Logging and Reporting	Alert on PAM Bypass Devices	Is there a requirement for the PAM solution to provide visibility into endpoints that are not directly onboarded or managed by the platform?	Yes

RESPONSE TO QUERY SET – 5

Sr No	Section No	Clause	Clause Details	Queries	IIBX Response
1	4.3	Authentication & Access Control	Zero-Trust principles with posture checking and MFA integration	Pls help us understand requirement of posture check.	The PAM solution must enforce Zero Trust principles by validating both user identity and device health before granting access. Device posture checks must include OS version and patch level, security agent presence (AV/EDR/DLP), TPM and secure boot status, encryption status, and compliance with corporate security policies. Non-compliant devices must either be blocked or granted restricted access, and posture check results must be logged and integrated with SOC and SIEM systems for real-time monitoring and audit readiness
2			User IP-based access control, schedule-based access control, and ZTNA device-tag-based access control.	Pls help us understand requirement of ZTNA device-tag-based access control.	The PAM solution must integrate with the organization's ZTNA framework to enforce device-tag-based access control. The system should dynamically evaluate user identity, device compliance (OS patches, antivirus, MDM enrollment, disk encryption), and risk posture before granting privileged access. Access should be allowed only from

Sr No	Section No	Clause	Clause Details	Queries	IIBX Response
					managed, trusted devices.
3	4.5	Session Management & Monitoring	Session watermarking and tamper-proof logs	Pls help us understand requirement of Session watermarking.	The PAM solution must support dynamic session watermarking to overlay session-specific identifiers such as username, session ID, source IP, and timestamp on all privileged sessions (RDP, SSH, and Web). The watermark must appear both during live sessions and on session recordings to ensure traceability and deter data leakage.
4	4.6	Connectivity & Protocol Support	Native access for PuTTY, RDP, REALVNC, and browsers (Chrome, Firefox, Edge)	Pls help us understand requirement of Native Access for browsers.	Kindly read as Native access for PuTTY, RDP, REALVNC. The Native access for Browsers shall be removed in modified RFP.
5	4.7	Security & Compliance	Built-in DLP and antivirus scanning	Pls help us understand requirement in detail.	The solution should be able to integrate with Antivirus (AV) and Data Loss Prevention (DLP) solutions for file scanning purposes
6			Anti-virus scanning for file transfers	Pls help us understand requirement in detail.	The solution should be able to integrate with Antivirus (AV) and Data Loss Prevention (DLP) solutions for file scanning purposes
7			TPM support for private key protection	Pls help us understand requirement in detail.	This is a generic requirement.

RESPONSE TO QUERY SET – 6

Sr No	Page	Section No	Section Heading	Exact Statement from RFP	Query	IIBX Response
1	6	4.3	Authentication & Access Control	"Application based restrictions – Windows / Linux"	Regarding the requirement for "Application based restrictions – Windows / Linux", could IIBX provide more detail on the specific use cases or types of applications for which these restrictions are intended? Is the requirement to restrict which applications privileged users can launch through PAM, or to restrict PAM access itself based on the specific applications running on the target device?	Restrict applications/command through PAM. For example restrict command in CLI based environment in case of Linux/SSH and restrict processes / exes / PID in case of Windows.
2	6	4.3	Authentication & Access Control	"Screen sharing for device access through PAM should be possible using various remote tools, such as Microsoft Teams."	The RFP states that "Screen sharing for device access through PAM should be possible using various remote tools, such as Microsoft Teams". Could IIBX clarify if the expectation is for the PAM solution to facilitate screen sharing through external collaboration tools, or if it requires direct integration with specific tools like Microsoft Teams to enable	Direct integration with specific tools like Microsoft Teams to enable screen sharing functionality within the PAM session itself

Sr No	Page	Section No	Section Heading	Exact Statement from RFP	Query	IIBX Response
					screen sharing functionality within the PAM session itself (e.g., through an embedded viewer or controlled launch)?	
3	6, 7	4.1, 4.6	Deployment Architecture, Connectivity & Protocol Support	"On-prem deployment", "Support Hybrid Infrastructure – Cloud, On-Prem, Legacy"	Section 4.1 explicitly specifies "On-prem deployment" for the PAM solution. However, Section 4.6 mentions the need to "Support Hybrid Infrastructure – Cloud, On-Prem, Legacy". Could IIBX clarify the extent to which cloud infrastructure support is required? Is this primarily for managing privileged accounts residing in cloud environments from the on-prem PAM solution, or does it imply the possibility of a hybrid deployment model for certain PAM components (e.g., satellite connectors in cloud environments)?	It is for managing privileged accounts residing in cloud environments from the on-prem PAM solution,
4	8	4.8	Integration & Platform Requirements	"Single endpoint agent compatible with	To ensure full compatibility with the "Single endpoint agent compatible with Firewall SSL VPN",	IIBX has yet not planned on any specific SSL VPN.

Sr No	Page	Section No	Section Heading	Exact Statement from RFP	Query	IIBX Response
				Firewall SSL VPN"	could IIBX provide examples of the specific Firewall SSL VPN solutions currently in use or planned for use within their environment?	
5	8	4.8	Integration & Platform Requirements	"Integration with Thin Client (SSMS, Checkpoint Smart Console)"	What specific functionalities or use cases are expected for the "Integration with Thin Client (SSMS, Checkpoint Smart Console)"? Is the requirement primarily to launch these applications through the PAM solution, manage privileged access to these thin client environments, facilitate session recording for activities performed within them, or a combination of these?	Yes. The requirement is to launch these applications through the PAM solution, manage privileged access to these thin client environments, facilitate session recording for activities performed within them.
6	8	4.10	Audit, Logging and Reporting	"Pre-built compliance reports (e.g., SOX, PCI, HIPAA)"	The RFP requires "Pre-built compliance reports (e.g., SOX, PCI, HIPAA)". Could IIBX specify which of these listed compliance reports (SOX, PCI, HIPAA) are mandatory for their operational and auditing requirements?	This is a generic requirement.
7	10	5.A	A. SPECIFIC	"Concurrent Sessions	For the parameter "Concurrent Sessions for each	The concurrent session for each user refer to the

Sr No	Page	Section No	Section Heading	Exact Statement from RFP	Query	IIBX Response
			REQUIREMENTS FOR SOLUTION SIZING	for each user Initial Phase 10 Scalability Requirement over 3 years 15"	user," the requirement states "Initial Phase 10 Scalability Requirement over 3 years 15". Could IIBX confirm if this refers to 10 concurrent sessions per individual PAM user (meaning 100 users * 10 sessions = 1000 total concurrent sessions initially), or if it represents the total maximum number of concurrent sessions across all PAM users (i.e., a maximum of 10 concurrent sessions for the entire 100 users initially)? This distinction is critical for accurate solution sizing and resource allocation.	number of concurrent session that the user can open with various target devices after login to PAM. For example, if X user is login to PAM, he should be able to concurrently connect to atleast 10 target devices at a time.
8	10	5.A	A. SPECIFIC REQUIREMENTS FOR SOLUTION SIZING	"Number of Devices Initial Phase 200 Scalability Requirement over 3 years 300"	While the RFP specifies the number of devices to be supported (200 initially, scaling to 300), it does not explicitly state the estimated number of privileged accounts (e.g., local administrator accounts, service accounts, database accounts, SSH keys, application-specific accounts) that will need to be	Currently, only the information related to devices is available for sizing.

Sr No	Page	Section No	Section Heading	Exact Statement from RFP	Query	IIBX Response
					discovered, onboarded, and managed on these devices. Could IIBX provide an estimate for the total number of distinct privileged accounts/secrets to be managed by the PAM solution?	
9	13	8 (Note 3)	TECHNICAL BID & SCORING FORMAT (ANNEXURE 1)	"The score would be allotted to each bidder out of 50 based on the compliances confirmed as "Y" by the bidder for the requirements mentioned in Schedule 1."	Note 3 under the Technical Bid & Scoring Format states that scores for "Compliance to Solution Requirements" will be allotted based on compliances confirmed as "Y". Could IIBX clarify if partial compliance (e.g., indicated with a 'P' or 'N' with a detailed explanation of how it can be met or a roadmap) will be accepted and how it would be scored, or if only full compliance ('Y') receives points for a given requirement?	Only Full compliance (Y) receives points for a given requirement.
10	15	9	FINANCIAL BID FORMAT (ANNEXURE 2)	"This commercial bid provides pricing details for the perpetual licensing of PAM	The Financial Bid Format refers to "perpetual licensing of PAM solutions," while the table requests a "Subscription cost for 3 years." Could IIBX clarify whether they are	This is a typo error in Financial Bid Format. The word "perpetual" shall be removed in the revised RFP that shall be published along with the responses to the queries raised by

Sr No	Page	Section No	Section Heading	Exact Statement from RFP	Query	IIBX Response
				solutions... ", "Subscription cost for 3 years".	seeking a perpetual license model for the core PAM solution with a separate 3-year support/maintenance subscription, or if a pure 3-year subscription model for the entire PAM solution (including software usage) is also acceptable? This distinction is crucial for structuring the financial proposal accurately.	the bidders. The bidders can either quote for Perpetual or Subscription based licenses, but total cost of ownership for 3 years shall be considered by IIBX.

RESPONSE TO QUERY SET – 7

Sr No	Page No.	Section No.	Technical Specification (Schedule 1)	Technical Specification	Bidder's Clarification Sought	IIBX Response
1	7.0	4.6	Connectivity & Protocol Support	Support for Windows, Linux, and MacOS (including MacOS screen sharing over RDP)	Request you to kindly elaborate on the use case for screen sharing over RDP within the scope of PAM	The PAM solution must provide secure, collaborative screen sharing capabilities during privileged sessions, allowing multiple authorized users (e.g., administrators, auditors, support engineers) to View, request control, chat and Record & Audit.
2	7.0	4.7	Security & Compliance	Anti-virus scanning for file transfers (Web SFTP, Web SAMBA, SCP)	Request you to please provide more details regarding the anti-virus scanning use case within PAM.	Anti-virus scanning for web-based file transfers (like Web SFTP and Web SAMBA) and SCP-based file transfers within a Privileged Access Management (PAM) solution involves integrating the PAM system with an anti-malware engine. This integration ensures that any files being transferred through the PAM-managed channels are scanned for threats before reaching their destination.
3			Kindly provide details on the payment terms			The payment will be linked to delivery & Implementation Milestones
4			what will be the implementation mode: Remote or			Either

Sr No	Page No.	Section No.	Technical Specification (Schedule 1)	Technical Specification	Bidder's Clarification Sought	IIBX Response
			Onsite or Hybrid ?			
5			Does the bidder require to share the infrastructure hardware cost for implementing the solution or IIBX will help cater to it.			Yes in case the solution is software base, then the indicative infrastructure hardware cost & configuration for implementing the solution needs to be shared by bidder.
6			Is there a need for onsite or remote support after implementation ?			L3 remote support is expected

RESPONSE TO QUERY SET – 8

Sr No	Section No	Clause	Clause Details	Queries	IIBX Response
1	4.3	Authentication & Access Control	Zero-Trust principles with posture checking and MFA integration	Pls help us understand requirement of posture check.	The PAM solution must enforce Zero Trust principles by validating both user identity and device health before granting access. Device posture checks must include OS version and patch level, security agent presence (AV/EDR/DLP), TPM and secure boot status, encryption status, and compliance with corporate security policies. Non-compliant devices must either be blocked or granted restricted access, and posture check results must be logged and integrated with SOC and SIEM systems for real-time monitoring and audit readiness
2			User IP-based access control, schedule-based access control, and ZTNA device-tag-based access control.	Pls help us understand requirement of ZTNA device-tag-based access control.	The PAM solution must integrate with the organization's ZTNA framework to enforce device-tag-based access control. The system should dynamically evaluate user identity, device compliance (OS patches, antivirus, MDM enrollment, disk encryption), and risk posture before granting privileged access. Access should be allowed only from

Sr No	Section No	Clause	Clause Details	Queries	IIBX Response
					managed, trusted devices.
3	4.5	Session Management & Monitoring	Session watermarking and tamper-proof logs	Pls help us understand requirement of Session watermarking.	The PAM solution must support dynamic session watermarking to overlay session-specific identifiers such as username, session ID, source IP, and timestamp on all privileged sessions (RDP, SSH, and Web). The watermark must appear both during live sessions and on session recordings to ensure traceability and deter data leakage.
4	4.6	Connectivity & Protocol Support	Native access for PuTTY, RDP, REALVNC, and browsers (Chrome, Firefox, Edge)	Pls help us understand requirement of Native Access for browsers.	Kindly read as Native access for PuTTY, RDP, REALVNC. The Native access for Browsers shall be removed in modified RFP.
5	4.7	Security & Compliance	Built-in DLP and antivirus scanning	Pls help us understand requirement in detail.	The solution should be able to integrate with Antivirus (AV) and Data Loss Prevention (DLP) solutions for file scanning purposes
6			Anti-virus scanning for file transfers	Pls help us understand requirement in detail.	The solution should be able to integrate with Antivirus (AV) and Data Loss Prevention (DLP) solutions for file scanning purposes
7			TPM support for private key protection	Pls help us understand requirement in detail.	This is a generic requirement.

RESPONSE TO QUERY SET – 9

Sr No.	Section	Query	IIBX Response
1	General & Commercial	Please confirm environments: Prod + DR only, or Dev/UAT + Prod + DR.	Prod + DR only
2	Architecture & Availability (Sec. 4.1, 11)	Is external access to PAM (from internet) required for vendors/remote admins, or only on-prem/intranet?	Only on-prem/intranet
3	Sizing (Sec. 5)	Device counts include network/security gear, servers, DBs, and apps listed. Please confirm if cloud IaaS/PaaS (e.g., Azure/AWS) or SaaS admin consoles are also in scope for onboarding.	Device includes on-prem & SaaS admin consoles.
4	Authentication & Access Control (Sec. 4.3)	You require FIDO passwordless via SAML SSO "from day one." Please confirm the IdP (e.g., Entra ID/ADFS/Okta) and whether passkeys/FIDO2 authenticators are already enrolled for PAM admins.	Bidder can propose the IdP (e.g., Entra ID/ADFS/Okta). Currently, no passkeys/FIDO2 authenticators are enrolled, but the features for FIDO passwordless via SAML SSO is required to be available in Solution from Day one.
5	Security, Compliance, & Integrations (Sec. 4.7–4.10)	SIEM/SOAR: name/version, ITSM: confirm the primary platform (ServiceNow/Jira/ManageEngine)	IIBX is in the process of setting up SOC also, and therefore, SIEM/SOAR is still not finalized. However, the proposed solution should be able to integrate with any SIEM/SOAR. For ITSM, we currently have ManageEngine.

RESPONSE TO QUERY SET – 10

Sr No.	Page No.	Section No.	Technical Specification	Technical Specification	Bidder's Clarification	IIBX Response
1	7	4.6	Connectivity & Protocol Support	Support for Windows, Linux, and MacOS (including MacOS screen sharing over RDP)	Request you to kindly elaborate on the use case for screen sharing over RDP within the scope of PAM	The PAM solution must provide secure, collaborative screen sharing capabilities during privileged sessions, allowing multiple authorized users (e.g., administrators, auditors, support engineers) to View, request control, chat and Record & Audit.
2	7	4.7	Security & Compliance	Anti-virus scanning for file transfers (Web SFTP, Web SAMBA, SCP)	Request you to please provide more details regarding the anti-virus scanning use case within PAM.	Anti-virus scanning for web-based file transfers (like Web SFTP and Web SAMBA) and SCP-based file transfers within a Privileged Access Management (PAM) solution involves integrating the PAM system with an anti-malware engine. This integration ensures that any files being transferred through the PAM-managed channels are scanned for threats before reaching their destination.

RESPONSE TO QUERY SET – 11

Sr No	Bidder Queries	IIBX Response
1	Do we need to consider a ZTNA solution with PAM Solution ? Should this be considered in the next phase?	No
2	Regarding Point No. 23 – More details are required about the maker-checker activity.	Admin activity can't be perform with single admin user
3	For Points No. 40, 52, and 54 – In terms of mapping standards/compliance, can we integrate this with your SIEM solution? Do we need to consider any additional components or licensing for that?	The PAM Solution should independently generate compliance reports.
4	Regarding Point No. 60, is it acceptable to consider the backup as encrypted without explicitly mentioning a specific algorithm, such as AES-256?	AES-256 is the minimum encryption required.
5	Regarding Point No. 50, do you currently have an existing SIEM or SOAR solution in place? If yes, can this requirement be addressed through that platform?	The PAM Solution should independently generate compliance reports.