



INDIAN INSTITUTE OF BANKING & FINANCE

(An ISO 21001:2018 Certified Institute)

Kohinoor City, Commercial – II, Tower – I, 2nd Floor, Kirod Road, Kurla (West), Mumbai – 400 070

REQUEST FOR PROPOSAL (RFP)

FOR

**Selection of Service Provider(s) to Conduct Online Examinations, i.e. Computer Based Test (CBT),
of the Institute in Centre-Based Mode Across India**

RFP No.: IIBF/EXAM RFP-02/2026-27__

Dated: 13/08/2026

Cost of RFP Document: Nil (downloadable from www.iibf.org.in)

Earnest Money Deposit (EMD): ₹ 25,00,000/- (Rupees Twenty-Five Lakh only)

ADDRESSED TO:

Chief Executive Officer, Indian Institute of Banking & Finance

Kohinoor City, Commercial – II, Tower – I, 2nd Floor, Kirod Road, Kurla (West), Mumbai – 400 070

Website: www.iibf.org.in | E-mail: jd.exm2@iibf.org.in / add.dir@iibf.org.in

This document is the property of IIBF and is intended solely for the purpose of this procurement.

DISCLAIMER

The information contained in this Request for Proposal (RFP) document, and any information provided subsequently to prospective Service providers, whether verbally or in writing by or on behalf of the Indian Institute of Banking & Finance (IIBF), is provided solely for the purpose of assisting Service providers in preparing and submitting their proposals and is subject to the terms and conditions set out in this RFP and any other applicable conditions communicated by IIBF.

This RFP is not an offer by IIBF but an invitation to receive proposals from eligible Service providers. No contractual obligation whatsoever shall arise from this RFP process unless and until a formal contract is executed by duly authorized representatives of IIBF and the successful Service provider.

This RFP document does not purport to contain all the information that a Service provider may require. Each Service provider is encouraged to undertake its own independent investigations, assessments, and analyses and to verify the accuracy, adequacy, reliability, and completeness of the information contained herein. Where necessary, Service providers should obtain independent professional advice at their own cost.

While reasonable care has been taken in the preparation of this RFP, IIBF makes no representation or warranty, express or implied, and shall not be liable under any law, statute, rule, or regulation for the accuracy, adequacy, reliability, or completeness of the information contained in this RFP or otherwise made available to Service providers.

The RFP document and all related materials, communications, and information shall remain the property of IIBF and are protected by applicable copyright laws. Service providers shall not disclose, reproduce, distribute, or share any part of this RFP or related information with any third party without the prior written consent of IIBF.

IIBF reserves the right, at its sole discretion, to amend, modify, supplement, withdraw, suspend, cancel, or terminate the RFP process at any stage, and to accept or reject any or all proposals without assigning any reason whatsoever. IIBF may also, if deemed necessary, issue a fresh RFP for the same or similar services. In such circumstances, IIBF shall have no liability to any Service provider, nor shall it be obligated to provide reasons for any such decision or action.

TABLE OF CONTENTS

Content	Page no.
Disclaimer	2
Table of Content	3
Section 1 – Notice Inviting Tender	8
Bid schedule	9
Section 2 – Introduction	10
2.1 About IIBF	10
2.2 Background	10
2.3 Objective of this RFP	11
2.4 Cost of the RFP and Due Diligence	11
2.5 Definitions and Abbreviations	12
2.6 Ownership of this RFP	18
Section 3 – Scope of work	19
3.1 Broad Scope of Work	19
A. Pre-Examination activities:	19
A.1 Operations by IIBF	19
A.2 Operations by Service Provider	19
A.3 Minimum Hardware, Software and Network Specifications	21
A.4 Question Paper Management	27
A.5 Examination Venues	29
A.6 Audit and Freeze of Examination Venues	30
A.7 Venue Layout, Seating and Signage Norms	31
A.8 Exam Functionaries – Verification and Compliance	32
A.9 Mock Day / Preparedness Drill	35
A.10 CCTV Surveillance	36
A.11 SOPs, Testing and Contingency	37
A.12 Safety, Emergency Preparedness and Disaster Management at Examination Sites	38
A.13 Support	39
A.14 Escalation matrix	39
B. During Examination	40

Content	Page no.
B.1 Entry, Physical Security and Frisking	40
B.2 Biometric Authentication of Candidates	40
B.3 Conduct, Monitoring and Logging	41
B.4 PwD Candidates, Scribes and Special Requirements	43
C. Post-Examination	44
3.2 Roles and Responsibilities Matrix	45
3.3 Governance Model – Independent Examination Monitoring	49
3.4 Data Requirements for Audit / Analysis by Institute or agency authorised by Institute	49
3.5 Dataset to be provided by the Service provider for analysis (the "Mandatory Data Set")	50
3.6 Expected Volumes, Tenure and Single Point of Contact	51
3.7 Performance Evaluation	51
Section 4 – Eligibility Criteria	52
Section 5 – Instructions to Service Providers	54
5.1 Bidding Documents, Clarifications and Amendments	54
5.2 Earnest Money Deposit (EMD)	54
5.3 Preparation and Submission of Bids (Two-Bid System)	54
5.4 Language, Format, Signing and Deviations	55
5.5 Modification, Substitution and Withdrawal of Bids; Late Bids	55
5.6 Bid Opening, Preliminary Scrutiny and Clarifications	55
5.7 Contacting IIBF; Canvassing	56
5.8 IIBF's Rights	56
Section 6 – Evaluation Process	57
6.1 Overall Methodology	57
6.2 Technical Evaluation (100 marks)	57
6.2.1 Indicative Sub-Scoring Guidance	57
6.3 Commercial Evaluation	60
6.4 Techno-commercial evaluation:	61
6.5 Presentation and Demonstration — Mandatory Agenda	61
Section 7 – Service Level Agreement (SLA) Framework	63
7.1 Definitions and Measurement Methodology	66

Content	Page no.
7.2 Service-Credit Computation	66
7.3 SLA Governance	66
7.4 SLA Scorecard — Sample Format (per examination cycle)	67
Section 8 – Terms and Conditions	68
8.1 Legal Framework – Statutory Compliance	68
8.2 Processing Norms and Data Handling	68
8.3 Ownership of Examination Data	68
8.4 Right to Withhold Payment Linked to Compliance	68
8.5 Payment Terms	69
8.6 Liability for Data — Service provider's Absolute Data Accountability	69
8.7 Limitation of Liability	70
8.8 Performance Bank Guarantee	70
8.9 Exit Management and Transition Support	70
8.10 Confidentiality, Non-Disclosure and IPR	71
8.11 Appointment of third party by Service Provider	71
8.12 Termination and Suspension	71
8.13 Force Majeure	72
8.14 Indemnity	72
8.15 Integrity Pact; Fraudulent and Corrupt Practices	72
8.16 Governing Law, Jurisdiction and Dispute Resolution	72
8.17 Co-operation and Support; Right to Deny Entry; Representations	72
8.18 Insurance	73
8.19 Taxes, Duties and Statutory Levies	73
8.20 Personnel; No Employer–Employee Relationship	73
8.21 Audit, Inspection and Step-in Rights	73
8.22 Publicity; Notices; Assignment; Waiver; Severability; Survival	73
8.23 Order of Precedence	74
8.24 Re-examination	74
Section 9 – Penalties and Liquidated Damages	75
9.1 Penalties for Examination Integrity and Conduct Failures	75

Content	Page no.
9.2 Penalties for Data, Reporting and Surveillance Failures	77
9.3 Caps and General Provisions	79
9.4 Penalty Administration Process	79
Section 10 – List of Annexures	80
Annexure E1 – Service Provider’s Letter for EMD / Bid Security	82
Annexure E2 - Bid Security (Bank Guarantee) Format	83
Annexure E3 - Service Provider's Information and Financial Details	84
Annexure E4 - Declaration Regarding Application Software (Ownership of Source Code)	85
Annexure E5 - Eligibility Criteria Matrix	86
Annexure E6 – Declaration for Acceptance of RFP Terms and Conditions	87
Annexure E7 – Declaration for Acceptance of Scope of Work	88
Annexure E8 – Format of Power of Attorney / Board Resolution	89
Annexure E9 - Other Undertakings (Clean Track, No Blacklisting, Conflict of Interest)	90
Annexure E10 - Non-Disclosure Agreement (Draft)	91
Annexure E11 - Format of Performance Bank Guarantee (PBG)	92
Annexure E12 - Bid Submission Compliance Checklist	93
Annexure S1 - Catalogue of SOPs and Manuals to be Delivered	94
Annexure T1 - Compliance to Technical & Functional Requirements	95
Annexure T2 - Service Provider's Experience	98
Annexure T3 - Declaration Regarding Clean Track Record	99
Annexure T4 - Client Details for Reference	100
Annexure T5 - Project Plan (incl. Contingency, BCP/DR and Exit Plan)	101
Annexure T6 - Short Description of the Proposed Solution	102
Annexure T7 - Exam Software Security Declaration	103
Annexure T8 - Scope of Independent Audit and its Requirements	104
Annexure T9 - Exam-Day Proformas and List of Stationery Items	105
Annexure T10 - Formats of Exam-Day Proformas	106
Annexure T11 - Data Deliverables Dictionary (Formats, Frequency and Mode)	124
Annexure T12 - Organization Structure and Personnel to be Deployed	126
Annexure P1 - Commercial Bid / Price Bid Format	127

Content	Page no.
Annexure IP - Pre-Contract Integrity Pact	128
Annexure C1 - Instructions to Candidates (to accompany the Admit Letter)	130
Annexure D1 - Outline of the Draft Agreement / Contract	131
Annexure F1 - Details of exam centers owned by Service Provider	132
Annexure CTR - Indicative Centre/City List	139

SECTION 1

Notice Inviting Tender (NIT) to conduct Online Examinations i.e. Computer Based Test (CBT) of the Institute in centre-based mode across India

The Indian Institute of Banking & Finance (IIBF) invites bids from eligible and qualified entities for the conduct of Computer-Based Test (CBT) examinations for its various flagship, professional, certification, diploma, and other examinations conducted across the country.

The objective of this tender is to identify and engage a competent and experienced empanelled agency capable of delivering end-to-end examination services in CBT mode, in accordance with IIBF's operational, technical, security, and quality requirements.

Through this tender process, IIBF seeks to establish a contractual relationship with a qualified Service provider that demonstrates the necessary expertise, infrastructure, resources, and capabilities to ensure the secure, seamless, transparent, and efficient conduct of CBT examinations while maintaining the highest standards of confidentiality, integrity, and candidate experience

BID SCHEDULE

Name of the Project: Selection of Service Provider(s) to conduct Online Examinations, i.e. Computer Based Test (CBT), of the Institute in centre-based mode across India.

Sr. No.	Description of Item	Date / Details
1	Date of release of the Request for Proposal	13 th August 2026
2	Tender Reference Number	IIBF/EXAM RFP-2/2026-27
3	Last date for submission of written pre-bid queries (to jd.exm2@iibf.org.in / add.dir@iibf.org.in)	19 th August 2026
4	Pre-bid meeting for clarification of written queries	25 th August 2026
5	Uploading of responses to pre-bid queries on the Institute's website	29 th August 2026
6	Last date and time of submission of Proposals	5 th September 2026 by 3:00 p.m.
7	Opening of Technical Bids in the presence of Service providers	5 th September 2026 by 4:00 p.m.
8	Technical presentations / demonstration by Service providers satisfying mandatory requirements	To be announced later
9	Opening of Commercial Bids of technically qualified Service providers	To be announced later
10	Tentative date of issue of Letter of Intent / Purchase Order	To be announced later
11	Earnest Money Deposit (EMD)	₹ 25,00,000/- (Rupees Twenty-Five Lakh only)
12	Place of bid submission and opening of bids; address for communication	Chief Executive Officer, Indian Institute of Banking & Finance, Kohinoor City, Commercial – II, Tower – I, 2nd Floor, Kiroli Road, Kurla (West), Mumbai – 400 070

Note: Technical Bids will be opened in the presence of the Service providers' representatives. In case a Service provider does not depute a representative, its bid will nevertheless be opened in the presence of the other Service providers / their representatives present. IIBF reserves the right to change any of the dates above by way of a corrigendum published on its website.

SECTION 2 – INTRODUCTION

2.1 About IIBF

Established in 1928 as a Company, the Indian Institute of Banking & Finance (IIBF), formerly known as The Indian Institute of Bankers (IIB), is a professional body of banks, financial institutions and their employees in India, with a mission to develop professionally qualified and competent bankers and finance professionals primarily through a process of education, training, examination, consultancy/counselling and continuing professional development programmes. Over more than nine decades of service, IIBF has emerged as a premier institute in banking and finance education. Since inception, the Institute has awarded several banking and finance qualifications, viz. JAIIB, CAIIB, and Diplomas and Certificates in specialised areas. IIBF is an ISO 21001:2018 certified organisation with its Corporate Office in Mumbai and Professional Development Centres in Mumbai, Delhi, Chennai, Kolkata, Guwahati, Lucknow and Bengaluru. The Institute has over 11 lakh ordinary members and around 753 active institutional members (banks, NBFCs and financial institutions).

2.2 Background

Major activities of the Institute include membership services, flagship and specialised courses, publications (daily e-newsletter "Fin@Quest", monthly "IIBF-Vision", quarterly "Bank Quest"), research sponsorship, and continuing professional development programmes. The Institute currently offers, inter alia, the following courses, all backed by specially developed courseware:

Category	Courses (indicative)
Flagship courses	JAIIB; CAIIB; Diploma in Banking and Finance
Diploma courses	Diploma in Treasury, Investment and Risk Management; Diploma in International Banking and Finance; Certified Wealth Management Professional; Certificate in Urban Co-operative Banking; courses for Specialist Officers of Banks, etc.
Certificate courses	Anti-Money Laundering & KYC; Trade Finance; Information System Banker; IT Security; Cyber Crimes & Fraud Management; FEMA; Emerging Technologies; Strategic Management & Innovation in Banking; blended courses in Credit Management, Treasury, Compliance, Risk Management, Accounting & Auditing, etc.

The Institute conducts examinations for more than 30 courses/certificates covering 52-plus subjects/papers. The duration of each paper is around 2 hours. Each paper consists of 100 to 120 multiple-choice questions for 100 marks, with no negative marking. Around 6 lakh subject-wise candidates apply for these examinations once every six months, i.e. around 12 lakh subject-wise candidates in a year. The examinations are presently conducted in an online (CBT) mode through outsourced service providers across 254-plus cities in India, using a distributed model with nodes connected via LAN to a local test server at each venue. Question banks are prepared solely by the Institute, and the data received from the Service Provider after each examination is processed internally by the Institute for evaluation of final scores and declaration of results; test batteries are loaded centrally into the Service Provider's test engine and downloaded in encrypted form through secured VPN (with at least 256-bit SSL encryption) at the venue servers shortly before the commencement of a test. Enrolment/registration is done by IIBF through its web portal, and candidate data (photo, signature, etc.) is provided to the Service Provider after registration.

Broad examination pattern (indicative; parameters vary by examination and are configured as per IIBF's instructions):

Parameter	Typical Value
Number of courses / subjects	30+ courses; 52+ subjects/papers
Duration of each paper	Around 2 hours (1/2/3-hour configurations possible)
Question format	100–120 multiple-choice questions per 100 marks; case-study/group questions and numeric key-in questions;
Negative marking	None
Sessions per day	Preferably in one or two sessions, but not more than 3 sessions, with a gap of at least 45 minutes between each session.
Peak single-day volume	Upto 1,00,000 candidates across all centres
Annual volume	Around 12 lakh subject-wise candidate tests ($\approx$ 6 lakh per half-yearly cycle)
Cities	254+ across India
Languages	English, Hindi and other Indian languages as notified, in IIBF-specified fonts

2.3 Objective of this RFP

Through this RFP, the Institute desires to select capable, reputed and experienced Service Provider(s) to conduct CBT (online) assessments/examinations at centres across India in a secure, transparent and fully auditable manner and in strict compliance with all the applicable laws, rules, regulations, policies and guidelines in force from time to time. The selected Service Provider(s) shall take responsibility for conducting CBT examinations for up to 1,00,000 candidates in any single day (with a maximum of 3 sessions of one or two hours' duration each, with a gap of at least 45 minutes between two sessions) across all centres in India. The Service Provider should possess prior experience of conducting large-scale public examinations for governments, reputed educational institutes and major organisations, with utmost confidentiality and best-in-class physical and logical security features.

2.4 Cost of the RFP and Due Diligence

Service providers shall bear all costs associated with the preparation and submission of their bids, and IIBF shall in no case be held responsible or liable for these costs, regardless of the conduct or outcome of the bidding process. Service providers should examine this RFP carefully; any ambiguity, contradiction, inconsistency, gap and/or discrepancy shall be raised as a pre-bid query within the timeline in Section 1. The Bid shall be deemed to have been submitted after careful study and examination of this RFP. Failure to furnish all information, or submission of a bid not responsive to this RFP, shall be at the Service provider's risk and may result in rejection of the bid. IIBF reserves the right to cancel the RFP process at any point in time without assigning any reason whatsoever.

2.5 Definitions and Abbreviations

Term / Abbreviation	Full Form	Definition
AI	Artificial Intelligence	Computer systems designed to perform tasks that normally require human intelligence, such as facial recognition and anomaly detection.
AI/ML Face Match	Artificial Intelligence / Machine Learning based Face Matching	Automated comparison of a candidate's live photograph with the registered photograph to verify identity.
API	Application Programming Interface	A set of protocols and methods that enables secure communication and data exchange between two software applications.
Audit Trail	-	A chronological electronic record of all actions, transactions, user activities and system events.
Authentication	-	Process of verifying the identity of a user, candidate or system before granting access.
Authoring Tool	-	Software used by IIBF for creating, managing and maintaining question banks and question papers.
BCP	Business Continuity Plan	Documented plan to ensure continuation of services during disruptions or disasters.
Bandwidth Monitoring	-	Process of measuring and tracking network usage and capacity to ensure sufficient connectivity during examinations.
Biometric Authentication	-	Identity verification using unique biological characteristics such as fingerprints or facial images.
Blacklisting	-	Process of permanently blocking a device, system, venue or user from participating in examination activities.
Buffer Node	-	Spare candidate workstation kept ready to replace failed examination nodes.

Term / Abbreviation	Full Form	Definition
CAPTCHA	Completely Automated Public Turing Test to Tell Computers and Humans Apart	Security mechanism used to distinguish humans from automated systems.
CAPA	Corrective and Preventive Action	Structured process to identify root causes of issues and prevent recurrence.
CBT	Computer Based Test	Examination conducted electronically using computers rather than paper-based methods.
CERT-In	Computer Emergency Response Team - India	National agency responsible for cyber-security incident response and security certification in India.
Central Server	-	Primary server used to manage examination data, question papers, responses and system controls centrally.
Click-by-click log	-	Detailed record of every mouse click, response selection and navigation activity performed by a candidate.
Cloud Storage	-	Secure storage of data on remote internet-based servers.
Command Centre	-	Central monitoring facility used for real-time oversight of examination operations across venues.
Concurrent Users	-	Number of users accessing a system simultaneously.
Cyber Security Incident	-	Any event that threatens confidentiality, integrity or availability of systems or data.
Data at Rest	-	Data stored on servers, storage devices or databases.
Data in Transit	-	Data being transmitted across networks.
Data in Use	-	Data actively being processed by applications or systems.
Data Centre (DC)	-	Centralized facility housing servers, networking equipment and storage systems.

Term / Abbreviation	Full Form	Definition
De-mapping	-	Removal of a candidate's original seat or node assignment.
Disaster Recovery (DR)	Disaster Recovery Site	Secondary infrastructure maintained for business continuity if the primary site fails.
DG Set	Diesel Generator Set	Backup power source used during electricity outages.
Encryption	-	Process of converting data into a secure format accessible only through authorized decryption methods.
Exam Engine / Test Engine	-	Software platform used to conduct and manage CBT examinations.
Examination Functionary	-	Any authorised individual involved in examination operations, including venue in charge, invigilators, IT staff, security personnel and registration operators etc.
Face Recognition	-	Technology used to identify or verify individuals using facial features.
Firewall	-	Security system that controls and filters network traffic.
Frisking	-	Physical security screening conducted before candidate entry into examination venues.
GUI	Graphical User Interface	Visual interface through which users interact with software applications.
Heartbeat Monitoring	-	Mechanism used to continuously verify whether a server or system remains operational.
HHMD	Hand Held Metal Detector	Device used for detecting prohibited metallic objects during frisking.
HLS	HTTP Live Streaming	Standard video streaming protocol for delivering live CCTV feeds.
HTML	HyperText Markup Language	Standard language used for displaying content within web-based applications.
Intrusion Detection	-	Monitoring mechanism used to identify unauthorized system or network access attempts.
IP Address	Internet Protocol Address	Unique numerical identifier assigned to a device connected to a network.

Term / Abbreviation	Full Form	Definition
IPR	Intellectual Property Rights	Legal rights covering copyrights, patents, trademarks and proprietary technologies.
ISO	International Organization for Standardization	International body that develops quality, security and management standards.
ISO 9001	-	International standard for Quality Management Systems (QMS).
ISO 27001	-	International standard for Information Security Management Systems (ISMS).
ISO 20000-1	-	International standard for IT Service Management Systems.
Jammer	-	Device used to block wireless communication signals around examination venues.
JSON	JavaScript Object Notation	Structured data format used for system-to-system information exchange.
LAN	Local Area Network	Network connecting computers and servers within a limited area such as an examination venue.
LAN Sanitisation	-	Process of inspecting and cleaning the examination network to ensure no unauthorized devices or connections exist.
LAN Scaping	-	Comprehensive mapping, scanning, verification and certification of the entire LAN environment, including nodes, switches, IP addresses, MAC addresses and connected devices, to identify unauthorized, suspicious or non-compliant devices before examination commencement.
Liveness Detection	-	Technology used to confirm that a biometric sample originates from a real person and not a photograph or spoofing attempt.
Load Monitoring	-	Tracking system performance and utilization under expected examination loads.

Term / Abbreviation	Full Form	Definition
MAC Address	Media Access Control Address	Unique hardware identifier assigned to a network interface card.
MFA	Multi-Factor Authentication	Security mechanism requiring multiple identity verification methods before access is granted.
MIS	Management Information System	Reporting framework used for operational and management analytics.
MOU	Memorandum of Understanding	Formal agreement establishing obligations between parties.
MTS	Multi Tasking Staff	Support personnel deployed for various operational activities.
Netboot	Network Boot	A secure mechanism through which examination computers boot directly from a network server instead of a local hard drive.
NOC	No Objection Certificate	Official confirmation permitting a specific activity.
Node	-	Individual computer terminal allocated to a candidate for examination.
OTP	One Time Password	Time-bound authentication code valid for a single use.
OS	Operating System	Core software enabling computer hardware and application functionality.
Proxy Candidate	-	Unauthorized person appearing in place of a registered candidate.
Public IP	Public Internet Protocol Address	Globally accessible IP address assigned by an internet service provider.
PwD	Persons with Disabilities	Candidates eligible for examination accessibility support, extra time, scribe etc. as per applicable guidelines.
QB	Question Bank	Repository of examination questions maintained by IIBF.
QP	Question Paper	Final examination paper generated from the question bank.
QR Code	Quick Response Code	Machine-readable code used for candidate verification and information retrieval.

Term / Abbreviation	Full Form	Definition
RCA	Root Cause Analysis	Structured investigation to determine the fundamental cause of an issue or failure.
Real-Time Synchronization	-	Immediate transfer and updating of examination data between systems without manual intervention.
RTSP	Real Time Streaming Protocol	Protocol used for streaming live CCTV video feeds.
RTO	Recovery Time Objective	Maximum acceptable time required to restore services after disruption.
RPO	Recovery Point Objective	Maximum acceptable amount of data loss measured in time.
Safe to Host Certification	-	Security certification confirming that a software application can be securely deployed in production environments.
SPOC	Single Point of Contact	Designated person responsible for communication and coordination.
SSL	Secure Sockets Layer	Encryption protocol used to secure data transmission over networks.
STQC	Standardisation Testing and Quality Certification	Government certification body that validates quality, security and compliance of IT products and systems.
STR	System Test Run	Controlled testing exercise conducted before production deployment.
Tier-III Data Centre	-	High-availability data centre infrastructure designed with redundancy and fault tolerance.
UAT	User Acceptance Testing	Process of validating whether a solution satisfies user requirements before deployment.
UFM	Unfair Means	Any activity that compromises examination integrity, confidentiality or fairness.
UIDAI	Unique Identification Authority of India	Authority responsible for Aadhaar-related services and authentication.
Unicode	-	International character encoding standard supporting multiple languages and symbols.

Term / Abbreviation	Full Form	Definition
UPS	Uninterruptible Power Supply	Backup battery system providing immediate power during outages.
VPN (with at least 256-bit SSL encryption)	Virtual Private Network	Secure encrypted communication channel used to transmit examination data between systems.
VLAN	Virtual Local Area Network	Logical segmentation of a network to improve security and traffic isolation.
Whitelisting	-	Restricting system access exclusively to pre-approved devices, applications, users or network addresses.
XML	Extensible Markup Language	Structured format for storing and exchanging data between systems.

2.6 Ownership of this RFP

The content of this RFP is copyright material of IIBF. No part of this RFP shall be published by Service providers in print or electronic media without prior written permission from IIBF.

SECTION 3 – SCOPE OF WORK

3.1 Broad Scope of Work

The broad scope of work covers:

- A. Pre-Examination activities;
- B. During-Examination activities; and
- C. Post-Examination activities.

The Service provider shall provide the services with the highest degree of integrity and confidentiality. The Institute has maintained very high standards in the conduct of its examinations, and the Service Provider must ensure that the performance of its services does not adversely affect or damage the Institute's reputation. Compliance with all Technical & Functional Requirements in Annexure T1 is mandatory.

A. Pre-Examination activities:

A.1 Operations by IIBF

1. Enrolment/registration for the examination will be done by IIBF using its web portal; eligible candidate data will be provided to the Service Provider.
2. Uploading and rendering of Question Papers and verification of candidates' logins will be done by IIBF with the assistance of the Service Provider.
3. Preparation of question papers / question bank and evaluation of candidates' scores: The preparation of the question bank/question papers, the marking scheme, the final evaluation of candidates' scores and processing of results, shall remain the sole and exclusive responsibility of IIBF and shall be carried out internally by the Institute. The Service Provider's role is strictly limited to the secure hosting, rendering and delivery of the question papers provided by IIBF, the secure capture and transmission of candidate responses, showing provisional scores on exam submission by the candidate and providing link for downloading provisional score card within 2-3 days after examination, and the provision of complete examination data to the Institute for its internal result processing.

A.2 Operations by Service provider

1. The Service provider must own the CBT software (test engine), including its source code and all components, used to conduct the online examinations, and provide documentary proof thereof. The software shall be certified as "Safe to Host" by a CERT-In empanelled agency; the certification exercise must be conducted every year at the Service provider's cost, kept valid throughout the Contract term, and made available to the Institute. The examination software should be STQC/CERT-In certified and the Service provider's processes should conform to ISO 9001, ISO 20000-1 & ISO 27001 Certification standards.
2. Timer and compensation: The system must automatically stop the examination when the prescribed examination duration is completed. In the event of any delay, interruption, break in connectivity, system failure, power failure, server/node failure or any similar technical/operational disruption not attributable to the candidate, the examination timer shall automatically pause and, upon restoration/resumption, shall restart from the exact point at which it had stopped, so that the candidate receives only the balance unutilised examination time. No additional or compensatory time shall be granted for any break voluntarily taken by the candidate, including bio-breaks or any absence from the candidate node for reasons attributable to the candidate. The system shall maintain complete logs

of all timer pauses, resumptions, interruptions and compensations, including candidate-wise timestamps and reasons, and such logs shall be provided to the Institute.

3. The application shall allow candidates to appear only at the pre-determined date/time and venue mentioned on the admit card, after verification of identity, admit card and original photo ID; AI/ML-based face matching of the photo captured at the venue against the photo shared by IIBF shall be performed before allowing entry, and mismatch logs shall be shared with IIBF.
4. Random, automated seat (candidate node) allocation shall be performed by the system at registration desk, without any discretion of ground staff; the candidate's examination shall open only on the allotted node. Any request for de-mapping or re-mapping of a candidate shall be initiated by the Service Provider through the system to IIBF in the prescribed format, along with the reason for such change, candidate details, original allotted node details and the details of the proposed buffer node to which the candidate is required to be re-mapped. Such de-mapping/re-mapping shall be carried out only after approval from IIBF. Upon approval, the Service Provider shall generate a candidate-specific one-time password with defined expiry time for enabling login on the approved buffer node. Such password shall be valid for one-time use only, shall be used only by the specific candidate for whom it has been generated, and shall not be transferable, reusable, usable by any other candidate, or usable on any node other than the node approved by IIBF. Complete system logs of the request, approval, OTP generation, expiry, usage, candidate login and node mapping shall be maintained and submitted to IIBF as part of the incident report after each examination.
5. The exam software shall provide a summary panel (attempted/un-attempted/bookmarked questions), auto-save, review and auto-submit on expiry of duration, with early submission permitted only after the minimum time specified by IIBF.
6. Every venue shall have UPS and generator/adequate power backup for uninterrupted conduct of the examination before, during and after the exam. Mock run should be done at least one day before the actual examination. Service Provider to ensure that the power backup solution suffices as per the seating capacity of the examination venue.
7. The service provider shall maintain a secured environment for uploading question papers and candidate responses and shall indicate the degree of customisation required in the test engine to meet the Institute's requirements.
8. The Service Provider will have to carry/ demonstrate complete System Test Run (STR) with test data to IIBF before implementation of the Information Technology/ Tech Solution. IIBF can deploy an independent agency to oversee this activity.
9. Computer based examination software shall support standard features such as display of details of candidates, including photo, signature etc, detailed instruction upon login, start and closure of examination at scheduled time, time left, flag questions for review, marking/ unmarking of question(s), display of status of questions with different colour and symbols, switching between sections (if applicable), switching between Hindi and English languages or any other language as applicable, provision for enlargement of font, navigation to unanswered questions and prompt for submission. If IIBF decides for timer(s) for answering questions or sections, the same needs to be provided by Service Provider in its Exam Software Solution.
10. There shall be malpractice awareness message before instructions page and candidates shall be required to read it mandatorily and confirm having understood the same.

A.3 Minimum Hardware, Software and Network Specifications

The following are minimum specifications; the Service provider may propose higher configurations. All installations shall be on a lease/rent/owned basis at the Service provider's cost, included in the quoted rates.

1. **Service Provider's test engine:** The test engine shall support the following
 - (a) Bilingual display (English/Hindi and other Indian languages in IIBF-specified fonts).
 - (b) Display of image and group/case-study with questions based on the case.
 - (c) Display images of different formats along with the text on the same screen.
 - (d) To ensure high-clarity and complete image within the display area along with the respective question in the same screen.
 - (e) Date Format: All functionalities must properly display and transmit date data in DDMMYYYY format.
 - (f) Different sections with individual timings.
 - (g) To enable candidates to navigate between questions within the stipulated time (within a section, if the Question Paper is designed as such).
 - (h) Capable of rule-based, module-wise examinations.
 - (i) Export/import of data in XLS/XML/JSON (should support questions with table and symbols).
 - (j) Capture candidate feedback, provide summary and give report.
 - (k) Option to set parameters while submitting an examination.
 - (l) Option for parameter-based question paper generation for candidate display.
 - (m) Display of candidate details, photo and signature on the exam screen.
 - (n) A virtual keyboard, virtual simple calculator for calculations and virtual notepad for rough work during exam on the exam screen.
 - (o) Automatic randomised generation/shuffling of question papers. To present questions and answer options in a randomized way in such a manner that every candidate gets a different version of randomized question set.
 - (p) "Question without options" (numeric key-in) questions with virtual keyboard, as detailed in Annexure T1.
 - (q) In the event of any revision to a question paper or answer key, the test engine shall support correction/modification of the specific question paper, question, option, answer key or related content in which the error has been identified, as per IIBF's instructions.
 - (r) For flagship exams the question bank and answer key shall be pushed separately. The answer key shall be pushed to the Central Server only 30 minutes prior to the completion of the respective examination session, in a secure and encrypted manner as per IIBF's instructions.

- (s) Candidates shall be permitted to submit the examination only after completion of 1:45 hours from the commencement of the examination, or such minimum duration as may be specified by IIBF for the respective examination.
- (t) Mock test facility shall be provided to candidates before starting the actual examination

2. Test Engine Deployed at Institute's Premises: Features are as follows

- (a) The Service Provider shall deploy the test engine at IIBF's premises on a laptop/system supplied by the Service Provider and ensure that it supports the complete QB/QP lifecycle, including master creation, subject structure creation, QB/QP upload, validation, mapping/cloning, verification, and encryption/security.
- (b) The test engine shall provide facility to upload QB/QP data, including text, images, symbols and other required content, in XLS, JSON, XML or any other format prescribed by IIBF.
- (c) The application shall support all Unicode fonts, bilingual display of questions in English, Hindi and other languages, scrolling of questions/options where content exceeds screen length, and accurate upload and display of images forming part of questions or answer options.
- (d) The application shall provide QP mapping and cloning functionality, including mapping one set of QP to multiple examination batches, mapping/cloning QP of normal candidates to visually impaired candidates/extra-time batches, and mapping/cloning one QP from one exam code/subject code to another exam code/subject code across all applicable languages.
- (e) The application shall support parameter-based shuffling of questions and answer options.
- (f) The system shall validate all prescribed parameters at the time of QB upload, including module-wise, unit-wise and marks-wise availability/selection of questions, and the QB/QP shall not be uploaded or accepted if any prescribed parameter does not match IIBF's requirements.
- (g) For questions without options, including numeric key-in questions, the test engine shall support answers based on absolute value or with decimals as well as answers falling within a predefined permissible range.
- (h) For numeric/key-in questions, the system shall provide a virtual keyboard for candidates to enter their answers.
- (i) After successful upload of QB/QP, the system shall provide a dummy/test candidate login facility for IIBF to verify content accuracy, formatting, question rendering, image rendering, question-wise answers and marks assigned after test submission.
- (j) The dummy/test candidate login facility shall be disabled immediately after completion of checking/validation and before the live examination.
- (k) The Service Provider shall certify that all uploaded content is identical to the upload file provided by IIBF, without truncation of text, additional or missing characters, cropping, distortion or loss of image clarity, and that the dummy/test candidate login facility has been disabled after validation.
- (l) The Service Provider shall maintain strict confidentiality and security of QB/QP data at all levels and at all stages.

- (m) All QB/QP data hosted on servers shall remain encrypted.
- (n) The password/credentials required to decrypt the QB/QP on the examination day(s) shall be shared only with authorised personnel approved by IIBF.
- (o) The Service Provider shall provide encrypted API integration with IIBF's Authoring Tool/Question Bank software for secure transfer of QB files from the Authoring Tool to the test engine deployed at IIBF Corporate Office / Question Bank Department.
- (p) Upon completion of the examination cycle, generation of all reports and confirmation from the Examination Department, the system shall provide a facility to the authorised QB Admin of IIBF to delete the uploaded QB/QP content.
- (q) After deletion of QB/QP content, the Service Provider shall provide a certificate confirming that the data has been completely deleted and that no trace of QB/QP data remains at the Service Provider's site, central server, venue server, systems, backups or any other storage location, except where retention is expressly approved in writing by IIBF.
- (r) The Service Provider shall depute authorised representatives at IIBF's Question Bank Department during the QB upload process and on all examination days, as required by IIBF

3. Central Server

- (a) The Central Server shall provide a centralized, secure, and system-driven platform for onboarding, registration, authentication, and management of authorized examination functionaries involved in examination operations.
- (b) The Central Server shall facilitate secure retrieval and distribution of question papers from the IIBF systems to venue servers only through authorized and system-controlled processes.
- (c) All examination-related data, including question papers, candidate information, candidate responses, logs, audit trails, and administrative transactions, shall remain encrypted during transmission and storage.
- (d) The Central Server shall support configurable, automated, and system-driven approval workflows for examination activities, requests, and access controls as defined by IIBF from time to time.
- (e) All requests, approvals, authorizations, and workflow transactions shall be electronically recorded, time-stamped, auditable, and traceable.
- (f) Access to critical examination functions, systems, and any data, shall be governed through policy-based authorization and role-based access controls.
- (g) All authorizations for critical activities shall be time-bound, purpose-specific, and automatically expire upon completion of the defined validity period, examination shift, event, or approved activity.
- (h) The system shall ensure that question papers are released only to authorized and validated examination locations, systems, and devices mapped through predefined security controls.

- (i) Question paper distribution shall be restricted to registered and authorized infrastructure, including designated IP addresses, examination venues, servers, and candidate node approved for the concerned examination session/batch.
- (j) The Central Server shall maintain complete audit logs of all authentication events, approvals, question paper downloads, data transfers, administrative actions, and security-related activities.
- (k) The Central Server shall be capable of securely decrypting candidate response data received from venue servers and processing the same for evaluation, reporting, and result-generation purposes.
- (l) The Central Server shall implement appropriate controls to ensure data integrity, confidentiality, availability, non-repudiation, and traceability throughout the examination lifecycle.
- (m) All critical transactions and data exchanges between the Central Server and other examination systems shall be monitored, logged, and protected against unauthorized access, alteration, disclosure, or misuse.
- (n) All the data pertaining to QB/QP shall be deleted from the Service Provider's site, central server, venue server, systems, backups or any other storage location, except where retention is expressly approved in writing by IIBF on same day after completion of examination batch/session. After deletion of QB/QP content, the Service Provider shall provide a certificate confirming that the data has been completely deleted and that no trace of QB/QP data remains.

4. Venue Server (primary; plus one backup server per 200 candidates and a registration server):

- (a) The Service Provider shall deploy Venue server which includes one Primary Venue Server, one Registration Server, and at least one Backup Venue Server for every 200 candidates at each examination venue.
- (b) The Primary Server shall have a minimum processor speed of 1.5 GHz and minimum 4 GB RAM or higher, as required to ensure uninterrupted examination operations.
- (c) The server infrastructure shall support at least 200 concurrent candidates without any perceptible degradation in performance.
- (d) Question paper and examination page loading time shall not exceed one second under normal operating conditions.
- (e) The registration server shall support candidate registration, candidate verification, and automated node allocation.
- (f) All candidate actions, including mouse clicks, keyboard inputs, navigation activities, virtual calculator inputs, notepad inputs and responses, shall be recorded with accurate timestamps and captured in real time.
- (g) Only authorized candidate nodes shall be permitted to communicate with the Primary Venue Server.
- (h) The Primary Venue Server shall be a hardened and secured server configured exclusively for examination operations.

- (i) All question papers, candidate data, candidate responses, biometric data, photographs, logs, audit trails, backups, and all other examination-related data shall remain encrypted at rest, in transit, and during processing on all venue servers.
- (j) All data exchange between IIBF systems, Service Provider systems, Central Servers, Venue Servers, Backup Servers, and examination nodes shall take place only through secure VPN (with at least 256-bit SSL encryption) connectivity protected by Multi-Factor Authentication (MFA) through out the examination cycle.
- (k) Question paper decryption shall be carried out only in memory, and no decrypted question paper shall be stored on any server, workstation, or local device.
- (l) Randomization of question papers and questions shall be carried out securely in memory before delivery to candidates.
- (m) No candidate response data shall be stored locally on candidate nodes. The examination software shall synchronize candidate responses with the Venue Server in real time, leaving no residual data on any candidate node.
- (n) Candidate response data shall be shared with IIBF after completion of each the subject examination in the prescribed format through secured channel.
- (o) The examination network shall be segregated through VLAN architecture, and unauthorized network access shall be prevented through appropriate security controls.
- (p) Remote access services, non-essential services, and sensitive ports on the Venue Servers shall remain disabled throughout the examination process.
- (q) Access to USB devices, removable media, external storage devices, peripherals, and any unauthorized hardware shall be blocked on all Venue Servers, and no external device shall be permitted to connect to the Primary Venue Server at any stage of the examination lifecycle.
- (r) The Service Provider shall perform periodic LAN scanning to identify unauthorized or non-compliant devices, and such devices shall be automatically isolated, blacklisted/blocked, logged, and reported.
- (s) Any attempted intrusion, cyber-security incident, unauthorized access, malware detection, or security breach shall be immediately reported to IIBF in accordance with the prescribed SOP and incident reporting requirements.
- (t) The Primary Venue Server shall continuously and automatically replicate candidate response, examination data, logs, audit records, etc. to the Backup Venue Server in real time without loss of data.
- (u) In the event of server failure, network disruption, or connectivity loss, the examination system shall automatically recover and enable candidates to resume the examination from the exact point of interruption without any loss of data.
- (v) The system shall ensure complete data integrity, confidentiality, traceability, and availability of all examination-related information at all times.

5. Candidate Node (each examination terminal):

- (a) Each candidate node shall have at least a 15-inch monitor with screen resolution of 1024 × 768 or higher and shall be equipped with a mouse. A physical keyboard may be provided where required (only for inputting password at the start of the exam); however, for numeric/key-in questions, the system shall also provide an on-screen virtual keyboard as prescribed by IIBF.
- (b) The CBT examination shall be conducted on a secured Netboot-based environment. Candidate nodes shall boot only from the authorised CBT exam interface provided and shall not run any local operating system, local software, dual-boot configuration or unauthorised application from hard disk, static storage or any other local storage device.
- (c) The examination interface shall disable or restrict all non-essential functions and access during the examination, including USB access, local storage of responses, remote desktop access, sensitive ports, unauthorised web resources, screen switching, screen capture, copy-paste, cut-paste and unauthorised keyboard shortcuts.
- (d) Only the genuine and authorised interface required to interact with the venue/local server shall be available on the candidate node. No unauthorised hardware, software, process, service, peripheral, external network, foreign traffic or external storage device shall be permitted to connect to or operate on the candidate node during the examination.
- (e) The system shall be capable of detecting, logging and preventing network intrusion, foreign traffic, unauthorised devices, unauthorised processes, external networks and any other non-compliant activity affecting candidate nodes, venue/local servers or the central server. The Service Provider shall maintain detailed logs of such events and submit reports to IIBF as and when required.
- (f) If any unauthorised hardware, software, process, traffic or other non-compliance is detected, the system shall immediately trigger appropriate stop-exam/blacklisting/de-mapping controls for that node and prevent the examination from continuing on such node.
- (g) Any blacklisted or de-mapped candidate node shall be used again for examination purposes only after sanitisation, rectification, successful revalidation and due approval from IIBF, and only from the subsequent examination shift or such later time as may be approved by IIBF.
- (h) Any issues in content/QP/other functionalities displayed during examination at candidate node shall be the sole responsibility of Service provider.

6. Network and Connectivity per venue:

- (a) Two separate independent secure internet connections one exclusively for QP/response transmission over secure VPN, the second for CCTV and general use each with sufficient bandwidth measured and certified during the mock (bandwidth monitoring).
- (b) Managed switches with access logging, LAN-based (intranet) exam delivery, documented network diagram per venue and public IPs of all servers used by venues should be shared with IIBF.
- (c) Full power backup (UPS and DG) sized for all nodes, servers, CCTV, jammer support if required in future, lighting and air-conditioning, before, during and after the examination.

7. Command Centre and Communication Protocol

- (a) The Service provider shall establish and operate, for every examination day (including mock day), a central Command Centre integrating live CCTV wall of specified venues; real-time exam-progress dashboard; incident-ticketing with severity classification; helpdesk/toll-free lines; and direct hotlines to every Venue In-charge and City Head. IIBF shall be provided dedicated dashboard logins and a seat-view at the Service provider's Command Centre, and equivalent feeds to IIBF's own monitoring facility.
- (b) The Service Provider must provide an automated Dashboard in the control room at IIBF HQ. Service provider shall provide the required hardware, peripherals including LEDs and Software. Control Room at Institute's HQ to consist of:
 - (i) Live CCTV monitoring facilities through LED screens.
 - (ii) Live feeds of CCTV surveillance data (on demand) as prescribed by IIBF. It shall be available on Graphical User Interface (GUI) drilling down to the venue level.
 - (iii) A National Level status indicator will be available at the HQ which will display the status of Examinations at Pan-India Level and at City/ Venue level.
 - (iv) Dashboards must be real time to the extent possible. Information that cannot be shown Real-time shall be available on Near-Real-time' mode.
 - (v) Other information, as desired by the IIBF shall be made available as downloadable reports for end of shift, end of day and end of complete examination.
 - (vi) The dashboard will contain the following aspects: Attendance at each venue (no. of candidates appearing for exam), Number of blacklisted nodes, Number of de-mapping cases, Number of Invigilators/ other exam functionaries, except for the candidate's examination data, all major aspects of venue will be available on this dashboard such as status of start & end of each examination batch, capturing of biometric details, status of random seat allocation, download of question paper from Data Centre to Venue Server, no. of live nodes, status of any node getting affected, status of transfer of exam data to central system, status of gate closure of the batch once the exam starts, any other relevant information.
 - (vii) The Service Provider shall depute authorised representatives on the exam days to the Exam Department of the Institute to facilitate monitoring of exams and resolution of issues if any at the centres/venues.
 - (viii) Checklist of facilities at each venue must be made available for IIBF.

A.4 Question Paper Management

1. The test engine shall provide facility to upload the question paper using XLS/XML/JSON files as per IIBF formats and fonts, including zip files (encrypted with unique batch-wise passwords) containing images in .jpeg/.jpg. The QB will be created by IIBF and uploaded, with Service provider support, on a standalone local server (with the same test engine software) provided by the Service provider at IIBF premises, without internet connectivity.
2. On completion of QB/QP upload onto the test engine of the Service provider, summary reports (section/module/marks-wise) to be provided by the Service provider as required by IIBF. Facility of

customized reports to verify the uploaded data summary (like section/module/unit wise marks wise) is required in the application.

3. Test engine should have security features like data encryption for content during all three states of data i.e. data in rest, data in transition and during process of data (question paper).
4. It should have the feature of administering the “Question without Answer option” (numeric questions), where candidate will not be provided any options (no choice for answer), candidate has to key in the answer. Description of ‘Question without option, numeric’ given below:
 - a. These questions will not be in the MCQ format i.e. no answer options will be provided.
 - b. After every question, a response box will be provided for keying in the answers.
 - c. The candidate will have to key-in the response for each such question.
 - d. Candidate will be required to only use ‘Virtual keyboard’ in-built into the system to key in the numbers /sign.
 - e. These questions will be numerical in nature. The candidate will be required to key in numbers (0 to 9) along with appropriate prefix. If the answer is negative, it should be preceded by ‘-’ sign.
 - f. The ‘-’ sign wherever applicable should precede the number. For example, if the correct answer is -27, in the response box, the candidate has to key in ‘-’ sign first followed by 27, i.e. the answer should be shown as -27.
 - g. In case the candidate has to provide the answer in decimals, he/she will have to key in the required number of digits after the decimal (.) sign, as specified in the question.
 - h. Candidate can key-in only numbers, ‘-’ signs or (.) decimal point. No alphabet and other character/s like coma (,) or hyphen (-) will be accepted.
 - i. After keying-in the response, the candidate will have to save the answer by clicking the “Save” button before moving to the next question. A prompt should be given to save the typed answer. If the candidate does not click on the “Save” button, the response keyed-in by the candidate will not be saved and consequently, the question concerned will be considered “not attempted”.
 - j. Facility of virtual keyboard (English only for numeric operated through ‘Mouse’ required along with physical keyboard).
5. Login-based application interfaces (with no manual intervention) shall be provided for:
 - a. Transfer of encrypted QB files from the IIBF standalone server to the Service provider's central servers 45 mins prior to each examination session.
 - b. Transfer of encrypted QB files from the Service provider's central server to venue servers 15 minutes before the scheduled examination time, batch-wise and
 - c. Transmission of decryption passwords through the application interface or with SMS delivery to authorised functionaries immediately upon the Institute inputting the password. The QB shall remain encrypted throughout and shall be decrypted only on the candidate's screen when the candidate starts the examination by inputting password.

6. For flagship exams, after completion of all batches for the day, all QB and response data shall be securely purged from venue servers and nodes as per the sanitisation protocol in Annexure T1, with certification to the institute.

A.5 Examination Venues

1. The Service provider shall identify secure venues in the cities specified by IIBF (indicative list at Annexure CTR), ensuring accessibility, location within city limits, proximity to public transport, and accessibility for differently abled (PwD) candidates including ramps/lifts, and PwD-appropriate computers and software.
2. Coaching venues or residential property shall not be used as examination venues for IIBF examinations. Premises owned, operated or controlled by coaching institutes, or entities engaged in training/coaching for banking or similar examinations, are prohibited. Further, no premises shall be used as an examination venue if any coaching, training or tutorial institute, whether or not related to banking and finance operates within the same building or within the same gated complex/compound, and the Service Provider shall certify this as part of the venue audit and Centre Master submission.
3. Congested areas to be avoided for conduct of examination. The examination lab shall not be located in the basement of any building. Venues shall have proper ventilation, lighting, ambient temperature (with heaters in hilly areas during winter), drinking water, clean washrooms, fire-safety, female medical and hygiene aids and first-aid arrangements. For the purpose of this sub-point, room heaters shall be provided in all venues in low-temperature regions (not limited to hilly areas) whenever the prevailing ambient temperature during the examination window is expected to fall.
4. Venues located within commercial complexes or multi-occupancy buildings should be avoided as the examination centre may not have a dedicated and exclusive entrance and exit, physically segregated from the entrance for the examination venue/lab with CCTV coverage from gate to lab, separate security for frisking etc. The nature of the premises (standalone / commercial complex / institutional) and the entrance arrangement shall be recorded in the venue audit.
5. All blocks of a venue shall be within the same premises, with controlled entry and exit gates covered by security guards to prevent unauthorised access.
6. Each venue shall maintain at least 10% buffer computer nodes (and sufficient additional switches) per shift, over and above the scheduled nodes.
7. Each venue shall have two separate independent secure internet connections, one exclusively for transmission of QPs and responses, and the second for general use such as CCTV streaming.
8. Every venue used to conduct IIBF examination(s) must have a wireline telephone connection along with wire line broadband connectivity at the server room in order to have seamless connectivity during the exam even when jammers are switched on wherever applicable in future.
9. The Service Provider shall not use any temporary, ad-hoc, make-shift, provisional or non-permanent venues for conduct of the examination. All examination venues must be established, regular and fully functional premises having adequate infrastructure, power backup, network connectivity, security arrangements, seating capacity, candidate amenities and statutory/local permissions required for conducting CBT examinations.
10. Service Provider's should prioritize conduct of the Institute's examinations at its owned centres.

A.6 Audit and Freeze of Examination Venues

1. Antecedent detail of the venue owner, in case of hired/ leased venues must be verified by the Service Provider and made available to the IIBF, if desired. The Service Provider should provide list of centre/venue owners and the name of person in charge appointed by them to oversee the operations at centre.
2. The Service Provider should have an agreement between them and exam centre which specifically specifies the terms & conditions of the conduct of examination which shall be presented to IIBF as and when requested.
3. Before booking of venue Service Provider should obtain an MOU/written confirmation from exam centre regarding availability for the exam period/dates and NOC which shall be presented to IIBF as and when requested.
4. Service Provider to ensure the availability of sufficient number of examination venues across the country covering all States and UTs.
5. The Service Provider must have back up arrangement of examination venue, if any of the venues offered earlier is dropped during IIBF audit.
6. For fair and smooth conduct of examination(s), IIBF is authorized to take any step as deemed fit in the venue(s) (including venue replacement) and bidder will unconditionally agree to it.
7. The vendor has to ensure that venues are arranged /available as per the requirements specified on the exam days.
8. All examination venues shall be audited by the service provider for compliance with infrastructure, security and operational requirements. Only audited and approved venues shall be used. Audit to be completed atleast 30 days prior to the examination. Institute may separately also verify the audited report.
9. The Service provider shall make available all information, data and access to infrastructure required of such audit(s) as and when required by IIBF. Meeting before every exam will be conducted at IIBF HQ with the Service Provider in order to discuss the issues, problems etc. (venue wise) faced during the previous exams and shall rectify all critical observations before the examination to the satisfaction of IIBF and shall replace any venue found unsuitable in such audit at no cost to the Institute. Non-compliant venues may be blacklisted. Any change or modification in this venue list (due to some operational issues) is to be made after approval from IIBF.
10. Service provider to ensure that the venues meet all the standard requirements of the RFP.
11. The list of approved venues shall be frozen at least 30 days prior to the examination, and no changes shall be permitted thereafter without the written approval of the Institute. The final soft copy of the Admit card data (including venue name, complete address, time slot etc.) as per the required format shall be provided to IIBF as per the agreed schedule; delay shall attract penalty as per Section 9.
12. Where such change results in candidate inconvenience, delay in commencement of examination, denial of entry, crowd management issues, confusion in reporting location, additional travel burden, adverse candidate complaints, reputational impact to IIBF, or requirement of re-scheduling/re-conduct of examination, IIBF may impose additional penalties as per Section 9, recover all related costs and

losses from the Service Provider, withhold payments, and/or take any other action available under the Contract.

13. Any emergency change of centre/venue shall be permitted only with prior written approval of IIBF and subject to the Service Provider providing complete justification, revised venue audit report, candidate communication plan, logistical arrangements and confirmation that all security, infrastructure, accessibility and examination-readiness requirements are fully complied with.
14. Service provider shall perform due diligence and police verification on the owner of the premises. In case of adverse findings such premises and owner should be added to debarred list which shall then be submitted to IIBF before freezing examination venues.

A.7 Venue Layout, Seating and Signage Norms

1. Seating: minimum spacing between candidate nodes as per IIBF requirement, with staggered/partitioned seating that prevents screen visibility between adjacent candidates; seat numbers displayed at each node; the candidate seating plan (room, seat, node ID/IP/MAC) generated by the system and preserved for the Mandatory Data Set. Each seat/node shall display exactly one unique seat number; no seat shall carry multiple or superseded numbers, and numbering shall run in a single continuous, logical sequence per lab consistent with the system-generated seating plan, verified during the mock run and certified in the node-certification proforma.
2. Minimum 2.5 feet seat width shall be available for candidates in such a way that a candidate cannot see the other candidate's screens. Ideally the seating should not be in the same direction.
3. There should be Partition between candidates. Partition between candidate screens shall be rigid. Partition shall not be done with Cardboard, transparent material, Polystyrene, asbestos.
4. Seating furniture shall be ergonomically comfortable and shall be of good quality.
5. Adequate space shall be available for candidates to place papers for rough work, if applicable.
6. Non-shadow lighting is mandatory for every hall of examination.
7. Computer node number (label) shall be clearly displayed prominently. Label print shall cover about 50% of the label. The label shall be clearly visible in the CCTV footage. Seating plan of the lab will be scanned and uploaded to the data centre along with other documents.
8. Signage and displays: prominent display at the venue of, venue code and name, direction signage from gate to labs; prohibited-items list; candidate instructions; emergency evacuation routes and assembly point; and helpline numbers. Adequate displays and instructions shall also be provided inside labs and at registration desks (with whiteboard background for image capture).
9. Segregated zones: Distinct, CCTV-covered zones for frisking (gender-segregated), document verification, registration, waiting area, CCTV monitoring room, and the server/strong room (access-controlled, entry-logged, CCTV-covered); the server room shall be occupied only by authorised IT personnel listed in Proforma 3.
10. In case the service provider has an office in the same building as of exam venue, separate entry and exit clearly isolating the exam venue shall be done. Service Provider shall ensure that there is no unauthorized access to the Exam Venue.

11. Each examination venue shall have a separate/ separated server room with proper access control mechanism, the servers must be in a room separate from the computer lab(s).
12. Proper and sufficient sockets should be available in each lab of exam venues for jammer installation if applicable in future and preferably these should be away from candidate nodes.
13. Examination venues must provide separate washroom facilities for examination functionaries and candidates. Additionally, separate washrooms must be available for male and female candidates. At designated PwD centres, accessible washroom facilities must also be provided for Persons with Disabilities (PwD) candidates.

A.8 Exam Functionaries – Verification and Compliance

1. The Service Provider shall do the due diligence, get the background check, police verification, criminal-record report conducted for all exam-related functionaries deployed at exam venues. Such verification shall not be more than one year old and shall be shared with IIBF before the examination as and when requested.
2. The list of all exam functionaries (all individuals associated with the exam deployed at each venue) shall be provided to IIBF atleast two week prior to the commencement of the examination along with details viz. name, father's name, mother's name, gender, DOB, mobile number, ID (Aadhar), address, education qualification etc.
3. The Service Provider shall keep a repository of documents and contact details of all manpower deployed at exam venues and share the same with IIBF as and when required.
4. The Service Provider shall rotate exam functionaries to different labs/venues during the exam or between different examinations, and Invigilators shall be shuffled after every shift. Service Provider shall ensure that invigilators are allocated to exam Labs randomly.
5. The Service Provider shall obtain a declaration from all functionaries (employed for the examination concerned) that none of them has any near relation (children, brother, sister, nephew, niece of self or spouse) or any person in whom they have a special interest appearing in the concerned examination (No-Relation Certificate, Annexure T10-Proforma).
6. Minimum staffing norms per venue:

S. No.	Position	Roles and responsibilities	Terms of engagement	Count
1	Chief Co-ordinator	Overall coordination with IIBF, central oversee the examination operations, escalation management and coordination with city/venue teams. Will be stationed at IIBF HQ	On-roll employee of the Service Provider	One assisted by one or more employees of the Service Provider.
2	City Head	Coordinates examination operations across all venues in the city, manages city-level escalation, supports venue readiness	On-roll employee of the Service Provider	1 per examination city

S. No.	Position	Roles and responsibilities	Terms of engagement	Count
		and liaises with the Command Centre and IIBF as required.		
3	Exam Controller/Venue In charge	Responsible for end-to-end venue operations, readiness, candidate movement, coordination with invigilators, IT staff, security/frisking staff and reporting of incidents.	Employee of the Service Provider	One per venue
4	IT Manager	Responsible for network coordination, technical troubleshooting	Employees/Contractual employees	One per venue
5	Server Administrator	Responsible for server administration, node readiness, QP download support, logs and secure data transfer.	Employee of the Service Provider. List must be provided to IIBF in advance.	1 per 250 nodes, minimum 1
6	Registration desk Manager	Manage the registration desk.	Employees/Contractual employees	One per 30 candidates.
7	Invigilators	Responsible for candidate supervision, maintaining exam discipline, monitoring suspicious conduct, issuing/collecting rough sheets if allowed, reporting incidents and assisting candidates for any issues only as per permitted instructions.	Employees/Contractual employees	1 per 15 nodes, minimum 2 per room for sensitive venues; 1 per 30 nodes, minimum 2 per room otherwise. Plus dedicated individual invigilator for every 5 scribe candidate
8	Support Staff	Supports candidate movement, queue management, signage guidance, document flow, housekeeping coordination and general venue support under the Venue In-charge.	Employees/Contractual employees	Minimum 1 per 100 candidates
9	Electrician	Responsible for electrical readiness, power backup coordination, UPS and DG support and immediate rectification of electrical issues.	Employees/Contractual employees	1 per venue

S. No.	Position	Roles and responsibilities	Terms of engagement	Count
10	Security Guards	Responsible for gate control, queue management, prevention of unauthorised access, crowd control and support to frisking and venue security protocols.	Only from registered professional security agencies.	Minimum 1 per 100 candidates
11	Frisking Staff	Conduct gender-appropriate frisking, operate HHMD/body-check procedures, ensure prohibited items are not carried inside and coordinate with security staff.	Only from registered professional security agencies.	Minimum 1 male staff per 50 male candidates and 1 female staff per 50 female candidates; at least one male and one female per venue

7. Invigilators shall be at least Graduates and above 21 years of age. The security agency/personnel deployed must be duly, trained and professional. Above staff should be increased proportionately based on candidates allotted to a venue.
8. All deployed personnel must report at least 2.5 hours prior to commencement of the examination, be in professional attire (uniform dress code), and carry valid photo IDs. The Service Provider shall be solely responsible for all clearances, licences and compliance with labour laws and statutory obligations for its personnel and all the functionaries. In addition to the photo ID, all deployed personnel shall wear role-wise colour-coded identification (lanyards or badges) as per a colour scheme finalised with IIBF in the SOPs (e.g., distinct colours for invigilators, IT personnel, security/frisking staff and registration operators), so that each functionary's role is visually identifiable at a distance inside the venue. The Service Provider shall be responsible for maintaining dress code by the personnel deployed at the venues.
9. All the staff engaged in any capacity should be given proper training regarding the “Do’s and Don’ts” of the examination. Service Provider shall certify that training has been given to all exam functionaries and security personnel before the exam day.
10. The Service provider should certify after every examination that they have deployed adequate staff/personnel for the examination as per the above-mentioned Point no. 6
11. An Exam Functionaries Register shall be maintained at every venue on the mock day and the exam day, in which every person deployed in any capacity, including the Service Provider's staff, invigilators, IT personnel, security and frisking staff, jammer operators if required in future, biometric/registration operators, housekeeping, and observers or monitoring personnel of IIBF (if any) shall be entered with name, role, employer, ID particulars and in/out times. Biometric/Aadhaar-based (applicable as and when mandated by IIBF in future) registration of all exam functionaries at the venue shall be completed before candidate entry commences for each session, and the register (distinct from the visitor register under Clause A.9(9)) shall be submitted to IIBF with the post-exam documentation.

12. The IT Manager and any person handling the venue server, question-paper decryption or response data shall be an employee on the rolls of the Service Provider, and shall in no case be the venue owner, the venue's own staff, or personnel arranged locally by the venue. The venue owner, landlord, their employees and any local IT personnel of the venue shall not enter the server room or examination labs at any time between venue sealing and completion of post-exam sanitisation; any such entry shall be treated as an unauthorised-access incident reportable under Proforma 18.
13. All exam functionaries (other than the Venue In-charge, and the IT Manager to the extent of one designated venue communication device) shall deposit their mobile phones, smart watches and personal electronic devices at a supervised deposit facility before entering the operational area, prior to commencement of candidate entry, and shall retrieve them only after the close of their duty; the deposit shall be recorded in the functionaries register, no functionary shall use a personal mobile phone inside any examination lab or server room at any time, and the permitted devices of the Venue In-charge and IT Manager shall be listed in Proforma 3 and used only outside the candidate seating area. Violation shall be treated as a security incident reportable to IIBF.

A.9 Mock Day / Preparedness Drill

1. The Service Provider shall complete pre-examination activities / preparedness drill / mock run at all venues at least one day prior to the start of the IIBF examination. All exam functionaries participating in the conduct of the examination shall be present full-time during the mock run, and their training/briefing shall be conducted on the same day.
2. The mock run shall start preferably at 1100 hours and not later than 1500 hours on the date preceding the examination.
3. The venue shall not host any other examination on the day of the IIBF exam or mock run.
4. All computer nodes scheduled for the examination, including buffer nodes, shall be used in the mock run (100% load, not sample nodes). The mock exam shall be run for the actual duration of the exam with the actual question-paper size to be used on the exam day. One full-load mock run (dry run) is mandatory prior to the start of the examination as per the mutually agreed schedule.
5. The venue shall be taken into the Service Provider's possession at least one day in advance. The mock run shall be performed in a synthetic scenario with 100% load, and this activity shall be made available for online CCTV monitoring as and when required by IIBF. All nodes (including buffer) must be thoroughly checked and sanitised, and it shall be ensured that there are no blind spots in CCTV coverage. IIBF or IIBF designated auditors may conduct infrastructure review of examination venues as and when required. The sanitisation and inspection shall extend to all rooms, cabins and enclosed spaces adjacent to or on the same floor as the examination labs and server room; rooms not required for the examination shall be inspected for electronic devices, locked and sealed until the end of the last session, and the sealing recorded in the mock certification. Checklist and certification for completion of all these activities shall be provided to IIBF before examination.
6. During the mock, the following five activities shall mandatorily be carried out and certified:
 - (a) Network sanitisation;
 - (b) Node sanitisation;
 - (c) LAN scaping;

- (d) Bandwidth monitoring; and
- (e) Load monitoring.

7. After conduct of the mock run, the venue/lab shall be sealed and the keys kept in the custody of the authorised representative of the Service Provider; the sealed lab shall not be used for any activity until the examination day. The Service Provider shall submit certification of the nodes eligible for the examination and of sealing of the venue after a successful mock run, and shall certify that suitable training has been imparted to all exam functionaries and security personnel on their roles and responsibilities before the exam day.
8. The Service Provider shall be responsible for installing signal jammers (if required and mandated in future) during the exam day as well as the mock day to maintain the integrity of the examinations. If jammers are required to be installed in future, only wired CCTV cameras shall be used, since jammers will be operational during the exam period.
9. Every person entering the exam venue on the mock day and the actual exam day shall be recorded in a visitor register, a copy of which shall be sent by the Service Provider to IIBF along with other documentation. All entry and exit gates of the venue shall be covered by guards.

A.10 CCTV Surveillance

1. CCTV surveillance must be made functionally available in all examination venues. Minimum one wired IP-based CCTV camera of 2-megapixel or higher resolution per 12 candidates in each examination room, and shall cover every candidate desirably from 3 angles (minimum 2 angles). There shall not be any blind spots in the CCTV coverage. The sound recording feature to CCTVs to be installed within 1 year from the date of award of Contract.
2. Apart from examination rooms, CCTV surveillance should provide full coverage (no blind spots) of all common areas, frisking areas, registration desks, (activity at Registration desk shall be covered by CCTV Camera to show the clear frontal face of the candidate as well as the registration activity/ Manager), server rooms, corridors/passages, entry/exit gates, drinking water facility and other convenience facilities, UPS and DG Room, room of the venue manager/ other functionaries (if any), front, back, side area of the Examination venue and nearby areas such as parking, driveway and centre compound, and any points specifically indicated by the IIBF for comprehensive surveillance coverage of the Examination venue.
3. CCTV surveillance shall cover the complete movement of candidates from their entry into the examination venue till their exit from venue.
4. CCTV coverage has to be clear for monitoring/ post examination verification. The picture/video quality shall be clear enough under zooming also.
5. CCTV camera must capture examination venue activities starting from opening of the venue of examination to closing after the completion of examination.
6. The Service Provider shall ensure that live CCTV feed is time synchronized across all cameras. All venues (as per the requirement of IIBF) shall have the provision for live streaming of all CCTV cameras' feed to IIBF central command centre during conduct of examination. Uninterrupted live streaming (with centre code, venue name, room number, date and time overlay) and recording of all venues to the IIBF Command/Monitoring Centre (as required), through a media streaming server

enabling multiple simultaneous viewers, with sufficient internet bandwidth and power backup at each venue.

7. One computer screen with one CCTV operator at every venue for the Venue Head/Venue In-charge, and sufficient screens/manpower at the IIBF monitoring facility, at no extra cost.
8. The CCTV monitoring room shall be a dedicated room separate from exam labs and server room.
9. The Service Provider shall ensure that the watermark label of CCTV camera (appearing on live stream) shall match with the location or nomenclature of the room/ lab. CCTV timing shall match with screen time.
10. The surveillance video shall be recorded to a system other than the 'Examination Servers' at the Examination Venue.
11. Recorded footage shall be submitted to IIBF on external hard drives with clear, structured labelling, mapped per candidate room, within one week of completion of exam along with a certificate that recording is complete without any tampering; the Service provider shall retain a copy for the contract period as directed by IIBF, with one copy on secure cloud storage. The database and application servers shall be maintained at two different seismic zones in India (cloud DC and DR).

A.11 SOPs, Testing and Contingency

1. The Service Provider is expected to design the examination plan and examination process as required by IIBF. Broadly the requirements will be as follows.

Complete Security related management processes

- Physical Security
- Information Security
- Server Security
- Network Security

Candidate Handling processes

- Mapping of candidate details with exam venues.
 - Validation and verification of identity.
 - Attendance and biometric (photograph/ finger impression) handling/ authentication (AADHAAR based if required in future)
 - Candidates' seat allocation in a random manner.
 - AI/ML face matching of captured photo with registered photo.
2. The Service Provider shall provide SOPs and documentary manuals for all processes for safe and secure examinations, including rules for contingency, exception handling and emergency procedures, within 21 days of signing the Agreement; amendments incorporating previous feedback shall also be provided. SOPs shall be prepared in consultation with, and with the approval of IIBF.
 3. The Service Provider shall have a contingency plan for candidate management/ shifting in case of any emergency. No candidates shall be allowed to appear at exam venue(s) without pre-scheduling. Any re-mapping shall be allowed only if directed by IIBF.

4. The Service provider shall have an in-house quality assurance and product testing team with a robust, documented quality management process to test and certify the exam system, maintaining documented test cases and evidence of execution for all test cases, with rigorous testing of major, minor and patch releases. Testing shall cover functionality, performance, security, usability, high availability, business continuity and disaster recovery.
5. The CBT software shall meet the cyber-security audit requirements specified by MeitY, Government of India i.e., audited and certified by a CERT-In empanelled agency and such certificates shall remain valid throughout the Contract term; renewal shall be the sole responsibility of the Service provider without recourse to IIBF. Service providers shall also facilitate checks by I4C/CERT-In to prevent tampering with server operating systems.
6. Suitable emergency-management plans for crisis situations, redundancy of additional venue locations, candidate data, etc., shall be maintained and clearly described in the Technical Proposal (Annexure T5).

A.12 Safety, Emergency Preparedness and Disaster Management at Examination Sites

1. Fire safety: Every venue shall have adequate life-safety measures, including valid fire-safety compliance for the premises, adequate and serviceable fire-fighting equipment (fire extinguishers on every floor/lab, checked and tagged), unobstructed and clearly marked emergency exits and staircases, illuminated exit signage, and prohibition of inflammable material storage in or near examination labs. Electrical wiring, DG sets and UPS installations shall be safely installed and periodically inspected to prevent short-circuit/fire hazards.
2. Emergency evacuation plan: The Service Provider shall prepare a venue-specific emergency evacuation plan (covering fire, earthquake, flood, structural incident, medical emergency and any other crisis), display evacuation routes prominently in each lab and common area, designate assembly points, and brief all exam functionaries and security personnel on the plan during the mock-day training. Evacuation-readiness shall form part of the pre-exam venue audit.
3. First aid and medical preparedness: First-aid kits shall be available at every venue, with staff trained in basic first aid; contact details of the nearest hospital, ambulance, fire brigade and police station shall be displayed at the venue and held by the Venue In-charge.
4. Natural disaster / crisis contingency: In the event of a natural disaster (earthquake, flood, cyclone, etc.), fire or any other emergency at or affecting an examination site before or during the examination the safety of candidates and staff shall take absolute precedence. The Service Provider shall immediately and safely evacuate the premises where warranted, secure the examination systems and data (ensuring no loss of already-recorded responses and logs by virtue of real-time server synchronisation), inform IIBF and local authorities without delay, and submit a detailed incident report within 24 hours.
5. Alternate arrangements: The Service Provider shall maintain contingency plans for candidate management and shifting in emergencies, including redundant/alternate venue locations, and, where a venue becomes unusable due to such an event, shall in consultation with IIBF arrange alternate venues, inform candidates, arrange suitable transport and refreshments where candidates are relocated, and support re-scheduling/re-conduct of the affected session. Where the event constitutes a Force Majeure Event under Clause 8.13, penalties for the disruption itself shall not apply, but the safety, evacuation,

reporting, data-preservation and re-conduct-support obligations of this clause shall continue to apply in full.

6. The candidate seating plan shall not exceed the safe occupancy of the premises, and access for emergency services (approach for fire tenders/ambulances) shall be kept unobstructed on mock and exam days.

A.13 Support

1. The Service provider shall provide a helpdesk/toll-free support facility for candidates and the Institute.
2. Access to CCTV feeds: The Service provider shall share access to CCTV cameras deployed at examination venues (specifically requested by IIBF) via login id and also through RTSP/HLS links to IIBF and to any third party as designated by IIBF for live CCTV for monitoring and surveillance purposes, in addition to live streaming to the Service provider's Monitoring Centre and the Institute's command centre.
3. The Service provider shall support all audits, inspections and monitoring activities as described in Clauses 3.4, 3.5 and Annexure T8.

A.14 Escalation matrix:

- Level 1 - Venue In-charge/IT Manager (immediate);
- Level 2 - City Head and Command Centre (within 5 minutes);
- Level 3 - SP's Programme Director and IIBF SPOC (within 10 minutes for Severity-1);
- Level 4 - Exam In-charge (IIBF) contact for exam-threatening incidents (immediate).

Every Severity-1 incident shall be intimated to IIBF in real time by telephone and in writing (e-mail) within 15 minutes, followed by the Proforma-18 incident report within 24 hours.

B. During Examination

B.1 Entry, Physical Security and Frisking

1. At the entry gate, the candidate's admit card shall be checked for identity verification against an original photo-bearing ID produced by the candidate. Only candidates, authorised functionaries and inspecting officials with verified credentials shall be permitted entry.
2. Two-level frisking (separately for male and female candidates) from head to toe shall be ensured: one level of frisking with body tapping and the next level with hand-held metal detector (HHMD) devices. Frisking of female candidates shall be conducted exclusively by female staff in a three-side covered enclosure.
3. Gate control shall log every exit of a candidate or any other person from the venue during the examination window; a candidate will not be allowed to leave the venue before the mandated minimum time of submission. Any exceptional event shall be flagged in real time on the monitoring dashboard, reported to IIBF in the exam-day report, and the candidate's response/click-log data preserved and flagged for post-exam anomaly review under Clause C.
4. During security check it has to be ensured that candidate is not carrying any disallowed items and has not written anything on the identity/admit card documents before allowing entry.

B.2 Biometric Authentication of Candidates

1. The Service Provider shall scan the QR code on the admit card to retrieve the candidate's roll number and verified details (name, date of birth, father's name, centre, venue and photograph, subject etc).
2. The solution shall encompass multi-modal biometrics, fingerprint, and face biometric, and shall capture fingerprint and photograph of each candidate and scribes appearing with PwD candidates at both entry and exit. The photograph captured shall be matched with the photograph on the admit card/registration database using AI/ML, and mismatch cases shall be shared with IIBF in real time.
 - (a) Where a candidate's fingerprint capture fails after the permitted retries, the system shall automatically escalate to AI/ML face-match verification. If the face match result fails then the candidate can proceed only with prior approval of IIBF. All such discrepancies shall be reported to IIBF immediately for further steps.
 - (b) Every fallback event, its reason, the modality finally used, and the override (if any) shall be system-logged and included in the biometric mismatch report to IIBF under sub-point (3).
3. Biometrics and frisking of candidates and scribes appearing with PwD candidates shall be taken at entry of the lab, and after each bio-break, with a mismatch report of biometrics taken at all stages provided to IIBF. Bio-break frisking and biometrics shall be uploaded to the Service Provider's Master Control Facility for live monitoring.
4. Candidate images shall be captured in proper lighting, correct camera angle and white background; the solution shall not accept poor/blurred, partial-face or multi-face images, and shall include liveness detection. The solution shall be capable of Aadhaar-based biometric authentication (if applicable, as and when mandated by IIBF in future) and the Service provider shall be responsible for obtaining the UIDAI audit and all other compliances relating to Aadhaar-based authentication (if applicable, as and when mandated by IIBF in future).

5. Registration data (including registration timestamps) shall be pushed seamlessly to the local server enabling automatic node allocation.
6. One registration desk shall be provided per 30 scheduled candidates (plus a buffer registration machine), preferably placed at the entry of the examination lab; registration desks shall be used dedicatedly for candidate registration and shall not be used as candidate terminals. Registration logs shall be maintained and provided to IIBF.

B.3 Conduct, Monitoring and Logging

1. Candidates shall be oriented on the do's & don't's on exam pattern, timing and guidelines for answering the question paper and consequences of violation of examination rules and involvement in any kind of malpractices; atleast 5-10 mins before start of the exam; login with secure credentials shall open 10 minutes before the start for reading instructions.
2. The Service Provider shall provide one rough Sheet (s) and one see through pen per candidate (only if required and mandated) for that particular subject/exam by IIBF.
3. While the exam is conducted on the local LAN, test-progress data shall be transferred from the local server to the central server on real time basis (or as specified by IIBF) for monitoring, with real-time reports to IIBF's dashboard covering all venues.
4. Primary and backup venue servers must connect to the Service Provider's central server only through a secure VPN, with at least 256-bit SSL encryption.
5. During the exam, this connection can be used only for:
 - (a) encrypted progress updates from the venue server to the central server;
 - (b) server "heartbeat" monitoring, i.e., checking whether the venue server is alive/working;
 - (c) communications specifically directed/approved by IIBF.
6. All other internet traffic must be blocked during the exam session. This means no other inbound/outbound traffic, ports, applications or services should work on the exam-server connection while the exam is live.
7. The blocked/lockdown status should be lifted only after the exam session, specifically for uploading candidate response data as per Clause C.
8. The Service Provider must maintain logs showing:
 - (a) when the lockdown started and ended
 - (b) what was allowed during the lockdown;
 - (c) the whitelist of approved traffic/services;
 - (d) related time stamps.
9. These logs will become part of the Mandatory Data Set under Clause 3.4 & 3.5, meaning IIBF can audit/check them later.
10. The separate second internet connection used for CCTV streaming will not be affected. It should continue working independently.

11. A comprehensive, click-by-click activity log of every candidate (with timestamps) shall be maintained for full auditability, along with detailed de-mapping/re-mapping reports. Attendance shall be captured through photographs, biometric, physical attendance sheets (non-staining inkpads) at each candidate's desk, compared against the allotted random seat, with discrepancies reported to IIBF immediately.
12. During the examination, no person shall occupy any sealed or non-designated room within the venue; the Venue In-charge shall conduct at least one recorded verification round per session covering sealed rooms, corridors and washrooms, any unauthorized person including centre owner/ centre IT person present at the centre, any room other than exam lab opened during exam, any broken seal, unauthorised occupation or suspicious material found shall be reported immediately to IIBF and recorded in the incident report (Proforma 18).
13. No hardware component (monitor, CPU, keyboard, mouse, cables or peripherals) of any certified node shall be replaced or altered after node certification and venue sealing. Where a replacement becomes unavoidable due to failure, it shall be performed only by the rostered IT Manager post approval from IIBF, using a certified buffer component/node, logged with component identifiers, node ID, reason and timestamps, verified against the hardware inventory maintained under Annexure T1, and shall be reported in the incident report; and the candidate shall instead be re-mapped to a buffer node post approval from IIBF, under the existing procedure of Proforma 10 with start time being where it stopped.
14. Washrooms accessible to candidates shall be physically inspected for chits, written material and electronic devices before the start of each session and thereafter at regular intervals not exceeding 30 minutes during the session, by a designated functionary of the same gender as the users of that washroom; each inspection shall be initialled in the washroom/bio-break log (Proforma 11), and any material found shall be seized, photographed, reported to IIBF immediately and recorded in the incident report, with the concerned time-window's bio-break entries reviewed against candidate logs.
15. Use of pen drives, external hard disks, memory cards or any removable storage media is strictly prohibited inside the server room and examination labs from the sealing of the venue after the mock run until completion of the post-exam data upload and sanitisation, except where a specific, time-bound written authorisation is issued for a defined recovery/handover operation; every such authorised use shall be logged (device identifier, purpose, operator, timestamps), performed under CCTV coverage, and reported in the incident report (Proforma 18). USB ports on all servers shall remain disabled per Annexure T1 except during such authorised operations.
16. Invigilators shall actively supervise by moving around the labs, taking rounds, continuously throughout the exam and shall not converse with each other. Rought sheets are not allowed, candidates will be required to use the onscreen notepad. Rough sheets if any mandated by IIBF to be issued during any subject/exam, shall be collected and shredded post-exam by the Service Provider (stationery list at Annexure T9). Candidate feedback shall be collected at the end of the examination and a summary report submitted to IIBF.
17. Candidate exit verification shall be performed in an orderly manner before candidate leaving the exam lab. Also, admit card shall be checked to ensure that nothing is written on the same while exiting the exam venue.

B.4 PwD Candidates, Scribes and Special Requirements

(The Scribe guidelines on Institute website be also referred)

1. At least one venue in each city shall be fully accessible to differently-abled candidates (ramp/lift, accessible washrooms, ground-floor or lift-served labs). PwD candidates shall be provided seating on the ground floor or lift-accessible labs, and computers/software appropriate to their needs (screen magnification, larger fonts, and other approved assistive features).
2. Where IIBF approves a scribe, the Service Provider shall verify and register the scribe (identity, eligibility per IIBF norms, photograph and biometrics captured alongside the candidate), seat the candidate-scribe pair as directed, and log the arrangement; scribe biometric images shall form part of the Mandatory Data Set (Clause 3.4 & 3.5). No scribe shall be permitted entry without the scribe approval letter/email issued by IIBF through its notified online scribe application process. At registration, the scribe's details shall be verified against the scribe approval letter/email and against the scribe's original government-issued photo identity document, and the scribe shall additionally undergo biometric capture (fingerprint and face with liveness detection) as the candidate; any mismatch between the approval letter from IIBF, the identity document and the person presenting shall result in denial of entry of the scribe and immediate reporting to IIBF and the Venue In-charge.
3. Compensatory time for eligible PwD candidates shall be configured in the exam engine as per IIBF's instructions and logged; the timer-compensation mechanism of Clause A.4 shall apply equally to PwD sessions.
4. Seating and supervision: candidates with scribes shall be seated with at least a three-seat gap between successive scribe-assisted candidates and seated separately from other candidates ensuring that they are not disturbed; one invigilator shall be dedicated for every five scribe-assisted candidates (minimum one wherever any scribe is present), and an announcement identifying the presence and rules of scribe assistance shall be made in the lab before the start of the examination.
5. Conduct monitoring: dedicated invigilators shall specifically watch for, and immediately report, scribe-conduct malpractice, including the scribe answering independently or altering answers without the candidate's instruction, repeatedly reading out a preferred option, prompting or nudging the candidate by gesture or contact, or operating the mouse/keyboard to select an option of the scribe's own choice; all scribe-assisted candidates shall be seated within direct CCTV coverage, such footage shall be preserved and flagged for review, and confirmed scribe malpractice shall be treated as unfair means
6. Unfair means: The Service Provider shall take immediate steps against any candidate caught indulging in malpractice, including the filing of FIR(s) (wherever instructed by the Institute) against culprits caught indulging in malpractice during the conduct of examinations, which shall be done by the Service Provider, in coordination with and after intimation to IIBF.

C. Post-Examination

1. Candidate responses (raw data), biometrics, photographs and audit trails shall be transmitted from the venue server to the Service provider's central server/data centre immediately (should be automated) on the conclusion of each exam session/batch leaving no traces on the venue server. This complete data should be encrypted and shall be submitted to IIBF within 2-3 days from the end of the exam session/batch, in the format prescribed by IIBF.
2. The Service provider shall provide a system-generated provisional-scores link within 2-3 days of completion of each examination. The evaluation of candidates' scores and the processing and declaration of results shall be done internally by IIBF; the Service provider's obligation is limited to providing complete, accurate and reconciled response data, logs, analysis, statistics and reports in the formats required by the Institute for such internal processing. However, the service provider shall be responsible for providing provisional scores to the candidates.
3. The Service Provider shall share the network logs and give a report of any intrusion or remote access detected.
4. All examination-related data and documents such as biometrics, photographs captured, attendance sheets, functionary attendance, firewall, audit logs, lab-wise seat-wise mapping, de-mapping certificates, face-comparison reports, exam-day and bio-break images, filled proformas, annexures, any declarations taken from candidates, rough sheets, and other documents specified by IIBF shall be scanned immediately at the venue and provided within 2-3 days from the date of completion of exam. All these documents are to be arranged batchwise before dispatch.
5. The Service Provider shall upload the segregated scanned documents viz. attendance sheets, declarations for mismatch cases, declarations from scribes, seat change (mapping/ demapping forms), etc. with proper nomenclature, venue and date shift wise.
6. CCTV recordings shall be submitted on hard disk drives, appropriately mapped per candidate/room, no later than a week from the date of request.
7. UFM/forensic analysis reports (physical verification, CCTV footage, clipped footage, biometric and face comparison) shall be submitted to IIBF within a week of the exam completion.
8. The Service Provider to maintain daily tracker to monitor availability of CCTV recordings of each exam venue.
9. Signed "read only" copies (non-editable soft copies) of all documents pertaining to results of all stages of the CBT shall be provided by the Service Provider before declaration of the result of that stage.
10. The Service provider shall provide post-examination analytics reports including: student performance analysis, fast/rapid answering report, time bucket report, item analysis of MCQ responses (difficulty index, discrimination index, etc.) and psychometric analysis of question papers flagging technically doubtful items, as data inputs for the Institute's internal evaluation; audit-log analysis (click by click logs, time logs, MAC/IP addresses); and reports on proxy candidates, unfair means and forensic anomalies (peeping, cheating, impersonation, response-pattern anomalies). Any UFM case shall be treated as per the rules & regulations of the Institute.
11. Service Provider to handover the list of suspected candidates identified through post exam analysis or candidates caught with unfair means. Service Provider to support IIBF team to evaluate the highlighted cases. Service Provider shall take immediate steps against culprit caught indulging in malpractice with

filing of FIR etc. Filing of FIR(s) against the culprits caught indulging in malpractices during and post the conduct of examinations will be done by the Service provider:-

12. The Service provider shall archive results and other examination data for the period of the contract as custodian from declaration of results, preserve server/firewall log files for the period of the contract, keep results and information accessible online for the period of the contract (or as specified by IIBF), provide documented support for candidate police/court queries in case of UFM, and provide candidate data as required authorities.
13. Test Data Archiving: The Service Provider shall archive the result and other examination data and retain the same for the period mentioned in point no. 12, until transfer of entire data to IIBF as per exit policy. After handing over data to IIBF, all examination related data will be deleted from the Service Provider's data center. Certificate to that effect to be provided by Service Provider. No data will be deleted without the approval of IIBF.
14. Any data desired by IIBF shall be shared with IIBF without any manipulation/ tampering.
15. All data that is generated/ captured/ logged/ stored shall be the property of IIBF.
16. MIS generation/ customized reports: The Service Provider shall provide adequate information as per the requirement of IIBF.
17. The Service Provider shall update its processes and technology to incorporate learnings from malpractices/UFM/legal cases, ensuring measures are in place to prevent recurrence, and shall maintain a database of all malpractices/UFM/legal cases during the Contract period, which shall be fully handed over to IIBF at the end of the Contract.
18. A daily exam-day report (incidents, SLA counters, biometric statistics, any candidate declarations taken, UFM cases) shall be submitted to IIBF by end of the day or maximum by next day on conclusion of each examination. Venue-wise attendance report shall be submitted to IIBF immediately after completion of each exam session and the total attendance (consolidated for all session on that particular day) immediately after final session.
19. All the above data or any other data as required by IIBF shall be shared through a secured channel only.

3.2 Roles and Responsibilities Matrix

The division of responsibilities between IIBF and the Service Provider is summarised below. Where an activity is marked joint, the Service Provider shall act only with the prior concurrence of IIBF.

Activity	IIBF	Service Provider
Pre-examination		
Candidate enrolment/registration, issue of login credentials and admit letters	Responsible	Consumes data; QR-based verification at venue
Preparation of question bank/question papers and marking scheme	Solely responsible	No role

Activity	IIBF	Service Provider
Secure upload of QB at IIBF premises (standalone server)	Executes upload	Provides server, application and on-site support, deployment, maintenance, security and lifecycle management of Test Engine
Encryption, distribution and rendering of QPs to venues	Approves and monitors	Responsible (encrypted, no manual intervention)
Venue identification, audit-readiness, infrastructure, manpower	Reviews; may audit	Responsible for compliance as per the requirements
Venue owner verification, antecedent checks and maintenance of debarred venue database	Reviews and may seek records	Responsible for verification, maintenance of records and submission to IIBF
Submission of venue agreements, MOU/NOC and venue readiness confirmations	Reviews and may seek records	Responsible
Venue audit and audit report submission for examination centres	Reviews and may seek records	Responsible for audit, conducting and submitting audit reports
Development of additional examination venues in deficient cities	Reviews and may seek records	Responsible for Identification
Full-load mock run, preparedness drill and venue sealing	Independently oversee CCTV or may seek records.	Responsible
Submission of mock run reports, logs and certifications	Receives and reviews	Responsible
Police verification, background verification and Biometric/Aadhaar authentication (applicable as and when mandated by IIBF in future) of examination functionaries	Reviews and receive reports	Responsible
Functionary manpower deployment as per prescribed norms	Reviews and receive reports	Responsible
Training and certification of all examination functionaries	Reviews and receive reports	Responsible
Uniform dress code and role-based identification of examination functionaries	Reviews and receive reports	Responsible

Activity	IIBF	Service Provider
Installation and operation of signal jammers (if mandated by IIBF at anytime in future)	Directs and approves	Responsible to obtain all required approvals and installation of jammers
Deployment and maintenance of Test Engine at IIBF premises	Reviews and approves	Responsible
API integration between IIBF Authoring Tool and CBT Test Engine	Provides authoring system	Responsible
QB/QP lifecycle management including mapping, cloning, validation and deletion	Executes upload and approval	Responsible
During examination		
Frisking, biometric registration/authentication, facial matching, random seat allocation, entry-exit verification and verification of documents at registration desk	Reviews and receive reports	Responsible and share reports with IIBF
Conduct of examination, invigilation, incident management	Command-centre oversee	Responsible
CCTV surveillance, live feed, recording, submission, archival, retention and retrieval obligations	Reviews and receives footage	Responsible
Capture, real-time synchronization, secure transmission of responses, biometrics, photographs, logs and audit trails	Reviews and receive reports	Responsible
Face-match verification using AI/ML and reporting of mismatches	Reviews, receive reports and approves exceptions	Responsible
Candidate registration, biometric capture, exit verification, bio-break verification and exception logs	Monitors and reviews reports	Responsible
Transfer of candidate response data from local/venue server to service provider central server on conclusion of each session/batch	Monitors through dashboard	Responsible
Real-time attendance reporting after each examination session	Reviews and receive reports	Responsible
Daily examination status report and incident reporting	Reviews and issues directions	Responsible

Activity	IIBF	Service Provider
Network intrusion detection, prevention, LAN sanitization, intrusion logs and cyber-forensics reporting	Reviews security reports	Responsible and to submit detailed report on how it was prevented
Command center / Dashboard infrastructure at IIBF HQ (if implemented)	Provides space and oversee	Responsible for infrastructure, setup, operation and maintenance
Command Centre dashboard reporting and live monitoring support	Reviews and monitors	Responsible
Face-match/mismatch reporting and exception management	Reviews and approves exceptions	Responsible
Post examination		
Evaluation of candidates' scores, result processing and declaration	Solely responsible (internal) for processing and declaration of final results	Provides complete data, reports and analytics inputs. Responsible to evaluate and provide provisional scores link on IIBF website
Generation and publication of provisional scores to candidates	Reviews outputs	Responsible
Question or Answer-key challenge management	Decides on challenges	Report to IIBF and perform root cause analysis. Provide details to IIBF.
UFM detection, evidence compilation and FIR filing	Directs; adjudicates UFM	Detects, reports, compiles evidence, files FIR wherever required
Submission of biometric reconciliation reports (matched/unmatched)	Reviews and receive reports	Responsible
Submission of scanned attendance sheets, declarations and examination documents	Reviews and receive reports	Responsible
Submission of Mandatory Data Set and audit data under Clause 3.4 & 3.5	Reviews and receive reports	Responsible
Support for Court Matters, Police Investigations and UFM cases	Reviews and receive reports	Responsible for data, reports, support and assistance required in relation to court matters,

Activity	IIBF	Service Provider
		police investigation and UFM cases.
Post-exam data handover, sanitisation, archival	Receives and certifies	Responsible
Maintenance, archival and retrieval of examination data, logs and CCTV records	Reviews and may audit	Responsible
QB data deletion and certification after completion/exit obligations	Reviews	Responsible and submit the report.
SLA reporting and governance	Reviews and receive reports	Measures, reports, remediates (RCA/CAPA)
Performance review observations, RCA, CAPA and implementation of corrective measures	Reviews and receive reports	Responsible
Management of re-examination arising due to Service Provider failure	Approves re-conduct schedule	Responsible for complete execution at own cost
OTP-based seat/node reassignment controls	Approves exceptions	Responsible
Test Engine data deletion certification and exit compliance	Reviews	Responsible

3.3 Governance Model – Independent Examination Monitoring

The Institute reserves the right to appoint an independent Examination Monitoring Agency or Unit (EMA) to oversee pre-examination, during examination and post-examination activities. The Service Provider shall provide unrestricted access to venues, systems, access to live CCTV feeds and recordings, logs, dashboards and reports to such monitoring agency, as required, without any additional cost to the Institute. Non-cooperation with the EMA shall constitute material breach and shall attract consequences under Sections 8 and 9.

3.4 Data Requirements for Audit / Analysis by Institute or agency authorised by Institute

IIBF may authorise and deploy an independent agency for audit of pre-, during- and post-exam activities. The Service provider shall provide all data including logs, trails, CCTV footage, documents and clarifications to IIBF without undue delay, as per the Institute's requirements, and shall promptly extend all required help in monitoring and resolving issues in consultation with IIBF. The Service provider 's responsibilities include:

1. Providing a detailed understanding of the technical architecture, exam-conduct processes, data flow and data dictionary before the start of the exam.
2. Providing timely details of Venue Heads/Centre Coordinators (contact numbers, authorisations), and timely access to exam-centre premises for pre-exam audit.

3. Mitigating, before exam start, the critical observations identified during pre-exam centre audit, to the satisfaction of IIBF; observations relating to pre-, during- or post-exam phases shall likewise be mitigated to IIBF's satisfaction.
4. Providing access to IIBF/IIBF authorised auditors during the exam at exam centres as independent observers, and facilitating download of application logs and system settings from sample machines and network switches identified by the auditors after the exam.
5. Capturing electronically, all the data listed below. Where any data is not readily available, all efforts shall be made to collect and share it; data that the Service Provider fails to provide shall attract the liability and penalty consequences set out in Clauses 8.6 and Section 9. All data shall be made available to IIBF in a secure manner, and processing of such data shall be performed by IIBF at its premises.

3.5 Dataset to be provided by the Service provider for analysis (the "Mandatory Data Set"):

Pre-exam

1. Configuration of servers and nodes (OS, RAM, MAC, IP, screen resolution, printer settings, sleep-mode settings, antivirus policy, services running, applications and hardware installed, etc.).
2. Details of exam venues and total capacity in seats and nodes; report of health check/IT audit of machines and physical-infrastructure audit of venues; list of whitelisted websites and applications on primary server, backup server and candidate nodes and LAN scape report.
3. Mock-exam-day logs

Post exam

4. Raw dump of click-by-click activity log of each candidate during the exam with timestamps (exam start, questions explored, options selected, responses submitted, break/resume times, section/question navigation, exam end time, seat numbers before and after seat change, incidents such as account lock etc.).
5. Raw dump of click-by-click activity log of the IT Manager/personnel on the venue servers (primary and backup) with timestamps (exam setup, QP download time, conduct, attendance marking, end-of-exam, data upload to central server, deletion of exam data, other user activities, application/service logs, OS event logs, remote logins, etc.).
6. Dump of services and applications running on the attendance/registration systems and the IT Manager's computer.
7. Raw incident-log dump of the exam application on each delivery node (hardware, network and software events).
8. Seating plan of candidates (venue, room number, seat number, node IP, node MAC, candidate present/absent status, and equivalent details for any change of node).
9. Candidate raw response data and system-recorded provisional scores of candidates (final evaluation of scores being IIBF's responsibility), and candidate feedback report.
10. Log of system/power issues and all technical/non-technical incidents during the exam, including historical incidents, and logs of any issues with firewalls or exam software.

11. Biometric registration data and logs (candidate details, timestamps, MAC address of registration desk, details and reason of any bypass venue details); along with face match report biometric images of candidates and scribes captured at the venue along with the face-match report.
12. Biometric registration logs of all the manpower deployed at the centres.
13. List of PwD candidates who actually appeared with scribes at the centres.
14. Log of exam data received at the central server with timestamps; network log of connections made to the venue servers from the central server or head office.
15. Incident report, CCTV footage of exam centres as and when requested
16. Any other data required by IIBF in connection with the particular exam.
17. All data shall be provided in the format specified in Annexure T11

3.6 Expected Volumes, Tenure and Single Point of Contact

1. Expected volumes: approximately 12 lakh subject-wise candidate tests per year across 254-plus cities, with peak single-day loads of up to 1,00,000 candidates across a maximum of 3 sessions. These volumes are indicative and create no minimum-business commitment on IIBF. IIBF reserves the right to conduct the examination in one or more sessions but not exceeding three sessions, as may be decided by IIBF based on operational and administrative requirements, and the Service Provider shall make necessary arrangements accordingly.
2. Tenure: The contract shall be awarded for an initial period of five (5) years. The performance of the selected Service Provider shall be reviewed by the Institute annually. Further, upon completion of the initial five-year term, the Institute reserves the right, at its sole discretion, to extend the contract for an additional period of up to two (2) years, either on the same terms and conditions or with such modifications as may be considered necessary by the Institute at the relevant time. However, any such modification in the commercial terms during the extended period shall not exceed twenty percent (20%) of the rates/charges agreed under the original contract, unless mutually agreed otherwise in writing.
3. The Service Provider shall designate a Single Point of Contact (SPOC) of appropriate seniority, with defined escalation matrix, for all engagement with IIBF.
4. Detailed technical and functional requirements are set out in Annexure T1; compliance thereto shall be confirmed item-by-item in the Technical Bid.

3.7 Performance Evaluation

IIBF shall undertake performance evaluation of the Service Provider after every examination cycle. All observations, deficiencies, deviations, incidents, service gaps, audit findings and other issues identified during the conduct of the examination shall be discussed with the Service Provider through a structured review mechanism. Based on such review, the Service Provider shall submit appropriate mitigation measures, corrective and preventive action plans, timelines and implementation responsibilities for the next examination cycle. The Service Provider shall be responsible for implementing such mitigation measures to the satisfaction of IIBF and ensuring that the identified observations do not recur in subsequent examination cycles.

SECTION 4 – ELIGIBILITY CRITERIA

Bids of only those Service providers who satisfy all of the following eligibility criteria (to be confirmed in the Eligibility Criteria Matrix at Annexure E5 with supporting documents) will be considered for technical evaluation:

Sr.	Eligibility Criterion	Supporting Documents
1	The Service provider shall be a company registered in India under the Companies Act, 1956/2013 (including PSUs), in existence for at least 5 years as on the date of bid submission. Consortium/joint-venture bids, proprietorships and partnership firms are not allowed.	Certificate of Incorporation, MoA/AoA, GST registration, PAN
2	The Service provider must hold valid SEI CMMI Level 3 and above certification for Software Services/Development (verifiable at cmmiinstitute.com/pars) and ISO 9001, ISO/IEC 27001 certifications; ISO/IEC 20000-1 preferred. Certifications must be retained during the currency of the Contract.	Copies of valid certificates
3	The Service provider must own the complete source code, copyrights and all components of the CBT software used.	Self-declaration by authorised signatory
4	The Service provider's examination software must be certified "Safe to Host" by a CERT-In empanelled agency (certificate not older than 12 months).	Copy of valid certificate
5	The Service provider should have successfully conducted CBTs in a single day, in a single session, on an all-India basis in 100 or more cities covering at least 20 States/UTs, during the preceding 3 calendar years.	Work orders and performance certificates from clients (Annexure T2/T4)
6	The Service provider must have successfully conducted a computer-based examination for at least 100,000 candidates in a single day, on a pan-India basis, at least once in the preceding 5 calendar years.	Work order and performance certificate
7	The Service provider should have an average annual turnover of at least ₹500 crore during the last 3 audited financial years, and positive net worth in each of those years.	Audited financials, CA certificate with UDIN (Annexure E3 / Financial Information, mentioning the turnover from CBT separately)
8	The Service provider should have a minimum of 450 staff on its rolls. The organization should have in-house 50 technical personnel to maintain software and data used to conduct the exam and should follow well defined Software Change Management processes to manage changes in the software	Certification by CEO/HR Head with EPFO evidence
9	The Service provider should not be blacklisted/debarred by any Central/State Government, PSU or autonomous body for exam-related activities, and neither the Service provider nor	Notarised undertaking on ₹100 non-judicial stamp paper (Annexure T3/E9)

Sr.	Eligibility Criterion	Supporting Documents
	its promoters/directors should be subject to any insolvency or bankruptcy proceedings before the NCLT or any other authority during the last 5 years.	
10	Conflict of Interest: The Service provider must not be engaged in coaching/training/education/certification business in banking and finance or in any activity that could influence the conduct of IIBF exams.	Self-declaration (Annexure E9)

The Institute's decision on eligibility shall be final and binding. Even where a Service provider meets the criteria above, it may be disqualified for misrepresentation or suppression of facts, a record of poor performance (abandoned work, incomplete contracts, financial weakness), adverse findings in confidential enquiry, or engagement in any activity that could influence the conduct of examinations.

SECTION 5 – INSTRUCTIONS TO SERVICE PROVIDERS

5.1 Bidding Documents, Clarifications and Amendments

1. "RFP", "Bid" and "Tender" are used interchangeably. The Service provider is expected to examine all instructions, forms, terms and conditions and technical specifications in this RFP; a non-responsive bid may be rejected without further notice.
2. Pre-bid queries shall be submitted in writing in the below format and within the timeline in Section 1. Responses to queries will be published on IIBF's website. Not more than 2 representatives per Service provider may attend the pre-bid meeting, with an authority letter/company ID.

Sr. No.	Document Reference	Page No.	Clause No.	Description in RFP	Clarification Sought	Remarks
---------	--------------------	----------	------------	--------------------	----------------------	---------

3. IIBF may amend the RFP at any time prior to the bid-submission deadline by addenda/corrigenda published on its website, which shall form an integral part of this RFP and be binding on all Service providers; the deadline may be extended at IIBF's discretion.

5.2 Earnest Money Deposit (EMD)

1. The Service provider shall submit an EMD of ₹25,00,000/- (Rupees Twenty-Five Lakh only) by Demand Draft/Pay Order or Bank Guarantee (formats at Annexures E1/E2) from a scheduled commercial bank in India, in favour of "Indian Institute of Banking & Finance", payable at Mumbai, valid for 6 months from the last date of submission. No interest shall be payable on the EMD. Bids without EMD shall be summarily rejected. MSEs/Startups registered as per Government of India policy may claim exemption with valid registration and a Bid-Securing Declaration.
2. EMDs of unsuccessful Service providers will be returned without interest upon finalisation of the successful Service provider. The successful Service provider's EMD will be returned after furnishing of the Performance Bank Guarantee and signing of the Contract.
3. The EMD shall be forfeited if the Service provider withdraws or modifies its bid during the validity period, fails to sign the Contract, fails to furnish the Performance Bank Guarantee, or is found to have engaged in any Prohibited Practice under Section 8.15.

5.3 Preparation and Submission of Bids (Two-Bid System)

1. Bids shall be submitted in two separately sealed envelopes, "Technical Bid" and "Commercial Bid", both placed in a single sealed outer envelope superscribed with the RFP reference and the Service provider's name, addressed to the Chief Executive Officer, IIBF, at the address in Section 1. Inclusion of any price information in the Technical Bid shall result in summary rejection of the bid.
2. The Technical Bid shall contain:
 - (a) Service Provider's Letter for EMD / Bid Security (Annexure E1);
 - (b) Bid Security (Bank Guarantee) Format (Annexure E2);

- (c) Service Provider's Information and Financial Details (Annexure E3);
 - (d) Declaration Regarding Application Software (Ownership of Source Code) (Annexure E4);
 - (e) Eligibility Criteria Matrix (Annexure E5);
 - (f) Declaration for Acceptance of RFP Terms and Conditions (Annexure E6);
 - (g) Declaration for Acceptance of Scope of Work (Annexure E7);
 - (h) Format of Power of Attorney / Board Resolution (Annexure E8);
 - (i) Other Undertakings (Clean Track, No Blacklisting, Conflict of Interest) (Annexure E9);
 - (j) Non-Disclosure Agreement (Annexure E10);
 - (k) Compliance to Technical & Functional Requirements (Annexure T1);
 - (l) Service provider's Experience (Annexure T2);
 - (m) Declaration Regarding Clean Track Record (Annexure T3);
 - (n) Client Details for Reference (Annexure T4);
 - (o) Project Plan (incl. Contingency, BCP/DR and Exit Plan) (Annexure T5);
 - (p) Short Description of the Proposed Solution (Annexure T6); and
 - (q) Exam Software Security Declaration (Annexure T7);
 - (r) Details of exam centers owned by Service Provider (Annexure F1)
3. The Commercial Bid shall contain only the price bid in the format at Annexure P1. Prices shall be quoted in Indian Rupees, exclusive of GST (taxes payable additionally at actuals), fixed for the Contract term, and written both in figures and words (words prevail in case of discrepancy). Quoting for all line items is mandatory.
4. Bids shall remain valid for a minimum of 180 days from the date of opening of the Technical Bids. Each page of the bid shall be signed by the authorised signatory. Conditional bids, joint bids and multiple bids by the same Service provider shall be rejected. Bids received after the deadline shall not be considered.

5.4 Language, Format, Signing and Deviations

1. The bid and all correspondence shall be in English. Bids shall be typewritten without overwriting, cutting or interpolation; corrections, if unavoidable, shall be initialled by the authorised signatory. All pages shall be serially numbered, indexed and signed with seal by the authorised signatory holding the Power of Attorney/Board Resolution (Annexure E8).
2. Bids shall be submitted strictly in the prescribed annexure formats. Incomplete information, unclear responses, alteration of prescribed formats, superfluous material, or deliberate suppression of information may result in disqualification. Where a query is not applicable, it shall be marked "Not Applicable".
3. No-deviation bids: This RFP does not contemplate deviations. Any deviation from the scope, SLA, penalty regime or terms and conditions shall render the bid liable to rejection as non-responsive. Assumptions material to the bid must be raised as pre-bid queries, not embedded in the bid.

5.5 Modification, Substitution and Withdrawal of Bids; Late Bids

1. A Service provider may modify, substitute or withdraw its bid by written notice received before the bid-submission deadline; modifications/substitutions shall be sealed and superscribed accordingly. No bid may be modified or withdrawn after the deadline and before expiry of the bid validity; such withdrawal/modification shall entail forfeiture of the EMD.

2. Bids received after the deadline (as per IIBF's receipt records) shall be rejected unopened and returned. IIBF shall not be responsible for postal/courier delays or mis-delivery.

5.6 Bid Opening, Preliminary Scrutiny and Clarifications

1. Technical Bids shall be opened at the date, time and place in Section 1 in the presence of Service providers' representatives who choose to attend (maximum two per Service provider, with authorisation letters). Names of Service providers and presence of EMD shall be read out; Commercial Bid envelopes shall remain sealed in IIBF's custody.
2. Preliminary scrutiny shall verify completeness, EMD, formats, signatures and eligibility compliance (Annexure E5). During evaluation, IIBF may, at its discretion, seek written clarification from any Service provider; the request and response shall be in writing, and no change in price or substance of the bid shall be sought, offered or permitted, except arithmetical-error correction in the Commercial Bid (unit rates in words prevailing).
3. IIBF may interact with, and independently verify, customer references submitted by Service providers, and may inspect the Service provider's facilities, data centre, monitoring centre and sample venues as part of evaluation process.

5.7 Contacting IIBF; Canvassing

From bid opening until award, no Service provider shall contact IIBF on any matter relating to its bid except in writing as provided herein. Any attempt to canvass, influence or pressure IIBF, its employees or evaluation committees directly or indirectly shall result in rejection of the bid and forfeiture of the EMD, without prejudice to action under the Integrity Pact (Annexure IP).

5.8 IIBF's Rights

IIBF reserves the right, without liability and without assigning reasons, to: accept or reject any or all bids in whole or in part; annul or cancel the RFP process at any stage and, if deemed fit, issue a fresh RFP; relax or waive any minor informality, non-conformity or irregularity that does not constitute a material deviation; extend any deadline; vary the quantum/volume of work.

SECTION 6 – EVALUATION PROCESS

6.1 Overall Methodology

The selection will follow a Quality-cum-Cost Based Selection (QCBS) with weightage of Technical Score 70% and Commercial Score 30%. Evaluation shall proceed in stages: (i) preliminary scrutiny of completeness, EMD and eligibility; (ii) technical evaluation, including mandatory demonstration of the exam platform (client and server software) using a live/synthetic examination and a presentation of capabilities; (iii) opening of Commercial Bids of only the technically qualified Service providers; and (iv) computation of the composite score. IIBF may seek clarifications and verify claims independently, including site visits and reference checks.

6.2 Technical Evaluation (100 marks)

Sr.	Criterion	Basis	Max Marks
1	Functional and technical features of the exam platform (compliance and demonstrated depth against Annexure T1)	Annexure T1 + demonstration	30
2	Exam software security, integrity and auditability: prevention/detection/logging of unauthorised devices and network intrusion; access controls; software-integrity checks; candidate-to-node mapping; time accuracy and compensation; encryption; data sanitisation; remote-access prevention; UFM detection (as per Annexure T7)	Annexure T7 + demonstration	20
3	Experience: years in CBT; largest single-shift candidate volume handled ($\geq 1,00,000$ candidates scores full marks); number of similar large-scale public-examination projects completed	Annexure T2/T4	15
4	Infrastructure capability: certified owned nodes across cities (city-wise vetted node list), Tier-III (or higher) primary data centre with DR at a different seismic zone, CERT-In certified application, monitoring command centre	Annexure T5/T6 + proofs	13
5	Service provider profile: IT staff strength; CMMI Level 3/5; ISO 9001 / 27001 / 20000-1; average annual turnover	Annexures E3/E5	12
6	Project plan, governance, SLA management approach, transition/exit plan, risk and contingency management, proposed innovations (AI-based proctoring analytics, fraud detection, etc.)	Annexure T5	10

6.2.1 Indicative Sub-Scoring Guidance

Within each criterion, the Technical Evaluation Committee shall apply the following indicative sub-scales; fractional scoring is permitted. The Committee's assessment shall be final.

Criterion	Sub-parameter	Indicative marks
Sr. 3 Experience (15)	Years in CBT: 3 to <5 years = 3; 5 to <8 years = 4; 8 years and above = 5	5
	Largest single-day candidate volume handled on pan-India basis: 1,00,000 to 1,24,999 = 1; 1,25,000 to 1,49,999 = 3; 1,50,000 and above = 5. Less than 1,00,000 shall not be evaluated as it does not meet eligibility.	5
	Similar completed large-scale public examination projects in preceding 5 calendar years: 1 project = 1; 2 projects = 3; 3 or more projects = 5. Projects must be supported by work order and performance certificate	5
Sr. 4 Infrastructure (13)	Certified owned nodes with city-wise vetted list: 50,000 to 74,999 nodes = 1; 75000 to 99999, nodes = 2; above 1,00,000 nodes = 3.	3
	No. of owned center out of the IIBF exam center list as per Annexure F1 175 to 199 = 1 200 to 224 = 2 More than 225 = 3	3
	Tier-III or higher primary data centre with DR at a different seismic zone: Compliant setup = 2; Compliant setup with documented RTO/RPO, periodic DR drill evidence and scalability proof = 3	3
	Valid CERT-In Safe-to-Host certificate not older than 12 months and demonstrated operational command/monitoring centre:	4

Criterion	Sub-parameter	Indicative marks
	Certificate = 2; Command centre demonstration = 2	
Sr. 5 Service provider profile (12)	Staff on rolls: 450 to 649 = 2; 650 to 850 = 3; 850 and above = 4. Evidence to be certified by CEO/HR Head with EPFO or equivalent statutory proof.	4
	CMMI and ISO maturity: Valid CMMI Level 3 = 1 service Valid CMMI Level 3 = 1 development; Valid CMMI Level 5 = 2 service Valid CMMI Level 5 = 2 development; ISO/IEC 20000-1 in addition to mandatory ISO 9001 and ISO/IEC 27001 = 1	5
	Financial strength: Average annual turnover of INR 500 crore <= INR 750 crore = 1; < INR 750 crore upto INR 1000 crore = 2; More than 1000 crore = 3.	3
Sr. 6 Project plan (10)	Mobilisation, staffing, training, venue readiness checks and mock-day plan quality	3
	Data-management plan mapping all question paper, candidate, centre, biometric, attendance, score, log, dashboard and archival deliverables 3.4 & 3.5 deliverable	3
	BCP/DR (RTO/RPO), contingency and exit plan; innovations	4

Criteria Sr. 1 (30 marks) and Sr. 2 (20 marks) shall be scored primarily through the mandatory live demonstration: the Service provider shall demonstrate its client and server software end-to-end using one of its conducted examinations, including QP upload-to-render workflow, timer compensation, node failure and recovery, biometric workflow, dashboard, and the security behaviours declared in Annexure T7, which IIBF may test in a live environment created by the Service provider. Failure to demonstrate a declared capability shall score zero for that capability and may attract action for misrepresentation.

Qualifying thresholds: Service providers must score at least 60% overall AND at least 60% in criterion Sr. 2 (Exam Software Security) to be declared technically qualified. Commercial Bids of only such Service providers shall be opened.

The bidders will be rated based on technical score in the technical round. The technical scores will be converted into technical weightage for a maximum of 70% and will be awarded to a bidder who scores highest points in technical round. The other vendors will be awarded the points proportionately in percentile basis.

Please note that technical scores will be provided based on both, demonstration and presentation by the bidder.

For example:

Suppose in response to the RFP, 3 bids are received from Bidder A, Bidder B and Bidder C then their scores will be calculated as under:

Assume, the bidders obtain the points as given below, based on the technical scoring matrix:

Bidder A gets say 65 points,

Bidder B gets say 70 points

and Bidder C gets say 90 points

As technical points are given 70% of weightage, the technical scores of each bidder are calculated as under: (arriving points proportionately with the highest points divided by points obtained by a bidder and multiplied by the technical weightage i.e., 70) (rounded to the nearest decimal)

The technical score of Bidder C will be = {Points awarded to Bidder C (90) / Points awarded to Bidder C (90)} $\times$ 70 = 70

The technical score of Bidder A will be = {Points awarded to Bidder A (65) / Points awarded to Bidder C (90)} $\times$ 70 = 51

The technical score of Bidder B will be = {Points awarded to Bidder B (70) / Points awarded to Bidder C (90)} $\times$ 70 = 54

6.3 Commercial Evaluation

The Commercial Bids shall be evaluated on the Total Cost of Ownership computed from Annexure P1 using the notional evaluation volumes stated therein. The lowest evaluated commercial bid (C-low) shall receive a Commercial Score of 30; other bids shall receive Commercial Score = $30 \times (C\text{-low} \div C\text{-bid})$

Example:

Assume three bidders qualify in the Technical Evaluation stage and obtain the following Technical Scores (based on presentation and demonstration) and Commercial Quotes:

Bidder	Rate per candidate (₹)
A	120
B	100

C	110
---	-----

Since Bidder B has submitted the lowest evaluated commercial bid (C-low = ₹100), Bidder B will receive a Commercial Score of 30.

Commercial Scores shall be calculated as follows:

- Bidder A = $30 \times (100 \div 120) = 25$
- Bidder B = $30 \times (100 \div 100) = 30$
- Bidder C = $30 \times (100 \div 110) = 27.27$

6.4 Techno-commercial evaluation:

The Service provider with the highest Composite Score (S1) shall be recommended for award. In case of a tie, the Service provider with the higher Technical Score shall be preferred. IIBF reserves the right to negotiate with the S1 Service provider as per applicable rules and to empanel more than one Service Provider, assigning any exam or exam-related activity fully or partly to any empanelled agency.

Composite Scores shall be calculated as:

Bidder	Technical Score (70%)	Commercial Score (30%)	Composite Score
A	51	25	76
B	54	30	84
C	70	27.27	97.27

Accordingly, Bidder C achieves the highest Composite Score (97.27) and shall be ranked S1 accordingly B will be S2 and A will be S3.

6.5 Presentation and Demonstration — Mandatory Agenda

Technically shortlisted Service providers shall make a presentation to technical committee not exceeding 30-45 mins and a live demonstration to technical team at IIBF's premises (or a venue notified by IIBF) covering, at minimum, the following, in this sequence. The date, time and venue shall be intimated separately; failure to attend or to demonstrate any declared capability shall be scored accordingly.

Item	Demonstration content
1	Corporate overview, examination credentials, organisation and governance for the IIBF engagement
2	End-to-end QP workflow: upload on standalone server, encryption, batch password release, distribution to a venue server, rendering verification, candidate-side display (bilingual, shuffling, numeric key-in)

Item	Demonstration content
3	Exam-engine behaviours: timer and automatic interruption compensation; node failure and re-mapping without data/time loss; auto-save/auto-submit; no local response storage (verified at the node)
4	Security behaviours per Annexure T7: VLAN segregation, USB/remote-desktop lockdown, intrusion detection/logging, access logs (who/what/when), sanitisation routine
5	Biometric and registration workflow: QR scan, fingerprint//photo capture/face with liveness, AI/ML face match with mismatch alert, random seat allocation
6	Command centre, dashboards (IIBF view), CCTV streaming with RTSP/HLS third-party access, incident ticketing and SLA counters
7	Data deliverables: extraction of the click-by-click log and sample Mandatory Data Set items; provisional-scores link generation
8	Q&A with the Technical Evaluation Committee

IIBF may empanel more than one Service Provider and distribute work among them; and negotiate with the successful Service providers on terms & condition and commercials. IIBF's decisions in all such matters shall be final and binding.

Where IIBF empanels or engages more than one Service Provider for an examination cycle, the concerned Service Providers shall ensure seamless interoperability and coordination of their systems. The dashboards provided by such Service Providers shall be synchronised in a manner prescribed by IIBF, and the test engine, examination interface, reporting parameters, data formats, security controls and operational workflows shall be uniform across all Service Providers, so as to ensure consistency, comparability and centralised monitoring by IIBF.

SECTION 7 – SERVICE LEVEL AGREEMENT (SLA) FRAMEWORK

The following service levels shall form the core of the SLA to be executed with the successful Service provider along with the Contract. Measurement shall be per examination cycle unless stated otherwise, based on system logs, dashboards, and IIBF verification. Service credits (penalties) for breach are specified in Section 9 and shall be deducted from invoices; SLA breaches are independent of, and in addition to, IIBF's other rights and remedies. Chronic breach (the same Severity-1 SLA breached in 3 consecutive examination cycles, or aggregate service credits exceeding 10% of annual contract value) shall constitute material breach entitling IIBF to terminate for default.

Sr. no.	Service Level	Target	Severity	Measurement
1	Venue finalization and freeze	Approved venue list and admit card data submitted minimum 30 days before examination; zero unapproved venue changes thereafter. Priority shall be given to center owner by the Service provider	Sev-1	IIBF approval records
2	Venue audit completion	100% venue audit reports submitted within 30 days prior to examination	Sev-1	Audit reports
3	Full-load Mock Run	Conducted at 100% venues, including all scheduled and buffer nodes, at least one day prior to examination. report and system logs submitted on mock day itself	Sev-1	Mock run certification
4	Venue sealing after mock run	100% compliance	Sev-1	Venue certification reports
5	Exam Functionary List Submission along with Police Verification & Due diligence and Background Check Compliance of all functionaries including documentation	Complete manpower list with verification details submitted at least 2 weeks before exam	Sev-1	Submission records
6	Exam Start Time	No delay exceeding 30 minutes at any venue	Sev-1	System logs

Sr. no.	Service Level	Target	Severity	Measurement
67	Examination Platform Availability	No loss of examination time for any candidate; automatic compensation where interruption occurs (system should automatically start where it stopped)	Sev-1	Application logs
8	Random Seat Allocation	100% automated random seat allocation (also no clustering); zero manual allocation without IIBF approval	Sev-1	Allocation logs
9	Power Backup Availability	UPS and DG backup available for entire examination duration at all venues	Sev-1	Inspection reports
10	Biometric Capture & Photograph Capture	100% successful capture at entry and in case of bio-break	Sev-1	Biometric reports
11	Face Match Verification	100% candidates subjected to AI/ML face matching before exam	Sev-1	Face match reports
12	Real-time Candidate Response Synchronization	Continuous synchronization during examination; zero local storage at candidate node and successful synchronization acknowledgement from venue server	Sev-1	System logs
13	Live CCTV feed availability to IIBF (RTSP/HLS)	Live CCTV availability from all required venues/cameras with no blind spots	Sev-1	Command Centre logs
14	Critical Incident Escalation	Severity-1 incidents reported within 15 minutes	Sev-1	Incident register
15	Daily Examination Report	Submitted by EOD or maximum by next day summary covering attendance, incidents, biometric statistics and UFM cases	Sev-2	Submission records
16	Response Transfer to Central Server	Immediate automated transfer after every session/batch	Sev-1	Transfer logs
17	Candidate Response Data Submission to IIBF	Complete encrypted response data submitted within 2–3 days of examination with hash	Sev-1	Delivery acknowledgement

Sr. no.	Service Level	Target	Severity	Measurement
		verification and integrity certificate		
18	Scanned Examination Documents Submission and CCTV Recording Submission	Attendance sheets, declarations, forms, logs and related scanned documents submitted within 2–3 days CCTV HDD and recordings submitted within one week of demand by IIBF	Sev-1	Delivery acknowledgement
19	Network Intrusion Report	Report on intrusion, remote access attempts and security events submitted within 24 hours of detection and final RCA within 7 days	Sev-1	Security report
20	Provisional Score Publication	Provisional scores are to be shown on submit. Also, link to download provisional score card to be made available within 2-3 days after examination on Institute's website.	Sev-2	Portal records
21	UFM / Forensic Analysis Report	Submitted within one week of examination completion	Sev-1	Report submission
22	Mandatory Data Set Submission	Complete Clause 3.4 & 3.5 data submitted within one week of exam completion	Sev-1	Delivery receipt
23	Network Logs & Security Logs Availability	100% availability whenever requested by IIBF	Sev-1	Audit verification
24	CCTV Data Retention & All examination Data Retention	For the contract period	Sev-1	Audit verification
25	Performance Review CAPA Closure	Corrective actions submitted and closed before next exam cycle	Sev-2	CAPA tracker
26	Data Integrity	Zero unauthorized deletion, manipulation, suppression or alteration of examination data	Sev-1	Audit & forensic verification
27	Test Engine Availability at IIBF Premises	100% uptime during QB upload, mapping and exam preparation period	Sev-1	System Logs

Sr. no.	Service Level	Target	Severity	Measurement
28	Authoring tool to CBT engine API integration	Successful API integration and validation before exam cycle commencement	Sev-1	UAT Reports
29	OTP-Based Seat / Node Reassignment	100% reassignment through OTP workflow; zero manual override without approval	Sev-1	System Logs
30	Command centre dashboard availability	100% uptime during examination window	Sev-1	Dashboard Logs
31	Test engine, central server, venue server data deletion certification	Deletion certification submitted within 15 days of completion of retention obligations	Sev-1	Deletion Certificate
32	Re-Examination Readiness Due to Service Provider Failure	Re-examination arrangements completed within timeline prescribed by IIBF	Sev-1	Re-exam Readiness Report

7.1 Definitions and Measurement Methodology

- "Examination cycle" means all sessions of a given examination window as notified by IIBF. "Severity-1" service levels are those whose breach directly threatens examination integrity, candidate experience or IIBF's statutory/reputational position and "Severity-2" affect operations materially;
- Measurement sources are, in order of precedence: system-generated logs and dashboards/command center; Observer reports; delivery receipts and registers; and IIBF verification. The Service Provider shall grant IIBF read access to raw measurement data; measurement disputes shall be resolved on the basis of raw logs, with IIBF's determination final.
- Exclusions: downtime or delay caused solely by IIBF's acts/omissions or by a Force Majeure Event (Clause 8.13) shall be excluded from SLA computation, provided the Service Provider demonstrates the exclusion with evidence and has complied with its mitigation, safety and reporting obligations.

7.2 Service-Credit Computation

- Service credits equal the penalty amounts specified in Section 9 for the corresponding default, and are deducted from the invoice of the examination cycle in which the breach occurred (or the next invoice, or the PBG, if the invoice is insufficient).
- Worked example: if, in a cycle of 50,000 candidates at a quoted rate of ₹X per candidate per session, biometric capture fails for 300 present candidates (SLA Sr. 11), the deduction is $(\text{₹X} \times 300 \text{ forfeited}) + (5\% \times \text{₹X} \times 300 \text{ penalty})$, plus ₹10,000 per venue where the failure exceeded 2% of candidates applied automatically with the invoice, supported by the biometric reconciliation report.
- Repeat-offence multiplier: recurrence of the same root cause after a CAPA doubles the applicable credit (Clause on RCA below); chronic breach triggers termination rights per the preamble to this Section.

7.3 SLA Governance

1. Governance forums: (i) exam-day war-room reviews between the Service Provider Command Centre and IIBF; (ii) post-cycle review within 10 days of each examination cycle covering SLA scorecard, incidents, RCA/CAPA and data-handover reconciliation; (iii) monthly compliance report by the 7th of each month; and (iv) quarterly steering-committee review at CEO/Programme-Director level covering trends, audits, risk register and improvement roadmap.
2. The SLA scorecard format, incident severity matrix and CAPA tracker shall be finalised with the SOPs (within 21 days of the Agreement) and may be refined by IIBF from time to time without increasing the SP's commercial entitlements.

7.4 SLA Scorecard — Sample Format (per examination cycle)

Sr.	Service level (Sr. per table above)	Target	Achieved	Breach instances (venues/candidates)	Service credit (₹)
1	Exam start time (Sr. 3)	No delay > 30 min			
2	Platform availability (Sr. 4)	≥ 100%			
3	Biometric capture (Sr. 6)	≥ 100%			
4	CCTV live feed (Sr. 7)	≥ 100%			
	... all remaining service levels ...				
	Total service credits for the cycle				

The scorecard shall be produced by the Service Provider with each invoice, reconciled against system logs, and countersigned at the post-cycle review.

Root-Cause Analysis: For every Severity-1 breach, the Service Provider shall submit a root-cause analysis and corrective-and-preventive action (CAPA) report within 5 working days. Repeat occurrence of the same root cause shall double the applicable service credit for that breach.

SECTION 8 – TERMS AND CONDITIONS

8.1 Legal Framework – Statutory Compliance

The Service Provider shall comply with the provisions of the relevant laws of the country, any rules or guidelines issued thereunder and best industrial practices. The Service Provider shall take all necessary measures to prevent impersonation, use of unfair means, data compromise, or any act that may affect the integrity of the examination. Any violation attributable to the Service Provider shall attract action under applicable law in addition to contractual remedies.

The Service Provider shall further be duty-bound to observe all laws, rules, regulations, policies, procedures and guidelines as in force from time to time, including: any norms or guidelines issued with regard to the conduct of examinations (the latest orders/guidelines under the relevant laws to be adhered to in letter and spirit); the cyber-security audit and certification requirements specified by MeitY, Government of India, through CERT-In empanelled agencies, together with STQC certification and ISO 9001, ISO/IEC 20000-1 and ISO/IEC 27001 standards for the examination software and processes; applicable UIDAI guidelines if mandated, audits and compliances for all Aadhaar-based authentication (applicable as and when mandated by IIBF in future); and all applicable labour laws and statutory obligations in respect of the personnel engaged by it.

8.2 Processing Norms and Data Handling

1. Candidate data, including personal data, images and biometric data of candidates, shall belong to IIBF, with the Service Provider acting purely as a data processor for IIBF. The Service Provider shall process such data only in accordance with the general or special guidelines, norms and instructions provided, validated or accepted by IIBF and agreed between the parties, and shall implement the security measures required under this RFP for data at rest, in transit and in use.
2. Any data loss, unauthorised disclosure or security incident affecting examination or candidate data shall be reported to IIBF immediately upon detection, with a detailed incident report and remediation plan; the consequences in Clauses 8.4, 8.6 and Section 9 shall apply.
3. In case of any investigation, enquiry or similar action by any statutory agency, IIBF shall primarily provide the required information to the agency, and the Service Provider shall provide the required information through IIBF without delay.
4. All candidate and examination data shall be hosted and processed only within India.

8.3 Ownership of Examination Data

All data generated or captured during the conduct of examinations including candidate data, biometric data, responses, logs, reports and CCTV recordings shall remain the sole and exclusive property of the Institute. The Service Provider shall not reuse, analyse, mine, or retain such data beyond the Contract period or beyond the retention periods specified herein, and shall certify deletion of all residual data upon completion or termination of the Contract, in the format prescribed by the Institute.

8.4 Right to Withhold Payment Linked to Compliance

Notwithstanding anything contained elsewhere in this RFP or the Contract, the Institute shall have the right to withhold, defer or suspend payment, in whole or in part, if the Service Provider fails to comply with any

contractual, statutory, procedural, security or reporting obligation under this RFP or the Contract. Such non-compliance may include, but shall not be limited to:

1. Non-submission or delayed submission of mandatory reports, audit trails, logs, CCTV footage or certifications;
2. Failure to provide complete and accurate examination data, biometric records or supporting documentation;
3. Non-cooperation with audits, inspections, monitoring agencies or Institute-designated authorities;
4. Non-compliance with statutory requirements, security protocols or examination-integrity measures;
5. Failure to complete data handover, reconciliation or certification requirements to the satisfaction of the Institute.

The withheld amount shall be released only after the Service Provider rectifies the non-compliance and completes all corrective actions to the satisfaction of the Institute. Exercise of this right shall be without prejudice to any other rights, remedies, penalties or contractual actions available to the Institute under this RFP, the Contract or applicable law.

8.5 Payment Terms

1. Payment shall be made in Indian Rupees only, examination-cycle-wise, upon successful performance of all exam-related activities in Section 3, submission of invoice in duplicate with all mandated deliverables and data, and due verification by IIBF. No advance payment shall be made.
2. Each invoice shall be accompanied by: (i) the complete data-handover certificate (Annexure T10-proforma) and (ii) SLA compliance report. Invoices unaccompanied by these shall not be due for payment.
3. Undisputed payments shall be released within 30 days of receipt of a complete and compliant invoice, after deduction of applicable penalties/service credits and taxes at source.

8.6 Liability for Data — Service provider's Absolute Data Accountability

1. The Service Provider shall be fully and strictly liable for all data required to be generated, captured, preserved and delivered to the Institute under this RFP (including the Mandatory Data Set at Clause 3.4 & 3.5, biometric data, CCTV recordings, logs and response data). Any data that the Service Provider cannot provide to the Institute whether due to loss, corruption, non-capture, deletion, technical failure or otherwise shall be treated as a material breach attributable to the Service Provider, without the need for IIBF to prove fault.
2. For every instance of non-providable data, the Service Provider shall be liable for: (i) the specific penalties in Section 9; (ii) withholding of payment under Clause 8.4 for the affected examination; (iii) the cost of any re-examination, re-verification or forensic reconstruction necessitated by such non-availability; and (iv) indemnification of IIBF against all claims, losses, regulatory penalties and litigation costs arising from such non-availability.
3. In case of non-fulfilment of the Service Provider's obligations leading to any data loss or non-compliance with event-based logging/data-saving requirements, the Service Provider shall indemnify IIBF to the extent of the loss suffered by IIBF. Repeated non-delivery of data (two or more

examination cycles) shall entitle IIBF to terminate for default, forfeit the Performance Bank Guarantee, and blacklist the Service Provider.

8.7 Limitation of Liability

Subject to the carve-outs below, the total aggregate liability of the Service Provider under the Contract shall be limited to the total contract value payable by IIBF for the relevant contract exam/year as applicable. This limitation shall NOT apply to:

- (i) liability arising from breach of confidentiality or data-protection obligations;
- (ii) liability arising from question-paper leakage, UFM facilitation or violation relevant laws and regulation of the country
- (iii) indemnity obligations for third-party IPR infringement, bodily injury or death, or fraud/wilful misconduct; and
- (iv) statutory penalties.

Neither party shall be liable to the other for indirect or consequential damages, except in the carved-out cases above.

8.8 Performance Bank Guarantee

The successful Service provider shall furnish, within 15 days of the Letter of Intent/award, an irrevocable and unconditional Performance Bank Guarantee from a scheduled commercial bank equal to 10% of the estimated contract value, valid for the Contract period plus a claim period of 12 months, in the format prescribed by IIBF (see Annexure E11 pattern). The PBG shall be extended for any extension of the Contract. Failure to furnish the PBG may result in cancellation of the award and forfeiture of the EMD. IIBF may invoke the PBG for non-performance, SLA default, data non-delivery or any loss caused to IIBF.

8.9 Exit Management and Transition Support

Upon expiry, termination or non-renewal of the Contract for any reason, the Service Provider shall provide full cooperation and support to ensure a smooth, uninterrupted transition of examination services to the Institute or to any successor agency designated by the Institute. During a transition period of up to 6 months, the Service Provider shall, without additional cost to the Institute:

1. Hand over all examination-related data that is candidate data, responses, biometric data, logs, reports, CCTV recordings and related documentation, in the formats specified by the Institute;
2. Provide necessary technical assistance, documentation, process details and knowledge transfer to enable continuity of examination operations;
3. Support data migration, system handover and reconciliation activities as required by the Institute or the successor agency;
4. Continue to maintain data confidentiality, integrity and security obligations during and after the transition period;
5. Certify deletion of all residual examination data from its systems after successful completion of data handover, as confirmed by the Institute.

The Service Provider shall not take any action that may disrupt examination processes or adversely affect the transition. Obligations under this clause shall survive expiry or termination of the Contract until successful completion of the transition to the satisfaction of the Institute. The last invoice of the Contract shall not fall due until the exit-management obligations are certified as complete by IIBF.

8.10 Confidentiality, Non-Disclosure and IPR

1. The Service provider and its personnel shall treat all documents, data and information as private and confidential, during and after the Contract, and shall execute the Non-Disclosure Agreement at Annexure E10. The Service provider shall not disclose any examination data to unauthorised parties at any stage and shall preserve the sanctity of the examination. Breach of confidentiality by the Service provider or its personnel shall render the Service provider liable in law and in contract.
2. IPR in the Service provider's standard software and application software shall remain with its owner; usage rights shall be granted to IIBF for the Contract term. All rights, title and interest in IIBF Data shall always remain with IIBF, and the Service provider shall have no right to use IIBF Data except upon written authority of IIBF. The Service provider warrants that its solution does not infringe any third-party IPR and shall indemnify IIBF against all losses or claims arising from any such infringement.

8.11 Appointment of third party by Service Provider

The Service Provider may use third-party providers only for enabling services (exam manpower such as invigilator, security guard, support staff, electrician and frisking staff, CCTV installation, biometric authentication including Aadhaar-based (applicable as and when mandated by IIBF in future), security guards, DG sets, exam infrastructure), with prior written approval of IIBF for any addition. The Service Provider shall remain fully and solely responsible and liable to IIBF for all acts and omissions of its third party, including compliance with background-verification, statutory and data-protection obligations. The core exam platform, the personnel handling the servers, responsibility of conduct of exam and data processing shall not be sub-contracted in any case.

8.12 Termination and Suspension

1. Termination for Default: IIBF may, by 90 days' written notice, terminate the Contract in whole if the Service Provider fails to perform its obligations, the quality of delivery is not to IIBF's satisfaction, chronic SLA breach occurs (Section 7), or the Service Provider commits material breach (including data non-delivery under Clause 8.6, breach of relevant laws, or breach of confidentiality). IIBF may procure the services elsewhere at the Service Provider's risk and cost; the PBG shall stand forfeited; and the Service Provider shall hand over all documents and data related to the exams to IIBF and lend all support, including data transfer, to the new agency.
2. Termination for Insolvency: IIBF may terminate forthwith, without compensation, if the Service Provider becomes bankrupt or insolvent.
3. Termination for Convenience: IIBF may terminate for convenience with 90 days' written notice; the Service Provider shall be paid for services satisfactorily rendered up to the effective date, subject to completion of exit-management obligations.
4. Suspension: IIBF may, after 15 days' written notice specifying the failure, suspend all payments if the Service Provider fails to perform its obligations, and may engage another agency to complete suspended work at the Service Provider's cost. No consequential damages shall be payable to the Service Provider in the event of termination or suspension.

8.13 Force Majeure

Neither party shall be liable for failure or delay caused by events beyond its reasonable control including fire, flood, earthquake, epidemics/pandemics, quarantine restrictions, acts of God, acts of State, strikes, war, terrorism, riots, civil disorder, embargoes and similar events ("Force Majeure Event"). Cyber-attacks shall qualify only where the affected party demonstrates that it had implemented the security measures mandated under this RFP. The affected party shall immediately notify the other with reasonable detail. If a Force Majeure Event continues for more than 30 days, IIBF may terminate the Agreement by written notice, without liability, subject to exit-management obligations.

8.14 Indemnity

The Service Provider shall indemnify, defend and hold IIBF harmless from and against all claims, demands, losses, damages, costs and expenses (including legal costs) arising out of or in connection with: (i) breach of the Contract, SLA or applicable law by the Service Provider or its personnel/sub-contractors; (ii) misappropriation of third-party trade secrets or infringement of any patent, trademark, copyright or other statutory rights under any law, including the Copyright Act, 1957 or the Information Technology Act, 2000; (iii) loss, unauthorised disclosure or non-availability of examination/candidate data; (iv) personal injury or property damage caused by its personnel; (v) claims by its personnel or sub-contractors; and (vi) penalties imposed on IIBF by any regulator on account of the Service Provider's acts or omissions.

8.15 Integrity Pact; Fraudulent and Corrupt Practices

The Service provider shall enter into an Integrity Pact with IIBF and shall not resort to any corrupt practice at any stage of the Contract, including not offering any benefit to IIBF employees, not entering into undisclosed arrangements with other Service providers, and disclosing agents/representatives and past transgressions. Service providers and their officers, employees, agents and advisers shall observe the highest standards of ethics. IIBF shall reject a proposal, forfeit the EMD/PBG and may debar the Service provider, without liability, if the Service provider engages, directly or indirectly, in any corrupt, fraudulent, coercive, undesirable or restrictive practice (as commonly defined in Government of India procurement, including cartelisation, misrepresentation, canvassing and conflict of interest) in the selection process or Contract performance.

8.16 Governing Law, Jurisdiction and Dispute Resolution

The Contract shall be governed by the laws of India. Any dispute shall first be resolved through good-faith escalation between senior management of both parties within 30 days; failing which, disputes shall be referred to arbitration by a sole arbitrator appointed in accordance with the Arbitration and Conciliation Act, 1996 (as amended), seat and venue at Mumbai, proceedings in English. Subject to the arbitration clause, courts at Mumbai shall have exclusive jurisdiction. Time is of the essence: examination dates declared by IIBF are absolute unless changed by IIBF, and the Service Provider shall strictly adhere to all schedules; delays shall attract penalties under Section 9, and no extension shall be granted having an adverse effect on the scheduled conduct of the examination.

8.17 Co-operation and Support; Right to Deny Entry; Representations

The Service Provider shall extend full cooperation to IIBF/all relevant Government agencies wherever applicable, including timely provision of information, compliance with documentation requests, and assistance in audits, inspections or evaluations. IIBF reserves the right to restrict or deny entry of any staff member of the Service Provider with valid and justified reason, and is authorised to take necessary actions at test centres for fair examination conduct, to which the Service provider agrees unconditionally. The

Service Provider warrants that the services will be provided in a skilful, workmanlike manner and in conformity with the scope defined in this RFP.

8.18 Insurance

The Service Provider shall obtain and maintain, at its cost, throughout the Contract term: (i) comprehensive general liability insurance covering venue operations (including third-party bodily injury and property damage at examination sites); (ii) workmen's compensation/employee insurance for all deployed personnel as per law; (iii) asset insurance for equipment deployed at venues; and (iv) cyber/crime insurance of adequate cover for data and examination-system incidents. Certificates of insurance shall be furnished to IIBF before the first examination and on each renewal.

8.19 Taxes, Duties and Statutory Levies

Quoted rates are exclusive of GST, which shall be paid additionally at the rates applicable at the time of invoicing against valid tax invoices; all other taxes, duties, levies and statutory payments (including those relating to the Service provider's personnel) shall be to the Service provider's account. IIBF shall deduct tax at source as required by law. Any new levy or change in rates shall be dealt with as per law, with no change to the basic contracted rates.

8.20 Personnel; No Employer–Employee Relationship

All persons deployed by the Service Provider or its third party shall remain their employees/engagees for all purposes; nothing in the Contract creates any employer–employee relationship between IIBF and such persons, and the Service Provider shall indemnify IIBF against any claim to the contrary. The Service Provider shall pay wages/dues in time, comply with EPF/ESI and all labour enactments, replace any person whose continued deployment IIBF reasonably objects to, and ensure that all deployed personnel are trained on their roles, examination-integrity duties, safety/evacuation procedures and conduct standards before every examination.

8.21 Audit, Inspection and Step-in Rights

In addition to Clause 3.4 & 3.5, IIBF and its designated may, on reasonable notice (and without notice on examination/mock days), inspect any venue, the Service provider's data centre/DR, monitoring centre, records and systems relating to the services, and audit SLA measurement and invoicing. Where an imminent threat to examination integrity is identified, IIBF may direct immediate remedial measures, drop a venue, or step in through another agency at the Service Provider's risk and cost, without prejudice to other remedies.

8.22 Publicity; Notices; Assignment; Waiver; Severability; Survival

1. **Publicity:** The Service Provider shall not use IIBF's name, logo or the fact of this engagement in any publicity, press release, client list or marketing material without IIBF's prior written consent.
2. **Notices:** All notices shall be in writing, delivered by hand, registered post/courier or e-mail (with confirmation), to the addresses/IDs notified by the parties, and shall be effective on receipt.
3. **Assignment:** The Service Provider shall not assign or transfer the Contract or any rights/obligations thereunder without IIBF's prior written consent; any change in control of the Service Provider shall be notified to IIBF forthwith.
4. **Waiver and severability:** No failure or delay by IIBF in exercising any right shall operate as a waiver; a waiver on one occasion shall not bar exercise on another. If any provision is held invalid, the

remainder shall continue in force, and the parties shall substitute a valid provision closest to the original intent.

5. Survival: Clauses relating to confidentiality, data ownership and accountability, indemnity, exit management, audit, penalties accrued, dispute resolution and any clause which by its nature should survive, shall survive expiry or termination of the Contract.

8.23 Order of Precedence

In case of any conflict, the order of precedence shall be as stated in Annexure D1: the signed Agreement and schedules; the SLA; this RFP with corrigenda; the Letter of Intent; and the Service provider's proposal. Usage terms of the Service Provider's proprietary application system, if any, shall apply only to the extent expressly accepted by IIBF in the Agreement and shall not dilute IIBF's rights over examination data, audit and exit management under this RFP.

8.24 Re-examination

In the event that any examination, session, batch, centre or group of candidates is required to be re-conducted on a buffer date, unused weekend or any other date decided by IIBF due to any technical, operational, administrative, security-related or other deficiency, failure, lapse, delay, disruption, non-compliance or negligence attributable to the Service Provider, including its personnel, venues or systems, the entire responsibility and cost of such re-conduct shall be borne solely by the Service Provider. Such costs shall include, without limitation, venue charges, manpower, infrastructure, technology, communication, candidate support, logistics, coordination, monitoring, data processing and all other direct or incidental costs associated with the re-conduct. No additional payment shall be payable by IIBF for such re-conduct.

The above shall be without prejudice to IIBF's right to levy applicable penalties, liquidated damages, recover losses, withhold payments, invoke the Performance Bank Guarantee, seek indemnification, terminate the contract, debar the Service Provider, or take any other action available under the RFP, contract or applicable law.

Where the re-examination or re-conduct is necessitated solely due to a decision of IIBF and is not attributable, directly or indirectly, to any act, omission, failure, deficiency or non-compliance of the Service Provider, the cost of such re-conduct shall be borne by IIBF at the contracted rates, strictly on a pro-rata basis and only for the candidates/sessions actually re-conducted.

The Service Provider shall be mandatorily required to conduct any such re-examination within thirty (30) calendar days from the originally scheduled examination date, or within such shorter timeline as may be directed by IIBF. Failure or inability of the Service Provider to conduct the re-examination within the stipulated timeline shall constitute a material breach of contract and shall attract additional penalties as specified in Section 9, without prejudice to any other rights or remedies available to IIBF.

SECTION 9 – PENALTIES AND LIQUIDATED DAMAGES

The Service provider shall strictly adhere to the processes, service levels (Section 7) and time schedules given by IIBF for each examination, failing which the penalties below shall apply. Penalties are genuine pre-estimates of loss, are cumulative across heads, and shall be recoverable by deduction from invoices, the PBG or otherwise. Imposition of penalty is without prejudice to IIBF's rights of withholding (Clause 8.4), indemnity (Clause 8.14), termination (Clause 8.12)

9.1 Penalties for Examination Integrity and Conduct Failures

Sr.	Default / Event	Penalty
1	Question paper leakage and/or security breach of the examination system (including unauthorised access to any node during the examination)	₹1 crore per incident plus full cost of re-examination recoverable from the Service provider; criminal action under the applicable laws against persons/parties responsible; IIBF may terminate and forfeit the PBG
2	Original marks of a candidate found altered	₹1,00,000 per candidate
3	Entire result calculated wrongly	₹1 crore plus re-conduct of examination by the Service provider at no cost to IIBF
4	Serving wrong QP to candidates	₹5,000 per affected candidate
5	Not able to serve QP to candidates for any reason	₹1,000 per affected candidate plus re-conduct at no cost to IIBF
6	Issues occurred during exam day due to non-conduct of mock run, or mock cancelled due to lack/defective level of services of the Service Provider or any other reason attributable to it	₹10,000 per venue plus ₹500 per scheduled candidate of that venue; repeated failure treated as material breach
7	Delay in commencement/conduct of examination beyond 30 minutes	₹1,000 per affected candidate; For delay beyond 60 minutes, additional 10% of the per-candidate quoted rate × affected candidates, doubling for every further 45 minutes of delay
8	Cancellation of examination/shift on account of disruption (power/connectivity/computer failure or any other reason attributable to the Service provider)	₹500 per affected candidate plus re-conduct at no cost to IIBF; if re-conduct not completed within 30 days of the original date, additional ₹5,000 per candidate

Sr.	Default / Event	Penalty
9	Unfair practices overlooked by invigilators/functionaries during the examination	₹5,000 per candidate/incident, without prejudice to action under any other law as applicable FIR to be filed as instructed by IIBF
10	10% buffer computers not available at any examination venue	₹1,000 per affected candidate
11	Deficiency/discrepancy in biometrics and photo capture before and after the exam (entry/exit/bio-break)	No payment for the affected candidate plus 5% of the per-candidate quoted rate for each such candidate; systemic failure (>2% of candidates at a venue) additional ₹10,000 per venue
12	Failure to detect unauthorised access (remote access/hacking, etc.) of a candidate computer during the examination, or failure to report the same to IIBF within 2 weeks of completion of the examination	₹5,00,000 per incident plus costs of forensic investigation and any consequential re-examination; wilful concealment shall be treated as security breach.
13	In each of the below case: - Failure to provide random, automated seat allocation to candidates, or any instance of manual/discretionary seat allocation by ground staff without prior approval of IIBF, shall be treated as a serious breach affecting examination integrity - Failure to obtain prior written approval of IIBF before de-mapping/re-mapping of candidate seat/node, or failure to maintain required logs and records for such changes. - Failure to conduct AI/ML facial verification of candidates or allowing candidates to appear without prescribed verification process.	₹5,000 per affected candidates where such failure is observed.
14	Failure to conduct mandatory venue audit prior to the examination as per prescribed guidelines or conduct of examination in an unaudited/unapproved venue.	₹1,00,000 per venue per occurrence.
15	- Deployment of manpower/ functionary below prescribed norms or deployment without police verification/background verification/Aadhaar authentication (applicable as and when mandated by IIBF in future) - Presence of unauthorised persons detected in the examination venue during the examination, including the venue owner, venue staff, local IT	₹10,000 per deficient/unverified functionary. ₹ 50,000 per unauthorised person

Sr.	Default / Event	Penalty
	personnel or any person not approved/authorised for examination duty by IIBF	
16	Failure to install, operate or maintain signal jammers where mandated by IIBF. (applicable as and when required in future)	₹25,000 per venue per session.
17	Failure to conduct re-examination within prescribed timeline where attributable to SP.	₹5,000 per affected candidate in addition to re-examination costs.
18	Failure to implement agreed CAPA/RCA before next examination cycle.	₹50,000 per unresolved observation.

9.2 Penalties for Data, Reporting and Surveillance Failures

Sr.	Default / Event	Penalty
1	Delay in each of the below case: - Submission of candidates' examination responses in encrypted format to IIBF beyond the timelines in Section 7 - Providing data (Mandatory Data Set, logs, trails, documents) to IIBF for audit/review beyond stipulated timelines - Providing scanned copies of attendance sheets and other documents mentioned in the RFP - Finalisation/freeze of Centre Master, cancellation or change of venue after freeze	₹ 10,000 per instance per day of delay. Additionally in case of change or cancellation of venue - Service provider to issue revised communications (email/SMS/calls) at its cost; movement of candidates to the other venue and any other cost involved in smooth conduct of examination as per the standards of IIBF.
2	Failure to provide (hard or soft copy) each of the below data: - CCTV footage of any venue for any exam day; mismanagement/mishandling of exam materials (e.g., attendance records) - Face-match verification reports, mismatch reports or exception reports. - Network intrusion detection reports, remote access reports or security incident reports. - UFM reports and necessary evidences within prescribed timeline. - Any other data critical for the examination as mentioned in the RFP (data lost, corrupted or otherwise not providable)	₹50,000 per data item per venue per instance/examination

Sr.	Default / Event	Penalty
3	Non-functional CCTV cameras or any blind spot detected in CCTV coverage at any venue.	25% of the per-candidate quoted rate for candidates in the affected rooms ₹500 per observed blind spot per day (as reported by Observer/observed by IIBF)
4	Improper venue infrastructure (ramp/lift for PwD, drinking water, washroom cleanliness, ventilation, etc.) Safety non-compliance at a venue: absent/expired fire-fighting equipment, blocked or unmarked emergency exits, no evacuation plan/first-aid kit, or failure of safety briefing.	₹5,000 per venue per day per instance
5	Non-cooperation with, or obstruction of, the IIBF/ third party authorised by IIBF or failure to mitigate critical audit observations before the exam	₹10,000 per instance plus withholding under Clause 8.4; persistent non-cooperation material breach
6	Data found to be tampered / manipulated / altered / deleted / overwritten / suppressed / fabricated, or where the integrity of examination data, logs, audit trails, biometric records, CCTV footage, candidate responses, attendance records, seating data, server records or any other examination-related record is compromised due to any act, omission, negligence, system failure, unauthorised access or lack of adequate controls attributable to the Service Provider.	₹1,00,00,000, in addition to recovery of all losses, costs, damages and expenses incurred by IIBF, including the cost of re-examination wherever required.
7	Failure to maintain archival or retain the following data: - Examination data, logs and records for prescribed retention period. - CCTV recordings for prescribed retention period.	₹1,00,000 per occurrence.
8	Failure of real-time synchronization of candidate responses from local server to central server, resulting in response loss, delayed upload or missing audit trail.	₹1,00,000 per venue/session plus consequential losses.
9	Instances identified around the following activities: - Non availability of test engine at IIBF Premises - API Integration & UAT Completion - QB/QP Audit Trail Availability - Test Engine/QB Data Deletion Certification	₹50,000 per instance.
10	Dashboard Availability	Dashboard unavailable for more than 30 continuous minutes during examination: ₹50,000 per incident.

Sr.	Default / Event	Penalty
11	Debarred Venue Database Maintenance	Failure resulting in use of previously debarred venue: ₹2,00,000 per venue per examination cycle.

9.3 Caps and General Provisions

1. The total combined penalty under Sections 9.1 and 9.2 shall not exceed 5% of the total cost for said examination cycle, excluding Sr. 9.1(1), 9.1(2) 9.1(3), and 9.2(2) 9.2 (6), which shall be recoverable in full without cap.
2. Penalties are indicative of, and not limited to, the listed defaults; failure to provide satisfactory examination services in any other respect shall attract proportionate penalty as determined by IIBF. If delay or default adversely affects the conduct of the examination, the security deposit/PBG may be forfeited and other legal action initiated.

9.4 Penalty Administration Process

1. Identification: defaults shall be identified from system logs, dashboards, Observer/EMA/auditor reports, proformas and IIBF verification. IIBF shall issue a penalty notice specifying the default, evidence and computed amount.
2. Representation: the Service Provider may make a written representation within 7 days of the notice, with evidence. IIBF shall consider the representation and communicate its decision, which shall be final for the purpose of deduction; the Service Provider's remedy, if aggrieved, lies in the dispute-resolution mechanism (Clause 8.16), without withholding of the deduction in the interim.
3. Recovery: penalties/service credits shall be deducted from the current or subsequent invoice; where invoices are insufficient, from the PBG or by direct demand payable within 15 days. Deduction shall not relieve the Service Provider of the obligation to cure the default.
4. No penalty shall be levied for delay or failure solely attributable to IIBF or to a Force Majeure Event, subject to the Service Provider's compliance with its mitigation, safety, reporting and re-conduct-support obligations.

SECTION 10 – LIST OF ANNEXURES

Annexure	Title
E1	Service provider's Letter for EMD / Bid Security
E2	Bid Security (Bank Guarantee) Format
E3	Service provider's Information and Financial Details
E4	Declaration Regarding Application Software (Ownership of Source Code)
E5	Eligibility Criteria Matrix
E6	Declaration for Acceptance of RFP Terms and Conditions
E7	Declaration for Acceptance of Scope of Work
E8	Format of Power of Attorney / Board Resolution
E9	Other Undertakings (Clean Track, No Blacklisting, Conflict of Interest)
E10	Non-Disclosure Agreement
E11	Format of Performance Bank Guarantee
E12	Bid Submission Compliance Checklist
S1	Catalogue of SOPs and Manuals to be Delivered
T1	Compliance to Technical & Functional Requirements
T2	Service provider's Experience
T3	Declaration Regarding Clean Track Record
T4	Client Details for Reference
T5	Project Plan (incl. Contingency, BCP/DR and Exit Plan)
T6	Short Description of the Proposed Solution
T7	Exam Software Security Declaration
T8	Scope of Independent Audit and its Requirements
T9	Exam-Day Proformas and List of Stationery Items
T10	Formats of Exam-Day Proformas
T11	Data Deliverables Dictionary
T12	Organisation Structure and Personnel to be Deployed
P1	Commercial Bid / Price Bid Format

Annexure	Title
IP	Pre-Contract Integrity Pact
C1	Instructions to Candidates (to accompany the Admit Letter)
D1	Outline of the Draft Agreement / Contract
F1	Details of exam centers owned by Service Provider
CTR	Indicative Centre/City List with Number of Candidates

Annexure E1 – Service Provider’s Letter for EMD / Bid Security

(To be submitted on the Service Provider’s letterhead)

To,
The Chief Executive Officer,
Indian Institute of Banking & Finance,
Mumbai.

Sub: EMD for RFP No. IIBF/EXAM RFP- __/20__ - __ for Selection of Service Provider(s) to conduct CBT Examinations.

Dear Sir/Madam,

We enclose herewith Demand Draft / Pay Order / Bank Guarantee No. dated drawn on (scheduled bank) for ₹25,00,000/- (Rupees Twenty-Five Lakh only) in favour of "Indian Institute of Banking & Finance", payable at Mumbai, towards Earnest Money Deposit. We agree that the EMD may be forfeited in the circumstances specified in Clause 5.2 of the RFP.

Signature of Authorised Signatory

Name:

Designation:

Company Seal

Date:

Annexure E2 - Bid Security (Bank Guarantee) Format

(On non-judicial stamp paper of requisite value, issued by a scheduled commercial bank)

In consideration of the Indian Institute of Banking & Finance ("IIBF") having agreed to accept from M/s ("the Service Provider") a Bank Guarantee in lieu of Demand Draft towards EMD of ₹25,00,000/- for RFP No., we, Bank, do hereby unconditionally and irrevocably undertake to pay to IIBF, on first written demand and without demur, protest or reference to the Service Provider, any amount not exceeding ₹25,00,000/- (Rupees Twenty-Five Lakh only), notwithstanding any dispute raised by the Service Provider. This guarantee shall remain valid up to (6 months from the last date of bid submission) and any demand must be received by the Bank on or before the expiry of the claim period. This guarantee shall not be affected by any change in the constitution of the Service Provider or the Bank.

Signed and sealed for and on behalf of the Bank.

Annexure E3 - Service Provider's Information and Financial Details

Particulars	Details to be furnished
Name of the Service Provider / Registered Office / Corporate Office	
Date and place of incorporation; CIN	
Constitution (Public/Private Ltd/PSU)	
PAN / TAN / GST Registration Number	
Contact person, designation, phone, e-mail	
Total IT staff strength (with EPFO evidence)	
Certifications held (CMMI level, ISO 9001, ISO/IEC 27001, ISO/IEC 20000-1, CERT-In Safe-to-Host) with validity	
Gross annual turnover: FY __ - __ / FY __ - __ / FY __ - __ (₹ crore)	
Turnover from CBT examination services only, for the same 3 years (₹ crore)	
Net worth and Profit/(Loss) for each of the last 3 audited FYs	
Location of Primary Data Centre and DR site (seismic zones)	
Number of CBT projects executed; number with ≥ 1 lakh candidates in a single day	

Enclose: Audited balance sheets and P&L for the last three financial years, CA turnover certificate with UDIN, and net-worth certificate. Signature with date and seal of the Service Provider.

Annexure E4 - Declaration Regarding Application Software (Ownership of Source Code)

We hereby declare that:

1. We own the complete source code of the application software (test engine) proposed for conducting IIBF's CBT examinations, together with all copyrights and components thereof, and no third party has any claim thereon that could impede the services;
2. The software is certified "Safe to Host" by a CERT-In empanelled agency (certificate enclosed) and we undertake to keep such certification valid, at our cost, throughout the Contract term;
3. The software complies with the Technical & Functional Requirements at Annexure T1, including automatic time-compensation for interruptions and non-storage of candidate responses at the node; and
4. We shall not deploy any unauthorised or unlicensed software in the delivery of services.

Signature of Authorised Signatory

Seal

Date

Annexure E5 - Eligibility Criteria Matrix

Sr.	Criterion (as per Section 4)	Complied (Yes/No)	Doc ref (page no.)
1	Registered Indian company, ≥ 5 years in existence; no consortium/JV/partnership/proprietorship		
2	CMMI L3/L5; ISO 9001, ISO/IEC 27001 (ISO/IEC 20000-1 preferred)		
3	Ownership of source code of CBT software		
4	Valid CERT-In empanelled "Safe to Host" certificate		
5	Single-day, single-session CBT in ≥ 100 cities across ≥ 20 States/UTs		
6	$\geq 1,00,000$ candidates in a single day, pan-India, within last 3 years		
7	Average annual turnover $\geq ₹500$ crore; positive net worth in each of the last 3 FYs		
8	≥ 450 staff on rolls		
9	Not blacklisted; no insolvency/bankruptcy (NCLT) proceedings in last 5 years		
10	No conflict of interest (no coaching/education/certification business in banking & finance)		

Annexure E6 – Declaration for Acceptance of RFP Terms and Conditions

(On Service Provider's letterhead)

We hereby certify that we have read the entire terms and conditions of RFP No. IIBF/EXAM RFP-2/2026-27 (including all sections, annexures and corrigenda), which shall form part of the Contract, and we unconditionally accept the same in totality. We further declare that our firm has not been blacklisted by any Central/State Government or PSU or autonomous body for any examination-related activity as on the date of submission, and that all information furnished is true and correct; if found otherwise, IIBF may summarily reject our bid or terminate the Contract, forfeiting the EMD/PBG, without prejudice to other rights and remedies.

Signature of Authorised Signatory

Seal

Date

Annexure E7 – Declaration for Acceptance of Scope of Work

(On Service Provider's letterhead)

We confirm that we have studied and understood the complete Scope of Work in Section 3 of the RFP, including the pre-examination, during-examination and post-examination deliverables, the SLA framework in Section 7, the data-accountability provisions in Clause 8.6 and the penalty regime in Section 9, and we unconditionally accept the same. We confirm our capability and undertake to perform the entire Scope of Work within the timelines specified.

Signature of Authorised Signatory

Seal

Date

Annexure E8 – Format of Power of Attorney / Board Resolution

(On non-judicial stamp paper of requisite value, notarised)

Know all men by these presents, we, M/s, do hereby constitute, appoint and authorise Mr./Ms., (designation), who is presently employed with us, as our attorney, to do in our name and on our behalf all acts, deeds and things necessary in connection with or incidental to submission of our bid for RFP No. of IIBF, including signing and submission of all applications, bids and other documents, participating in pre-bid and other conferences, providing information/responses to IIBF, and generally dealing with IIBF in all matters in connection with our bid. We ratify all acts done by our said attorney pursuant to this Power of Attorney. (Alternatively, a certified true copy of the Board Resolution conferring such authority may be submitted.)

Annexure E9 - Other Undertakings (Clean Track, No Blacklisting, Conflict of Interest)

(On ₹100 non-judicial stamp paper, duly notarised)

We hereby undertake and declare that:

1. We shall comply with all the relevant and applicable laws and regulations of the country and the rules/guidelines thereunder, acknowledge that we fall within the definition of "service provider" under such applicable law, and shall take all necessary measures to prevent impersonation, unfair means and data compromise; any violation attributable to us shall attract action under law in addition to contractual remedies.
2. We shall act purely as a data processor for IIBF in respect of candidate data, comply with the Processing Norms under Clause 8.2, maintain valid CERT-In empanelled certification (Safe to Host) and MeitY/STQC cyber-security audit requirements together with ISO 9001, ISO/IEC 20000-1 and ISO/IEC 27001 standards, obtain the UIDAI audit and all compliances for Aadhaar-based authentication (applicable as and when mandated by IIBF in future), and observe all applicable labour laws and other laws, rules, regulations and guidelines in force from time to time.
3. We are not currently blacklisted/debarred by any Central/State Government, PSU or autonomous body for exam-related activities; neither we nor our promoters/directors are subject to any insolvency/bankruptcy proceedings before the NCLT or any other authority; and we are not under any declaration of ineligibility for corrupt or fraudulent practices.
4. We have no conflict of interest, are not engaged in coaching/training/education/certification business in banking and finance, and shall not use coaching venues as examination venues.
5. We accept absolute data accountability under Clause 8.6 and the penalty regime under Section 9.
6. We shall abide by this bid for 180 days from bid opening; we shall sign the Contract and furnish the PBG within 15 days of the Letter of Intent; and we are participating as a single entity.

Annexure E10 - Non-Disclosure Agreement (Draft)

This Non-Disclosure Agreement ("NDA") is made at Mumbai on between the Indian Institute of Banking & Finance ("IIBF") and M/s ("the Company"), each a "Party" and, when receiving Confidential Information, the "Receiving Party".

1. Confidential information means all information disclosed by or on behalf of a Party, or generated in the course of the engagement, in any form, including: question banks and question papers; candidate personal data, photographs, signatures and biometric data; response data, scores and results; audit trails, logs and CCTV recordings; security architecture, network diagrams, encryption keys and credentials; SOPs, manuals and proformas; commercial terms; and any information marked or reasonably understood to be confidential. It excludes information that is publicly available without breach, independently developed without use of the disclosed information, or rightfully received from a third party without restriction.
2. Obligations: The Receiving Party shall (a) hold all Confidential Information in strict confidence with at least the same degree of care it uses for its own confidential information, and no less than reasonable care; (b) use it solely for performing the Contract/participating in the RFP; (c) restrict disclosure to employees, agents and approved sub-contractors on a strict need-to-know basis who are bound by obligations no less protective; (d) not copy, reverse-engineer, decompile or create derivative works except as required for the Contract; and (e) not remove proprietary markings.
3. Compelled disclosure: If disclosure is required by law, regulation or court/regulatory order, the Receiving Party shall, to the extent legally permissible, promptly notify the Disclosing Party, disclose only the minimum required, and cooperate in seeking protective treatment. For examination and candidate data, the route in Clause 8.2 of the RFP (through IIBF) shall be followed.
4. Breach and remedies: The Receiving Party shall notify the Disclosing Party immediately of any actual or suspected breach, and shall be responsible for breaches by its personnel and sub-contractors. The Parties agree that damages may be an inadequate remedy and the Disclosing Party shall be entitled to injunctive and equitable relief in addition to damages, penalties under Section 9 of the RFP and action under applicable law.
5. Return/destruction: Upon written request, or upon completion/termination of the engagement, the Receiving Party shall promptly return or destroy all Confidential Information (including all copies, extracts and summaries) and certify such return/destruction in writing, subject to the data-handover-first sequence in Clause 8.9 of the RFP.
6. Term: These obligations remain in force during the engagement and for 5 years thereafter, and perpetually for candidate personal data, biometric data, question banks/papers and security credentials. Nothing in this NDA grants any licence or IPR. Governing law: India; exclusive jurisdiction: Mumbai courts, subject to the arbitration clause of the Contract.

Signed by authorised signatories of both Parties with witnesses.

Annexure E11 — Format of Performance Bank Guarantee (PBG)

(On non-judicial stamp paper of requisite value, from a scheduled commercial bank)

To,

The Chief Executive Officer,

Indian Institute of Banking & Finance,

Mumbai.

WHEREAS M/s ("the Service Provider") has been awarded the contract for conducting CBT examinations of IIBF vide Letter of Intent/Agreement No. dated ("the Contract"), and the Contract requires the Service Provider to furnish a Performance Bank Guarantee for 10% of the estimated annual contract value, i.e. ₹.....

1. We, Bank, at the request of the Service Provider, hereby irrevocably and unconditionally guarantee payment to IIBF, on first written demand and without demur, protest, contestation or reference to the Service Provider, of any sum or sums not exceeding ₹..... in aggregate, upon IIBF stating that the Service Provider has failed to perform its obligations under the Contract. Any such demand shall be conclusive and binding on us notwithstanding any dispute raised by the Service Provider.
2. This guarantee shall remain in full force up to (Contract period plus a claim period of 6 months) and shall stand extended for any extension of the Contract; claims must be received by the Bank on or before expiry of the claim period. Our liability shall not be affected by any change in the constitution of the Service Provider or the Bank, by any indulgence, forbearance or extension granted by IIBF, or by the winding-up/insolvency of the Service Provider.
3. Notwithstanding anything contained herein, our liability is restricted to ₹..... and this guarantee shall expire on, unless a demand is lodged before such expiry.

Signed and sealed for and on behalf of the Bank (with banker's stamp, signature code numbers and witnesses).

Annexure E12 - Bid Submission Compliance Checklist

Service Providers shall complete and place this checklist on top of the Technical Bid. Missing items may render the bid non-responsive.

Sr.	Document	Enclosed (Y/N)	Page no.
1	Covering letter on letterhead, with bid index and page numbering		
2	EMD instrument with Service Provider's letter (E1) / Bank Guarantee (E2) or MSE exemption proof with Bid-Securing Declaration		
3	Service Provider's information and financials (E3) with audited statements and CA certificates (UDIN)		
4	Declaration regarding application software / source-code ownership (E4)		
5	Eligibility Criteria Matrix with all supporting proofs (E5)		
6	Acceptance of RFP terms (E6) and of Scope of Work (E7)		
7	Power of Attorney / Board Resolution (E8)		
8	Other undertakings on stamp paper, notarised (E9)		
9	Signed NDA draft (E10) and signed Integrity Pact (IP)		
10	Technical & functional compliance, Parts A–E (T1)		
11	Experience formats T2-A/B/C with work orders and performance certificates (T2); clean-track declaration (T3); client references (T4)		
12	Project plan (T5) and solution description (T6)		
13	Exam software security declaration (T7)		
14	CERT-In "Safe to Host" certificate; CMMI and ISO certificates		
15	State/city-wise certified venue and node list (per Annexure CTR note)		
16	Commercial Bid (Annexure P1) — in separate sealed envelope only		

Annexure S1 - Catalogue of SOPs and Manuals to be Delivered

Within 21 days of signing the Agreement (Milestone M2), the Service Provider shall deliver, for IIBF approval, documented SOPs/manuals covering at least the following. Each SOP shall specify purpose, scope, roles (RACI), step-by-step procedure, controls and evidence, exception handling, and linked proformas.

SOP No.	Subject
SOP-01	Venue identification, audit-readiness, compliance verification and venue freeze
SOP-02	Mock-day execution: mandatory activities, full-load dry run, node certification, sealing and key custody
SOP-03	Question-bank upload, encrypted distribution, password release and rendering verification
SOP-04	Exam-day operations: gate control, frisking, registration, biometric authentication, seat allocation, session management
SOP-05	Invigilation, bio-break management, de-mapping/re-mapping and time compensation
SOP-06	CCTV operations: installation checks, streaming (RTSP/HLS), recording, labelling and submission
SOP-07	Incident and crisis management: severity matrix, escalation, war-room protocol, safety and evacuation (fire/natural disaster), alternate-venue activation
SOP-08	UFM prevention, detection, evidence handling and FIR filing under the relevant and applicable laws and regulations of the country
SOP-09	Post-exam data consolidation, response transmission, Mandatory Data Set extraction, sanitisation and certification
SOP-10	Data security and access management: encryption, key management, access control, logging and monitoring
SOP-11	Manpower management: recruitment, background verification, Aadhaar authentication (applicable as and when mandated by IIBF in future), training, rotation and No-Relation declarations
SOP-12	Helpdesk and candidate support, including PwD/scribe handling
SOP-13	Business continuity and disaster recovery: DC/DR failover, RTO/RPO drills
SOP-14	Exit management: data handover, knowledge transfer, deletion certification

Annexure T1 - Compliance to Technical & Functional Requirements

The Service Provider shall confirm compliance (Complied / Not Complied / Complied with Customisation, with remarks) against EACH of the following requirements. This annexure will be scored under Sr. 1 of the technical evaluation.

Part A - Test Engine and Candidate Experience

Sr.	Requirement	Compliance
A1	Bilingual/multi-lingual question display (English, Hindi and other Indian languages, IIBF-specified fonts); language switching during exam	
A2	Shuffling of questions and options; automatic randomised QP generation; parameter/rule-based, module-wise papers with sectional timings; group/case-study questions; image-based questions; video-type question capability	
A3	Question without options (numeric key-in) with virtual keyboard, sign/decimal handling and save-prompt behaviour as specified in Section 3	
A4	Candidate details/photo/signature on screen; countdown timer at right-top; summary panel (attempted/unattempted/bookmarked); auto-save; review and auto-submit; controlled early submission; virtual calculator and rough sheet; descriptive-answer typing support	
A5	Auto-stop at expiry of duration WITH automatic compensation of any break/delay/interruption time so every candidate receives the full allotted duration; compensation logs available	
A6	No storage of candidate responses at the node; real-time synchronisation of responses with the local venue server; storage directly at server/cloud	
A7	Response time <1 second per question/page for at least 100 concurrent candidates per venue server; all clicks time-stamped for audit	
A8	Candidate mock-test facility to be given prior to the examination	

Part B - Security, Integrity and Infrastructure

Sr.	Requirement	Compliance
B1	Encryption of QP, responses, biometric data and logs at rest, in transit and in use; secure VPN for QP/candidate-data download; encrypted node-server-DC traffic	
B2	Detection, logging and prevention of unauthorised communication devices (Bluetooth, Wi-Fi, internet, KVM, USB, external drives, dongles, cameras); USB/keyboard/remote-desktop and sensitive ports disabled during exam	
B3	Detection, logging and prevention of network intrusion (foreign traffic from unknown nodes/external network to exam nodes and venue server) and of remote access to candidate computers	
B4	Software-integrity verification (version, executable, randomisation) before use; VLAN segregation of the exam-lab network; blocking of DHCP and peripheral access before exam start	
B5	Strong access controls before/during/after the exam on venue servers and HO/result servers; complete user-access logging (who, what, when) across nodes, servers, switches/routers and HO systems	
B6	Accurate candidate-to-venue/shift/node mapping with logged de-mapping/re-mapping; accurate time management (node time, start/stop, extra time, breaks, PwD compensatory time)	
B7	Post-exam sanitisation of all exam data from venue servers (primary, backup, registration), nodes and HO, with certification; hardware/software inventory of all nodes, servers and network devices	

Sr.	Requirement	Compliance
B8	Venue infrastructure: min. 15-inch monitors, 1024×768 resolution, OEM-supported OS/browser, LAN-based delivery; venue server ≥1.5 GHz CPU, ≥4 GB RAM; backup server per 250 candidates; two independent internet links; UPS/DG backup; jammer-compatible (wired) CCTV	
B9	Tier-III (or higher) primary data centre with DR in a different seismic zone (cloud DC-DR); CCTV feed via media streaming server with cloud copy; dashboards for IIBF command centre incl. functionary allocation, random candidate allocation and node mapping/de-mapping	
B10	Biometric solution: fingerprint + face capture with liveness detection; AI/ML face matching vs admit-card/registration photo; QR-code admit-card scanning; Aadhaar-based authentication capability (with UIDAI audit and compliances) (applicable as and when mandated by IIBF in future); entry/bio-break capture with mismatch reporting	
B11	Handling of network failure between venue and HO or between venue server and candidate node without loss of responses or time; automatic recovery and resumption	
B12	Detection and prevention of malpractice by unscheduled candidates; secure QP preparation/upload workflow as per Section 3.1	

Part C - CCTV, Surveillance and Command Centre

Sr.	Requirement	Compliance
C1	Wired IP CCTV, ≥2 MP, ≥1 camera per 12 candidates per room; full coverage of frisking areas, registration desks, strong rooms, corridors, entry/exit gates, locker areas, parking/driveway/compound; zero blind spots	
C2	Live streaming with centre code, venue name, room number, date-time overlay; media streaming server supporting multiple simultaneous viewers; RTSP/HLS access to IIBF and designated third parties (EMA/auditors)	
C3	Recording retention as mandated by IIBF (one copy on secure cloud); HDD submission mapped per candidate/room within 14 days; sufficient bandwidth and power backup dedicated to CCTV at every venue	
C4	Centralised Monitoring Centre with automated instant alerts (interruptions, idle nodes, unusual activity), live CCTV wall, and trained operators for the full exam window	
C5	IIBF-facing dashboards: real-time candidate status per venue; functionary allocation; random seat allocation; node mapping/de-mapping; incident tickets; SLA counters; with login credentials for IIBF and the EMA	

Part D - Biometric, Registration and Frisking Solution

Sr.	Requirement	Compliance
D1	QR-code scanning of admit card retrieving roll number and verified candidate details; 1 registration desk per 30 candidates plus buffer machine; registration desks not usable as candidate terminals; registration logs preserved	
D2	Fingerprint + face capture with liveness detection; rejection of blurred/partial/multi-face images; white-background, well-lit capture stations with whiteboard backdrop and seating	
D3	AI/ML face matching against admit-card/registration photo with real-time mismatch alerts to IIBF; entry, and bio-break capture with stage-wise mismatch reporting	

Sr.	Requirement	Compliance
D4	Aadhaar-based biometric authentication capability with UIDAI audit (applicable as and when mandated by IIBF in future) and compliances; secure biometric database with encryption and access controls; centre-wise signed summary sheet of biometric-verified candidates	
D5	HHMD-based two-level frisking workflow with gender-segregated enclosures, adequate trained personnel per the staffing norms, plank stands and enclosure infrastructure supplied by the Service Provider	

Part E - Data, Reporting and Integration

Sr.	Requirement	Compliance
E1	Secured ingestion of candidate master (member/registration no., venue, shift, photo, signature) and login credentials issued by IIBF; export of all data in XLS/XML/JSON per IIBF formats	
E2	Click-by-click candidate and server audit logs with timestamps, extractable end-of-day; incident logs per node; seating plans with node IP/MAC; whitelist inventories — the complete Mandatory Data Set of Clause 3.4 & 3.5	
E3	Test-progress push to central server every 10 minutes (configurable); real-time discrepancy reporting (attendance vs seat, biometric mismatch, unscheduled candidates)	
E4	MIS and customised report generation per IIBF requirements; candidate feedback capture with summary reporting; post-exam analytics data (item analysis, response-pattern anomalies) as inputs for IIBF's internal evaluation	
E5	Provisional-scores link generation within 2-3 days; result data to be shared on the secured portal, other exam related data through secure data handover on portable HDD plus link any other data pertaining to pre during and post examination activities.	

Annexure T2 - Service Provider's Experience

Sr.	Project / Client & Location	Nature of exam (CBT)	Candidates handled (largest single day)	Cities / States covered	Period (from-to)	Client contact
1						
2						
3						

Attach work orders and satisfactory-performance certificates for each engagement cited.

T2-A: Details of Similar Work Executed

Sr.	Project & client / sponsoring organisation	Total candidates handled / shifts	Centres / cities / states	Contract start & actual completion	Litigation/arbitration pending	Client officer for reference

T2-B: Details of Work Under Execution or Awarded

Sr.	Project & client / location	Total candidates	Contract commencement & stipulated completion	Up-to-date progress (%)	Slow progress, if any, and reasons	Client reference

T2-C: Performance Report (one per work cited in T2-A/T2-B)

Field	Details
Name of work/project and location; owner/sponsoring organisation with address and contact person	
Agreement number; estimated and contracted cost	
Date of start; stipulated and actual completion dates	
Compensation levied for delayed completion or other damages, if any	
Client's assessment — quality of work (Excellent/Very Good/Good/Fair)	
Client's assessment — resourcefulness (Excellent/Very Good/Good/Fair)	

Annexure T3 - Declaration Regarding Clean Track Record

I have carefully gone through the Terms and Conditions contained in the above referred RFP. I hereby declare that my company is not under a declaration of ineligibility / banned / blacklisted/ debarred by any State or Central Government / Central or State Government Department/Undertaking or any other Government Institutions / Autonomous Bodies currently in India or abroad. I further certify that I am competent officer in my company to make this declaration.

Or

I declare the following

S.No.	Country in which the company is Debarred / blacklisted /case is pending	Blacklisted / debarred by Government / Semi Government organizations/Institutions	Reason	Since when and for how long

NOTE:

1. In case the company was blacklisted previously, please provide the details regarding period for which the company was blacklisted and the reason/s for the same.
2. Any Adverse comments/complaints by any Institution should be mentioned.
3. We understand that suppression of facts shall lead to rejection/termination and forfeiture of EMD/PBG.

Yours faithfully,

(Signature of the Bidder)

Printed Name

Designation

Seal

Annexure T4 - Client Details for Reference

Sr.	Client organisation	Contact person & designation	Phone / E-mail	Services provided & period
1				
2				
3				

IIBF may independently verify performance with the clients listed and otherwise.

Annexure T5 - Project Plan (incl. Contingency, BCP/DR and Exit Plan)

The Service Provider shall describe (max. 30 pages):

1. Mobilisation and transition-in plan with timelines;
2. Venue identification, audit and freeze methodology;
3. Mock-day execution plan covering the five mandatory activities (network sanitisation, node sanitisation, LAN scaping, bandwidth monitoring, load monitoring), sealing and certification;
4. Staffing and training plan with background-verification workflow;
5. Exam-day command-and-control, escalation matrix and incident management;
6. Data management plan mapping every deliverable of Clause 3.4 & 3.5 to its generation, custody and delivery mechanism;
7. Business continuity and disaster recovery (DC/DR architecture, RTO/RPO);
8. Contingency plans for venue failure, power/connectivity failure and candidate shifting, including redundant venues;
9. UFM prevention, detection and FIR-handling process as per the relevant and applicable laws and regulations of the country; and
10. Exit-management and knowledge-transfer plan.

Annexure T6 - Short Description of the Proposed Solution

A concise description (max. 10 pages) of the proposed solution architecture: test-engine overview, deployment model (LAN/netboot), QP encryption and distribution workflow, biometric and frisking solution, CCTV/streaming architecture with RTSP/HLS third-party access, monitoring command centre and dashboards, data-centre/DR setup, and integration approach with IIBF's portal, together with the degree of customisation required for IIBF.

Annexure T7 - Exam Software Security Declaration

(On Service Provider's letterhead, to the Chief Executive Officer, IIBF)

We certify that our exam procedures and software adhere to the following, and that IIBF or its designated agency may test these requirements in a live environment created by us during technical evaluation:

1. We segregate and secure the exam-lab network (switch) before exam start by creating VLANs and blocking unwanted ports/services (DHCP) and peripheral access (USB, storage, KVM, AMT, iLO, virtualisation).
2. Ethics and integrity requirements form part of the contract of all staff (on-roll and contractual) involved in the execution of the exam.
3. On exam day, all user activities (network or physical) on nodes, venue servers and HO/result servers are logged with who/what/when detail: HO server (DB logs), venue server (DB, OS and application logs) and nodes (candidate and OS logs).
4. We provide accurate records of all seats allocated to a candidate (venue, room, seat number, machine identifier) throughout the exam.
5. All communication between HO and venue, and within the venue, is encrypted (QP transfers, data push/pull, server-node and primary-backup traffic), through VPN
6. We maintain inventory hardware and software of all exam-delivery machines (Ethernet cards, processor, RAM, HDD, USB devices, OS, software, services).
7. We understand that any information found incorrect/untrue shall entitle IIBF to summarily reject the bid or terminate the Contract and forfeit the EMD/Performance Guarantee, without prejudice to other rights and remedies.

Annexure T8 - Scope of Independent Audit and its Requirements

The independent audit (by the IIBF-designated auditor) shall cover pre-exam, during-exam and post-exam phases. The Service Provider's obligations and the complete Mandatory Data Set are as detailed in Clause 3.4 & 3.5 of this RFP, which is incorporated herein by reference. Additional requirements:

1. Pre-exam: venue infrastructure audit, mock observation, verification of node certification, CCTV coverage and functionary compliance.
2. During exam: independent observers at venues; live access to CCTV (RTSP/HLS) for specific locations as required by IIBF, dashboards and incident logs.
3. Post-exam: extraction of the Mandatory Data Set in the auditors' presence for validation; facilitation of application-log and system-settings downloads from sample machines and switches; reconciliation of attendance, biometric and response data; and mitigation of all observations to IIBF's satisfaction.

Annexure T9 - Exam-Day Proformas and List of Stationery Items

Stationery per venue/shift (indicative; may vary by examination):

- black ball-point pens (see through/transparent) and A4 rough sheets for candidates (wherever mandated by IIBF and applicable);
- red/blue pens for invigilators/Centre Head;
- non-staining ink stamp pads;
- glue sticks and staplers;
- printed attendance sheets and candidate lists (PDFs provided by IIBF);
- ID cards for all venue staff;
- Envelopes (A4 and full-size) for proformas, attendance sheets and admit cards.

Proformas to be maintained and submitted (formats at Annexure T10):

- (1) Feedback on the examination centre;
- (2) Document handing-over certificate;
- (3) Details of functionaries at the venue;
- (4) No-Relation Certificate of functionaries;
- (5) Certificate of successful activation;
- (6) Attendance sheet and consolidated absentee-cum-attendance statement;
- (7) Record of unfair booked at venue;
- (8) Centre Head's certificate of scrutiny and verification of attendance;
- (9) Certificate of conduct of examination;
- (10) De-mapping and re-mapping record;
- (11) Washroom/bio-break log;
- (12) Certificates of functioning and of temporary shutdown of signal jammer; (applicable as and when mandated by IIBF)
- (13) Certificate of live CCTV feed;
- (14) Certificate on frisking and gender sensitivity;
- (15) Visitor register (mock and exam day);
- (16) Node-certification and venue-sealing certificate;
- (17) Data handing-over-cum-deletion certificate.
- (18) Incident report

Annexure T10 - Formats of Exam-Day Proformas

The following formats shall be used at every venue on the mock day and the examination day, unless modified by IIBF. Completed proformas form part of the post-examination documentation deliverable and the Mandatory Data Set.

Proforma 1 - Feedback on the Examination Centre

Name & designation:

Venue name & code:

City / State:

Date & session(s) observed:

Rate each parameter (S = Satisfactory / U = Unsatisfactory) and record remarks:

Sr.	Parameter observed	S / U	Remarks
1	Venue infrastructure, signage, seating, amenities (drinking water, washrooms, PwD access)		
2	Entry control, admit-card & ID check, two-level frisking (gender-appropriate)		
3	Biometric registration, face-match, random seat allocation		
4	CCTV coverage (no blind spots), live feed, overlays		
5	Invigilation, bio-break/washroom checks, discipline in labs		
6	Server room security, jammers (as and when mandated by IIBF), network lockdown		
7	Adherence to SOP / timeliness of exam start		
8	Incident handling & escalation		

Overall assessment (Excellent / Very Good / Good / Fair / Poor):

Key observations / recommendations:

Signature of authorised personnel

Date

Proforma 2 - Document Handing-Over Certificate

Certified that the following documents pertaining to the IIBF examination held at venue (code ____) on have been handed over to IIBF / IIBF-
authorised representative as per the inventory below, arranged roll-number-wise and duly sealed.

Sr.	Document	No. of pages / envelopes	Remarks
1	Attendance sheets (session-wise)		
2	Admit cards collected on exit		
3	Filled proformas (this Annexure)		
4	Candidate declarations (mismatch / scribe / seat-change)		
5	Rough sheets (with shredding certificate,)wherever mandated and applicable		
6	Any other documents specified by IIBF		

Handed over by

(Service Provider authorised signatory)

Received by (IIBF)

Date

Proforma 3 - Details of Functionaries Deployed at the Venue

Sr.	Name	Role	Employer (SP/sub- contractor)	Photo-ID type & no.	Police verification date	Aadhaar auth. status

Proforma 4 - No-Relation Certificate of Functionaries

I,, deployed as at venue for the IIBF examination dated, hereby declare that none of my near relations (children, brother, sister, nephew, niece of self or spouse), nor any person in whom I have any special interest, is appearing in the said examination at this or any other venue. I understand that a false declaration shall render me liable to removal and legal action.

Signature

Name

Date

Proforma 5 - Certificate of Successful Activation

Certified that at venue (code ____) on, the examination system was successfully activated for session(s): the encrypted question batteries were downloaded to the venue server and decrypted only upon input of the IIBF-authorized password; all scheduled nodes (____) plus buffer nodes (____) were live and functioning; time synchronisation across nodes, servers and CCTV was verified; and the system was ready for candidate login at ____ hrs.

Signatures:

IT Manager

Venue In-charge.

Proforma 6 - Attendance Sheet & Consolidated Absentee-cum-Attendance Statement**6A - Attendance sheet (per room/session):**

Sr.	Membership/Registration number	Candidate name	Room / seat / node	Registered Photo	Date of Birth	Signature	Biometric (entry)

6B - Consolidated absentee-cum-attendance statement (per session):

Session	Candidates scheduled	Present	Absent	Biometrics (entry)	Biometrics (Bio break)	UFM cases
I						
II						
III						

Signatures: Invigilator(s)

Venue In-charge

Proforma 7 – Record of Unfair Means Cases Booked at Venue

Record of unfair means cases booked at venue on

Sr.	Roll number	Candidate name	Session	Nature of unfair means / incident	Time of detection	Material / evidence seized, if any	Action taken	Invigilator signature
-----	-------------	----------------	---------	-----------------------------------	-------------------	------------------------------------	--------------	-----------------------

Signature:

Venue In-charge

Proforma 8 - Centre Head's Certificate of Scrutiny and Verification of Attendance

Certified that I have scrutinised and verified, for venue on:
(a) the session-wise attendance against the biometric entry/exit records and the random seat-allocation logs;
(b) the reconciliation of present/absent candidates; (c) all mismatch, de-mapping and bio-break entries; and
(d) all UFM cases (if any) with supporting evidence. I confirm that the attendance and related records are complete and correct to the best of my verification, and that any discrepancy is separately reported in Proforma 18 / the incident record.

Signature:

Centre Head / Venue In-charge

Name

Date

Proforma 9 - Certificate of Conduct of Examination

Certified that the IIBF examination at venue (code ____) on
was conducted strictly in accordance with the approved SOPs and the RFP requirements. Session details:

Session	Scheduled start	Actual start	Actual end	Candidates present	Incidents (Y/N)
I					
II					
III					

No unauthorised person entered the labs/server room; jammers were operational (if mandated and applicable); CCTV coverage was continuous with no blind spots; and the venue was sealed after the last session. Any exception is recorded in the incident report.

Signatures:

IT Manager

Venue In-charge

Observer

Proforma 10 - De-Mapping and Re-Mapping Record

Sr.	Membership/Registration number	Original node (ID/IP)	New node (ID/IP)	Time of change	Reason	Time compensated & IT Mgr sign

Proforma 11 - Washroom / Bio-Break Log

Sr.	Roll number	Time out	Time in	Escorted by	Biometric re- verification (Y/N, time)	Invigilator signature

Proforma 12 - Certificates of Functioning / Temporary Shutdown of Signal Jammer (applicable as and when mandated by IIBF)

12A: Certified that ____ jammers installed at venue were tested and functional from ____ hrs to ____ hrs on covering all examination labs.

12B: Certified that the jammer(s) at venue were temporarily shut down from ____ to ____ hrs on for the reason with the approval of, and that compensating vigilance measures were deployed during the shutdown.

Signatures:

Jammer operator

Venue In-charge

Observer

Proforma 13 - Certificate of Live CCTV Feed

Certified that at venue, ____ of ____ cameras streamed live to the IIBF monitoring facility (RTSP/HLS) throughout the session(s) on; downtime, if any, is detailed below with room numbers, timings and reasons; recording with centre code, room number, date and time overlay was continuous; and no blind spots existed.

Signatures:

CCTV operator

Venue In-charge.

Proforma 14 - Certificate on Frisking and Gender Sensitivity

Certified that two-level frisking (body tapping and HHMD) was conducted for 100% of candidates and staff at venue on; female candidates were frisked exclusively by female personnel in a three-side covered enclosure under CCTV coverage of the enclosure exterior; ____ ; and no complaint regarding frisking conduct was received / complaints received are annexed.

Signatures:

Security supervisor

Venue In-charge.

Proforma 15 - Visitor Register (Mock Day and Exam Day)

Sr.	Name of visitor	Organisation / purpose	ID verified (type/no.)	Time in	Time out	Authorised by (signature)

Proforma 16 - Node-Certification and Venue-Sealing Certificate

Certified that at venue (code ____), a full-load mock run was conducted on from ____ to ____ hrs on all ____ nodes (including ____ buffer nodes) for the actual examination duration and question-paper size; the five mandatory activities (network sanitisation, node sanitisation, LAN scaping, bandwidth monitoring, load monitoring) were completed; ____ nodes are certified fit for the examination; CCTV coverage was verified with no blind spots; and the examination lab was sealed at ____ hrs, keys retained by

Signatures:

IT Manager,

Venue In-charge,

Observer (if present).

Proforma 17 - Data Handing-Over-cum-Deletion Certificate

Certified that all data pertaining to the IIBF examination held on — response data, biometric data, click-by-click logs, server/firewall logs, CCTV recordings (HDD serial nos.) and the consolidated master file — have been handed over to IIBF on as per the enclosed inventory, and that no copy of candidate data, responses or question papers is retained on any venue server, node or removable media, all of which have been sanitised as per the approved SOP. We acknowledge that any data item not handed over shall attract the consequences of Clause 8.6 and Section 9 of the RFP/Contract.

Signatures: Authorised signatory of the Service Provider; countersigned by IIBF official.

Proforma 18 – Incident Report

Field	Details
Venue / code / room / node	
Date, time of occurrence and time of detection	
Category (technical / power / network / security / UFM / safety / other)	
Description of incident and candidates affected (roll numbers)	
Immediate action taken; time compensated (if any)	
Reported to (IIBF / EMA / police / fire) with time	
Root cause (preliminary) and CAPA proposed	
Signatures: IT Manager / Venue In-charge / Observer	

Annexure T11 - Data Deliverables Dictionary (Formats and Mode)

The table below consolidates the principal data deliverables under this RFP, their formats, frequency and delivery mode. Detailed field-level layouts shall be finalised with the SOPs (Milestone M2). Every deliverable is subject to the absolute data accountability of Clause 8.6.

Sr.	Data deliverable	Format (details as specified by IIBF)	Mode
1	Click-by-click candidate activity log (raw dump, timestamped)	XLS/CSV/Text per IIBF layout	Secure transfer (SFTP/secured portal transfer)
2	Server/IT-Manager activity logs (primary and backup)	XLS/CSV/Text + native logs	Secured portal transfer + HDD
3	Encrypted candidate responses with raw scores data	Encrypted CSV/XLS/XML	Secured portal transfer
4	Biometric registration data, images (candidate and scribe) and face-match report	Images (.jpeg/.jpg) + CSV index	HDD + Secured portal transfer
5	Seating plans (venue, room, seat, node IP/MAC, changes)	XLS/CSV	Secured portal transfer
6	Attendance sheets (scanned), proformas 1–16, functionary attendance	XLS+PDF (non-editable)	Secured portal transfer + originals
7	Incident logs (node/application), firewall and exam-software issue logs	CSV+native	Secured portal transfer
8	Server/node configuration inventory; whitelists (server and node)	XLS/CSV	Secured portal transfer
9	CCTV recordings, room-mapped and labelled	Standard video on HDD	Secured portal transfer + HDD
10	Central-server receipt logs; network connection logs (HO–venue)	CSV/native	Secured portal transfer
11	Mock-day logs and certifications	PDF + CSV	Secured portal transfer
12	Candidate feedback summary; exam-day report	XLS	Secured portal transfer
13	Provisional-scores link	Web link (secured)	Secured portal transfer
14	Post-exam analytics (item analysis, anomaly/forensic reports) as inputs for IIBF's internal evaluation	XLS+PDF	Secured portal transfer
15	UFM case files with evidence (CCTV extracts, biometric comparison, images, logs)	PDF + media/evidence (CCTV extracts, biometric comparison, images, logs)	Secured portal transfer + HDD
16	Consolidated full exam data master file (incl. biometrics)	As specified by IIBF	Portable HDD + secured link
17	Signed read-only copies of all result-related documents of each CBT stage	PDF (non-editable)	Secured portal transfer
18	SLA scorecard and monthly compliance report	XLS/PDF	Secured portal transfer
19	Data handover-cum-deletion certificate (Proforma 1)	Signed PDF	Original + scan

Sr.	Data deliverable	Format (details as specified by IIBF)	Mode
20	Candidate recorded response (CRR)	XLS/CSV/Text	Secured portal transfer
21	Extra time report	XLS	Secured portal transfer

Annexure T12 - Organisation Structure and Personnel to be Deployed

T12-A: Structure of the organisation :

- furnish: legal status with registration particulars;
- names and titles of directors/officers concerned with this work and of individuals authorised to act;
- whether the Service Provider was ever required to suspend work for more than six months continuously after commencement (with project name and reasons); whether the Service Provider or its constituents ever left awarded work incomplete (details);
- whether ever debarred/blacklisted (details); areas of specialisation; and
- any other relevant information.

T12-B: Technical and Administrative Personnel for this Work

Sr.	Category / designation	Total employees in category	Number available for this work	Minimum qualification	Professional experience and role
1	Programme Director / Engagement Head				
2	Exam operations managers / City Heads				
3	IT Managers / server administrators				
4	Software development / QA team				
5	Information security team				
6	Command-centre / monitoring staff				
7	Biometric / registration operations				
8	Helpdesk and candidate support				

Field staff (invigilators, security, frisking, electricians, support staff) shall additionally be mobilised per the staffing norms in Clause 3.2-A(iii) and certified per Proforma 1 for every venue.

Annexure P1 — Commercial Bid / Price Bid Format

(To be submitted ONLY in the separately sealed Commercial Bid envelope. Prices in INR, exclusive of GST, in figures and words. Quoting all line items is mandatory.)

Sr.	Item	Rate (₹)
1	Examination rate per candidate allotted	
2	CCTV live streaming to IIBF (along with RTSP/HLS) (for centres/venues as requested by IIBF)	
	Other items if mandated by IIBF in future	
3	Aadhaar-based authentication (incl. UIDAI audit and compliances) (per candidate) (applicable as and when mandated by IIBF in future)	
4	Jammer installation (per venue)	

1. Rates mentioned in Sr. no. 1 shall only be considered for commercial evaluation, however, IIBF reserves the right to negotiate the rates provided in Sr. no. 2 to 4 with all the vendors
2. Payment shall be on scheduled candidate count at the quoted rates.
3. Rates shall remain the same for the entire Contract period, inclusive of all incidental costs (transport, installation, handling); "node" excludes buffer nodes, for which no extra payment is admissible. In case of discrepancy between figures and words, words shall prevail.

Annexure IP - Pre-Contract Integrity Pact

(To be executed on non-judicial stamp paper of requisite value between IIBF and each Service Provider, and to continue with the successful Service Provider for the Contract term)

This Pre-Contract Integrity Pact ("Pact") is made between the Indian Institute of Banking & Finance, Mumbai (hereinafter "the Principal") of the first part, and M/s (hereinafter "the Service Provider") of the second part, in respect of RFP No. IIBF/EXAM RFP-___/20___ - ___ for selection of Service Provider(s) to conduct CBT examinations (hereinafter "the Procurement").

1. Commitments of the Principal

1. The Principal commits to take all measures necessary to prevent corruption and to observe the following principles: no employee of the Principal will, in connection with the Procurement or the execution of the Contract, demand, take a promise for, or accept, for self or any third person, any material or immaterial benefit which the person is not legally entitled to.
2. The Principal will, during the tender process, treat all Service Providers with equity and fairness, and will provide all Service Providers the same information at the same time; confidential/additional information through which one Service Provider could obtain an advantage will not be provided.
3. The Principal will exclude from the process all known prejudiced persons, and if the Principal obtains information on the conduct of any of its employees which is a criminal offence under the relevant anti-corruption laws of India, or violates these principles, the Principal will inform the appropriate authority and take disciplinary action.

2. Commitments of the Service Provider

The Service Provider commits to take all measures necessary to prevent corruption in connection with the Procurement and during the Contract execution, and in particular commits:

1. Not to offer, promise or give, directly or indirectly, to any employee of the Principal or to any third person, any material or immaterial benefit which the person is not legally entitled to, in order to obtain in exchange any advantage of any kind whatsoever during the tender process or during the execution of the Contract.
2. Not to enter with other Service Providers into any undisclosed agreement or understanding, whether formal or informal, in particular regarding prices, specifications, certifications, subsidiary contracts, submission or non-submission of bids, or any other action to restrict competitiveness or to introduce cartelisation in the bidding process.
3. Not to commit any offence under the relevant anti-corruption laws of India, and not to use, for illegitimate purposes or for purposes of restrictive competition or personal gain, or pass on to others, any information provided by the Principal as part of the business relationship, including information contained or transmitted electronically.
4. To disclose the name and address of agents and representatives, if any, and all payments made to them in connection with this Procurement; foreign Service Providers (if any) to disclose their Indian agents/associates, and Indian Service Providers to disclose their foreign principals or associates.
5. To disclose any transgressions committed over the last five years with any other company in India or abroad that may impinge on the anti-corruption principle.
6. Not to instigate third persons to commit any of the above offences or to be an accessory to such offences, and to ensure that these commitments are equally binding on its sub-contractors and personnel.

3. Disqualification and Exclusion from Future Contracts

If the Service Provider, before award or during execution, has committed a transgression through a violation of Clause 2 above or in any other form that puts its reliability or credibility in question, the Principal is entitled to disqualify the Service Provider from the tender process, terminate the Contract for default, forfeit the EMD/Performance Bank Guarantee, recover all damages, and exclude the Service Provider from future tenders of the Principal for a period of up to five years, without prejudice to criminal action under applicable law where the transgression affects examination integrity.

4. Previous Transgression; Equal Treatment; Sanctions

1. The Service Provider declares that no previous transgression occurred in the last five years with any other public-sector undertaking or government body that could justify its exclusion from tender processes; an incorrect declaration shall be a ground for disqualification/termination.
2. The Service Provider undertakes to demand from all sub-contractors a commitment consistent with this Pact and to submit it to the Principal before Contract signing; the Principal will enter into identical pacts with all Service Providers.
3. For breach of this Pact, in addition to the sanctions above, the Principal may deduct from amounts payable, or claim, liquidated damages equal to 5% of the Contract value, or the undue benefit derived, whichever is higher.

5. Pact Duration and Other Provisions

This Pact begins when both parties have signed it and expires, for the successful Service Provider, 12 months after the last payment under the Contract, and for all other Service Providers, 6 months after the Contract award. This Pact is subject to Indian law; the place of performance and jurisdiction is Mumbai. Changes and supplements must be made in writing. Should one or several provisions of this Pact turn out to be invalid, the remainder remains valid, and the parties will strive to replace the invalid provision with a valid one closest to its original intent. Signed for the Principal and for the Service Provider, with witnesses, date and place.

Annexure C1 - Instructions to Candidates (to accompany the Admit Letter)

The Service Provider shall support IIBF in enforcing the following instructions, which shall be printed with/linked to the admit letter. These instructions also define the exam-day candidate-handling workflow that the Service Provider must implement uniformly at all venues:

1. **Reporting:** Candidates must report at the examination venue at the reporting time printed on the admit letter (at least 60 minutes before the session start). Gates will close 15 minutes before the session start; late arrivals shall not be admitted under any circumstances.
2. **Documents:** Candidates must carry (i) the admit letter with QR code, and (ii) a valid original photo identity document — Aadhaar card / employer's card / PAN card / driving licence / voter ID / passport. Photocopies or images on mobile phones shall not be accepted. Candidates without valid documents shall not be admitted.
3. **Verification:** Each candidate will pass through admit-card and ID verification at the gate, two-level frisking (body tapping followed by hand-held metal detector; separate enclosure with female staff for female candidates), QR-code scanning, photograph capture and biometric registration (fingerprint, and face with liveness detection) at the registration desk, AI/ML enabled face matching of captured photograph with registered photograph, followed by system-generated random seat allotment. Biometrics will again be captured after every bio-break.
4. **Prohibited items:** Mobile phones, smart/digital watches, Bluetooth or any electronic/communication devices, calculators, books, notes, papers, bags, wallets, stationery and any other material not expressly permitted are strictly prohibited inside the examination hall. Candidates are advised not to bring any valuables or prohibited items to the examination hall.
5. **Conduct during exam:** Candidates must occupy only the seat allotted by the system; log in only with the credentials on the admit letter; use only the rough sheet on the screen; not talk to, or exchange anything with, any other candidate; and seek assistance only from the invigilator by raising a hand. Bio-breaks are permitted one candidate at a time per room, with escort, logging and biometric re-verification.
6. **Timer and submission:** The on-screen timer at the right-top corner displays the remaining time; the examination will auto-submit on expiry. candidates should remain seated and follow invigilator instructions during any interruption.
7. **Unfair means:** Impersonation, possession of prohibited items, copying, communication with others, tampering with the computer system, or any conduct defined as unfair means shall render the candidate liable to cancellation of candidature, debarment from IIBF examinations, including filing of FIR if instructed by IIBF.
8. **Exit:** Candidates may leave only after submission of the examination and signing the attendance record as directed. Candidates must follow the emergency-evacuation instructions of venue staff in the event of any emergency. A candidate who leaves the examination before submitting will not be re-admitted to the same session, and the departure will be recorded and reported. Submit button is activated after 1:45 minutes of start of examination, Candidates are not allowed to leave the examination hall before 1:45 minutes of examination.
9. **PwD candidates:** Candidates with benchmark disabilities shall be provided the facilities notified by IIBF as per applicable norms, and other approved assistive support). Requests must follow the process notified in the examination notification.

Annexure D1 - Outline of the Draft Agreement / Contract

The Agreement to be executed with the successful Service Provider on non-judicial stamp paper of requisite value shall be based on this RFP (including all corrigenda), the Service Provider's accepted proposal, and the Letter of Intent, and shall broadly contain the following articles. In case of conflict, the order of precedence shall be: (1) the signed Agreement and its schedules, (2) the SLA, (3) this RFP with corrigenda, (4) the Letter of Intent, and (5) the Service Provider's proposal.

Article	Contents
Recitals & Definitions	Parties, background, definitions and interpretation (aligned to Clause 2.5 of the RFP)
Scope & Term	Scope of services (Section 3 of the RFP incorporated by reference), Contract period of 5 years with annual performance review and an extension option of up to 2 years
Service Levels	The executed SLA as Schedule I, including service credits and governance (Section 7)
Consideration & Payment	Contracted rates (Annexure P1 as accepted), invoicing, deliverable-linked payment, withholding rights (Clause 8.4)
Statutory Compliance	CERT-In/STQC/MeitY certifications; UIDAI audit and compliances (if mandated by IIBF in future); observation of all laws (Clause 8.1)
Data & Confidentiality	Ownership of examination data (Clause 8.3), Processing Norms (Clause 8.2), absolute data accountability (Clause 8.6), NDA (Annexure E10) as Schedule II
Security & Audit	Third-party audit rights, Mandatory Data Set (Clause 3.4 & 3.5), inspection and step-in rights
Personnel	Staffing norms, background verification, No-Relation declarations, rotation, no employer-employee relationship with IIBF
Performance Security	PBG of 10% of estimated annual contract value, validity, extension and invocation
Liability & Indemnity	Penalties/LDs (Section 9), limitation of liability with carve-outs (Clause 8.7), indemnities (Clause 8.14), insurance
Term & Termination	Termination for default/insolvency/convenience, suspension, consequences, exit management and transition (Clause 8.9) as Schedule III
Dispute Resolution	Escalation, arbitration under the Arbitration and Conciliation Act, 1996 (as amended), seat at Mumbai; exclusive jurisdiction of Mumbai courts
Miscellaneous	Force majeure, notices, assignment, waiver, severability, survival, publicity, entire agreement, counterparts
Schedules	I — SLA; II — NDA; III — Exit Management Plan; IV — Accepted Commercial Terms; V — Integrity Pact; VI — SOPs and Proformas (as approved)

Annexure F1 – Details of exam centers owned by Service Provider

Sr. No.	Location	No. of centers owned by Service Provider	No. of nodes
1	Abohar		
2	Adilabad Utnoor		
3	Adoni		
4	Agartala		
5	Agra		
6	Ahmedabad		
7	Ahmednagar		
8	Aizawl		
9	Ajmer		
10	Akola		
11	Aligarh		
12	Allahabad		
13	Alwar		
14	Ambala Cantt		
15	Ambikapur		
16	Amravati		
17	Amritsar		
18	Anantapur		
19	Anantnag		
20	Asansol		
21	Aurangabad		
22	Azamgarh		
23	Bagalkot		
24	Balaghat		
25	Balasore		
26	Ballari		
27	Banaskantha		
28	Banswara		
29	Baramulla		
30	Bardhaman		
31	Bareilly		
32	Barrackpore		
33	Begusarai		
34	Behar		
35	Belagavi		
36	Bengaluru		
37	Berhampur		
38	Betul		
39	Bhagalpur		
40	Bhatinda		
41	Bhavnagar		
42	Bhawanipatna		
43	Bhilai		
44	Bhilwara		
45	Bhopal		

Sr. No.	Location	No. of centers owned by Service Provider	No. of nodes
46	Bhubaneswar		
47	Bhuj		
48	Bidar		
49	Bijapur		
50	Bikaner		
51	Bilaspur Chh		
52	Blair		
53	Bokaro		
54	Bongaigaon		
55	Buldhana		
56	Cachar Silchar		
57	Cantt		
58	Chandigarh		
59	Chandrapur		
60	Chennai		
61	Chh		
62	Chhatarpur		
63	Chhindwara		
64	Chittoor		
65	Coimbatore		
66	Cooch Behar		
67	Cuttack		
68	Daltonganj		
69	Darbhanga		
70	Dehradun		
71	Delhi		
72	Deoghar		
73	Devanagere		
74	Dhanbad		
75	Dharmapuri		
76	Dharwad		
77	Dhubri		
78	Dhule		
79	Dibrugarh		
80	Dichpally		
81	Eluru Godavari		
82	Ernakulam		
83	Erode		
84	Etah		
85	Etawah		
86	Faizabad		
87	Faridabad		
88	Ferozepur		
89	Ganganagar		
90	Gangtok		
91	Gaya		

Sr. No.	Location	No. of centers owned by Service Provider	No. of nodes
92	Ghaziabad		
93	Ghazipur		
94	Godavari		
95	Gonda		
96	Gorakhpur		
97	Gulbarga		
98	Guna		
99	Guntur		
100	Gurugram		
101	Guwahati		
102	Gwalior		
103	Hamirpur		
104	Haridwar		
105	Hasanparthy		
106	Hassan		
107	Hazaribagh		
108	Hindupur		
109	Hoshiarpur		
110	Hp		
111	Hubballi		
112	Hyderabad		
113	Imphal		
114	Indore		
115	Jabalpur		
116	Jagdalpur		
117	Jaipur		
118	Jaisalmer		
119	Jalandhar		
120	Jalgaon		
121	Jammu		
122	Jamnagar		
123	Jamshedpur		
124	Jaunpur		
125	Jhansi		
126	Jodhpur		
127	Jorhat		
128	Junagadh		
129	Kadapa		
130	Kakinada		
131	Kalyan		
132	Kannur		
133	Kanpur		
134	Karimnagar		
135	Karnal		
136	Karur		
137	Kathua		

Sr. No.	Location	No. of centers owned by Service Provider	No. of nodes
138	Khammam		
139	Khandwa		
140	Kharagpur		
141	Khargone		
142	Kohima		
143	Kokrajhar		
144	Kolhapur		
145	Kolkata		
146	Kollam		
147	Koraput		
148	Kota		
149	Kottayam		
150	Kozhikode		
151	Kurnool		
152	Lakhimpur		
153	Latur		
154	Leh		
155	Lucknow		
156	Ludhiana		
157	Madhopur		
158	Madikeri		
159	Madurai		
160	Mahbubnagar		
161	Malda		
162	Mandi		
163	Mangaluru		
164	Mansa		
165	Margao		
166	Meerut		
167	Mehsana		
168	Midnapore		
169	Mira Road		
170	Mokokchung		
171	Moradabad		
172	Motihari		
173	Mp		
174	Mumbai		
175	Muzaffarnagar		
176	Muzaffarpur		
177	Mysuru		
178	Nagaon		
179	Nagercoil		
180	Nagpur		
181	Nainital		
182	Nalgonda		
183	Nanded		

Sr. No.	Location	No. of centers owned by Service Provider	No. of nodes
184	Nandyal		
185	Nashik		
186	Navi Mumbai		
187	Nellore		
188	New Delhi		
189	Nizamabad Dichpally		
190	North Lakhimpur		
191	Ongole Prakasam		
192	Ooty		
193	Palakkad		
194	Palakol		
195	Palampur (Hp		
196	Palampur Banaskantha		
197	Panaji		
198	Parbhani		
199	Pathankot		
200	Patiala		
201	Patna		
202	Poonch		
203	Porbandar		
204	Port Blair		
205	Prakasam		
206	Prayagraj Allahabad		
207	Puducherry		
208	Pune		
209	Purnea		
210	Raichur		
211	Raigarh		
212	Raipur		
213	Rajahmundry		
214	Rajkot		
215	Rajouri		
216	Ranchi		
217	Ratlam		
218	Ratnagiri		
219	Rewa		
220	Road		
221	Rourkela		
222	Sagar Mp		
223	Saharanpur		
224	Saharsa		
225	Sahibganj		
226	Salem		
227	Samastipur		
228	Sambalpur		
229	Sangli		

Sr. No.	Location	No. of centers owned by Service Provider	No. of nodes
230	Sangrur		
231	Sasaram		
232	Satara		
233	Satna		
234	Sawai Madhopur		
235	Secunderabad		
236	Serampore		
237	Shahdol		
238	Shahjahanpur		
239	Shillong		
240	Shimla		
241	Shivamogga		
242	Sikar		
243	Silchar		
244	Siliguri		
245	Solapur		
246	Sri Ganganagar		
247	Srikakulam		
248	Srinagar		
249	Surat		
250	Tezpur		
251	Thane		
252	Thanjavur		
253	Thiruvalla		
254	Thiruvananthapuram		
255	Thrissur		
256	Tinsukia		
257	Tiruchirappalli		
258	Tirunelveli		
259	Tirupati		
260	Tiruppur		
261	Tura		
262	Udaipur		
263	Udhampur		
264	Ujjain		
265	Utnoor		
266	Vadodara		
267	Vapi		
268	Varanasi		
269	Vellore		
270	Vijayawada		
271	Visakhapatnam		
272	Vizianagaram		
273	Warangal Hasanparthy		
274	Wardha		
275	Yamunanagar		

Note: Service provider can add additional location along with details of owned centers here.

Annexure CTR - Indicative Centre/City List

The Institute presently conducts examinations in 254-plus cities across all States and Union Territories. The list below is indicative (drawn from the current examination footprint); the actual list of cities for any examination cycle, with expected candidate counts, shall be notified by IIBF per examination. Service Providers shall furnish, with the Technical Bid, a State/city-wise list of available certified venues and nodes (with counts), duly authenticated by the authorised signatory. IIBF reserves the right to add, delete or change cities and venues.

JAIIB COUNT

SR. NO.	EXAM CENTRE NAME	S1	S2	S3	S4
1	ABOHAR	111	93	94	90
2	UTNOOR	147	129	129	115
3	ADONI	77	67	69	64
4	AGARTALA	288	238	264	227
5	AGRA	641	545	583	548
6	AHMEDABAD	1410	1182	1259	1110
7	AHMEDNAGAR	213	183	190	167
8	AIZAWL	122	101	118	103
9	AJMER	197	168	180	160
10	AKOLA	221	181	199	181
11	ALIGARH	290	238	265	237
12	ALWAR	201	169	180	169
13	CANTT	152	123	136	118
14	AMBIKAPUR	183	153	166	139
15	AMRAVATI	248	205	226	194
16	AMRITSAR	314	263	279	253
17	ANANTAPUR	338	290	312	278
18	ANANTNAG	94	73	81	73
19	ASANSOL	251	207	227	189
20	AURANGABAD	480	403	448	399
21	AZAMGARH	183	151	166	142
22	BAGALKOT	209	173	179	177
23	BALAGHAT	88	73	82	73
24	BALASORE	280	237	262	206
25	BALLARI	221	185	203	171
26	BANSWARA	110	97	100	93
27	BARAMULLA	117	99	107	99
28	BARDHAMAN	260	225	238	203
29	BAREILLY	474	408	439	403
30	BARRACKPORE	345	300	315	274
31	BEGUSARAI	113	96	103	92
32	BELAGAVI	264	230	243	206
33	BENGALURU	2088	1713	1896	1643
34	BERHAMPUR	220	190	203	177
35	BETUL	76	64	74	61
36	BHAGALPUR	241	222	224	219
37	BHATINDA	316	271	272	251
38	BHAVNAGAR	218	173	200	164
39	BHAWANIPATNA	93	80	89	68

SR. NO.	EXAM CENTRE NAME	S1	S2	S3	S4
40	BHILAI	241	192	214	182
41	BHILWARA	149	115	131	115
42	BHOPAL	823	655	742	648
43	BHUBANESHWAR	946	752	848	708
44	BHUJ	174	148	149	133
45	BIDAR	123	100	112	94
46	BIJAPUR	212	178	198	171
47	BIKANER	264	240	253	230
48	CHH	318	276	299	265
49	BOKARO	153	134	143	128
50	BONGAIGAON	95	73	88	77
51	BULDHANA	82	71	81	67
52	SILCHAR	173	138	154	132
53	CHANDIGARH	760	618	680	592
54	CHANDRAPUR	127	96	112	90
55	CHENNAI	1972	1593	1746	1525
56	CHHATARPUR	117	94	111	92
57	CHHINDWARA	141	126	137	115
58	CHITTOOR	173	149	162	136
59	COIMBATORE	621	506	548	461
60	BEHAR	141	117	129	105
61	CUTTACK	202	171	176	163
62	DALTONGANJ	121	109	114	109
63	DARBHANGA	252	209	234	226
64	DEHRADUN	606	514	557	485
65	DEOGHAR	243	216	221	210
66	DEVANAGERE	309	261	289	255
67	DHANBAD	199	165	178	158
68	DHARMAPURI	287	242	274	232
69	DHARWAD	96	84	85	83
70	DHUBRI	26	19	22	21
71	DHULE	158	119	144	118
72	DIBRUGARH	139	110	119	107
73	GODAVARI	164	134	146	129
74	ERNAKULAM	881	642	731	622
75	ERODE	291	237	262	227
76	ETAH	142	111	121	103
77	ETAWAH	193	161	171	159
78	FAIZABAD	255	200	227	199
79	FARIDABAD	284	221	246	219
80	FEROZEPUR	74	64	67	56
81	GANGTOK	49	39	41	34
82	GAYA	192	150	178	149
83	GHAZIABAD	571	471	518	456
84	GHAZIPUR	172	145	156	141
85	GONDA	309	273	291	255
86	GORAKHPUR	702	607	668	595

SR. NO.	EXAM CENTRE NAME	S1	S2	S3	S4
87	GULBARGA	245	214	227	207
88	GUNA	116	93	103	84
89	GUNTUR	537	452	485	437
90	GURUGRAM	609	502	557	491
91	GUWAHATI	647	541	597	517
92	GWALIOR	338	284	327	275
93	HAMIRPUR	189	161	174	155
94	HARIDWAR	150	116	128	111
95	HASSAN	278	237	254	222
96	HAZARIBAGH	131	119	123	108
97	HINDUPUR	130	114	122	111
98	HOSHIARPUR	126	111	119	97
99	HUBBALLI	475	389	423	378
100	HYDERABAD	1815	1488	1656	1423
101	IMPHAL	111	85	98	89
102	INDORE	594	476	538	475
103	JABALPUR	429	345	395	332
104	JAGDALPUR	136	113	123	110
105	JAIPUR	1003	853	913	829
106	JAISALMER	60	46	51	47
107	JALANDHAR	380	331	337	316
108	JALGAON	228	191	205	185
109	JAMMU	654	537	602	520
110	JAMNAGAR	136	113	130	112
111	JAMSHEDPUR	251	205	231	208
112	JAUNPUR	128	108	124	106
113	JHANSI	331	278	316	272
114	JODHPUR	482	414	432	410
115	JORHAT	205	179	196	173
116	JUNAGADH	213	182	188	173
117	KADAPA	321	267	298	270
118	KAKINADA	208	178	200	172
119	KALYAN	397	335	355	315
120	KANNUR	276	226	240	215
121	KANPUR	827	696	751	666
122	KARIMNAGAR	728	601	679	575
123	KARNAL	374	308	340	316
124	KARUR	148	117	126	98
125	KATHUA	99	86	89	79
126	KHAMMAM	434	369	415	368
127	KHANDWA	138	109	121	108
128	KHARAGPUR	194	155	178	157
129	KHARGONE	52	46	48	45
130	KOHIMA	56	53	55	48
131	KOKRAJHAR	30	24	27	27
132	KOLHAPUR	348	276	312	266
133	KOLKATA	1461	1225	1329	1157

SR. NO.	EXAM CENTRE NAME	S1	S2	S3	S4
134	KOLLAM	339	261	313	263
135	KORAPUT	107	78	91	80
136	KOTA	415	364	389	367
137	KOTTAYAM	363	262	308	256
138	KOZHIKODE	489	369	428	366
139	KURNOOL	228	198	215	183
140	LATUR	223	169	203	180
141	LEH	59	51	55	47
142	LUCKNOW	1487	1219	1360	1201
143	LUDHIANA	310	251	280	248
144	MADIKERI	65	53	55	49
145	MADURAI	956	777	849	751
146	MAHBUBNAGAR	253	207	238	196
147	MALDA	304	259	283	245
148	MANDI	210	177	199	168
149	MANGALURU	612	483	529	472
150	MANSA	80	68	71	69
151	MARGAO	166	133	151	120
152	MEERUT	370	303	345	292
153	MEHSANA	176	167	160	149
154	MIDNAPORE	123	103	106	104
155	Road	258	202	224	192
156	MOKOKCHUNG	18	13	15	12
157	MORADABAD	512	433	468	420
158	MOTIHARI	200	170	190	172
159	MUMBAI	2006	1635	1787	1574
160	MUZAFFARNAGAR	182	149	163	144
161	MUZAFFARPUR	348	301	329	284
162	MYSURU	500	430	466	423
163	NAGAON	115	96	108	96
164	NAGERCOIL	228	176	205	162
165	NAGPUR	739	629	691	604
166	NAINITAL	403	335	371	324
167	NALGONDA	245	205	229	197
168	NANDED	222	185	211	190
169	NANDYAL	130	105	118	96
170	NASHIK	416	347	380	313
171	MUMBAI	1225	956	1112	945
172	NELLORE	275	223	257	222
173	DELHI	2017	1706	1819	1635
174	DICHPALLY	438	368	409	358
175	LAKHIMPUR	113	96	107	92
176	PRAKASAM	286	234	270	227
177	OOTY	46	40	43	36
178	PALAKKAD	256	202	218	185
179	PALAKOL	124	100	103	83
180	HP	186	164	178	155

SR. NO.	EXAM CENTRE NAME	S1	S2	S3	S4
181	BANASKANTHA	175	146	157	147
182	PANAJI	239	196	216	176
183	PARBHANI	114	88	104	90
184	PATHANKOT	228	194	204	180
185	PATIALA	153	135	134	130
186	PATNA	1300	1124	1236	1103
187	POONCH	33	28	29	28
188	PORBANDAR	80	59	74	57
189	BLAIR	39	31	36	31
190	ALLAHABAD	490	413	451	387
191	PUDUCHERRY	483	374	434	364
192	PUNE	1336	1125	1153	1051
193	PURNEA	262	224	238	226
194	RAICHUR	174	149	161	151
195	RAIGARH	97	80	84	76
196	RAIPUR	471	377	430	372
197	RAJAHMUNDRY	329	276	297	258
198	RAJKOT	439	353	382	335
199	RAJOURI	26	23	26	25
200	RANCHI	571	474	511	445
201	Ratlam	150	115	130	114
202	RATNAGIRI	127	104	118	101
203	REWA	152	113	139	122
204	ROURKELA	128	107	115	90
205	MP	169	146	155	138
206	SAHARANPUR	123	101	106	105
207	SAHARSA	76	67	72	66
208	SAHIBGANJ	35	33	33	31
209	SALEM	500	403	464	386
210	SAMASTIPUR	112	105	106	98
211	SAMBALPUR	301	247	276	230
212	SANGLI	189	160	171	143
213	SANGRUR	98	82	87	79
214	SASARAM	124	100	113	103
215	SATARA	173	135	155	141
216	SATNA	132	102	119	102
217	MADHOPUR	101	93	94	92
218	SECUNDERABAD	493	384	423	360
219	SERAMPORE	210	159	172	147
220	SHAHDOL	150	122	127	110
221	SHAHJAHANPUR	213	177	192	165
222	SHILLONG	110	90	100	87
223	SHIMLA	378	339	362	321
224	SHIVAMOGGA	262	215	252	211
225	SIKAR	345	282	314	286
226	SILIGURI	349	294	312	271
227	SOLAPUR	314	270	293	260

SR. NO.	EXAM CENTRE NAME	S1	S2	S3	S4
228	GANGANAGAR	281	260	268	248
229	SRIKAKULAM	214	181	200	176
230	SRINAGAR	360	299	321	308
231	SURAT	681	562	582	534
232	TEZPUR	115	100	110	90
233	THANE	458	382	391	348
234	THANJAVUR	507	416	463	398
235	THIRUVALLA	244	172	197	172
236	THIRUVANANTHAPURAM	475	366	416	373
237	THRISSUR	440	348	381	335
238	TINSUKIA	108	91	96	81
239	TIRUCHIRAPPALLI	553	435	507	427
240	TIRUNELVELI	458	396	431	370
241	TIRUPATI	308	263	279	242
242	TIRUPPUR	209	147	173	151
243	TURA	33	25	26	27
244	UDAIPUR	346	296	303	294
245	UDHAMPUR	77	66	71	64
246	UJJAIN	196	153	184	151
247	VADODARA	835	712	771	669
248	VAPI	151	131	140	121
249	VARANASI	673	579	628	561
250	VELLORE	428	339	387	321
251	VIJAYAWADA	755	650	703	604
252	VISAKHAPATNAM	469	393	423	374
253	VIZIANAGARAM	260	201	221	203
254	HASANPARTHY	442	378	410	366
255	WARDHA	96	84	95	71
256	YAMUNANAGAR	122	109	114	111
	Total	85,504	70,791	77,557	68,096

CAIIB Count

Sr. No.	EXAM CENTRE NAME	S1	S2	S3	S4	S5
1	ADILABAD UTNOOR	47	56	50	40	45
2	ADONI	28	33	30	27	27
3	ANANTAPUR	106	154	136	109	116
4	CHITTOOR	61	75	69	52	64
5	KADAPA	142	181	167	139	145
6	ELURU GODAVARI	67	82	73	59	66
7	GUNTUR	230	311	275	234	235
8	HINDUPUR	51	65	57	47	48
9	HYDERABAD	865	1100	965	836	861
10	KAKINADA	126	174	154	134	134
11	KARIMNAGAR	251	330	274	231	244
12	KHAMMAM	170	212	195	154	169

Sr. No.	EXAM CENTRE NAME	S1	S2	S3	S4	S5
13	KURNOOL	111	149	120	111	106
14	MAHBUBNAGAR	79	101	93	80	76
15	NALGONDA	71	100	83	67	72
16	NANDYAL	47	57	50	45	46
17	NELLORE	122	154	133	116	118
18	NIZAMABAD DICHPALLY	157	198	177	146	149
19	ONGOLE PRAKASAM	141	164	156	133	146
20	PALAKOL	78	99	88	76	83
21	RAJAHMUNDRY	160	211	189	155	164
22	SECUNDERABAD	318	428	368	299	295
23	SRIKAKULAM	110	143	123	99	112
24	TIRUPATI	120	176	145	117	121
25	VIJAYAWADA	352	500	423	347	350
26	VISAKHAPATNAM	298	399	339	297	306
27	VIZIANAGARAM	133	170	148	126	137
28	WARANGAL HASANPARTHY	164	215	182	150	160
29	DHUBRI	6	8	7	7	7
30	DIBRUGARH	64	79	70	71	66
31	GUWAHATI	245	336	276	251	246
32	JORHAT	70	84	74	69	69
33	KOKRAJHAR	6	7	7	6	6
34	NORTH LAKHIMPUR	37	54	43	38	36
35	NAGAON	28	36	29	25	24
36	CACHAR SILCHAR	61	84	74	68	65
37	TEZPUR	39	50	42	37	36
38	TINSUKIA	36	50	41	34	34
39	BONGAIGAON	29	34	31	29	29
40	BEGUSARAI	44	62	53	46	40
41	BHAGALPUR	103	134	119	94	103
42	BOKARO	85	112	97	92	84
43	DALTONGANJ	40	46	44	37	39
44	DARBHANGA	106	141	122	111	118
45	DHANBAD	95	111	95	86	93
46	HAZARIBAGH	56	69	65	57	56
47	JAMSHEDPUR	139	173	147	129	134
48	MUZAFFARPUR	184	224	209	171	182
49	PATNA	627	788	681	607	623
50	PURNEA	113	139	125	109	110
51	RANCHI	240	296	252	230	233
52	SAHARSA	46	54	45	41	43
53	SAMASTIPUR	48	67	60	49	49
54	SASARAM	58	77	67	53	57
55	DEOGHAR	96	119	103	95	92
56	MOTIHARI	73	83	71	59	64
57	SAHIBGANJ	14	15	15	13	12
58	AHMEDABAD	706	922	770	689	691

Sr. No.	EXAM CENTRE NAME	S1	S2	S3	S4	S5
59	VADODARA	387	525	424	362	370
60	BHAVNAGAR	87	122	93	85	83
61	BHUJ	72	90	79	69	68
62	JAMNAGAR	34	44	38	33	32
63	JUNAGADH	91	110	97	84	85
64	MEHSANA	58	67	59	54	55
65	PALANPUR BANASKANTHA	47	59	58	45	47
66	PORBANDAR	16	20	17	17	16
67	RAJKOT	192	259	217	175	181
68	SURAT	255	334	284	257	265
69	AMBALA CANTT	88	112	91	76	84
70	FARIDABAD	98	142	106	94	98
71	GURUGRAM	373	503	415	360	377
72	KARNAL	185	244	199	168	179
73	YAMUNANAGAR	54	63	55	49	53
74	HAMIRPUR	79	106	88	74	77
75	MANDI	78	94	86	79	80
76	PALAMPUR (HP	83	103	93	85	84
77	SHIMLA	135	185	157	139	142
78	ANANTNAG	48	59	53	46	49
79	BARAMULLA	47	55	51	47	50
80	JAMMU	277	373	310	270	266
81	KATHUA	48	66	60	51	47
82	LEH	22	26	24	23	23
83	POONCH	28	30	28	28	27
84	RAJOURI	11	12	10	8	9
85	SRINAGAR	145	197	162	153	145
86	UDHAMPUR	32	40	31	28	30
87	BAGALKOT	97	113	98	89	90
88	BENGALURU	1143	1516	1291	1138	1135
89	BELAGAVI	67	95	83	67	64
90	BALLARI	97	114	103	87	88
91	BIDAR	36	43	39	33	35
92	BIJAPUR	52	76	61	48	53
93	DEVANAGERE	96	126	110	92	90
94	DHARWAD	34	47	41	30	30
95	GULBARGA	97	116	99	84	88
96	HASSAN	88	113	103	79	83
97	HUBBALLI	144	191	158	143	137
98	MADIKERI	28	39	34	30	25
99	MANGALURU	318	431	371	305	321
100	MYSURU	195	251	225	191	191
101	RAICHUR	67	92	78	64	64
102	SHIVAMOGGA	97	127	104	91	89
103	KOZHIKODE	223	301	252	220	221
104	KANNUR	121	153	131	116	116

Sr. No.	EXAM CENTRE NAME	S1	S2	S3	S4	S5
105	ERNAKULAM	434	592	474	437	427
106	KOTTAYAM	149	206	172	150	147
107	PALAKKAD	128	166	141	127	123
108	KOLLAM	161	206	184	169	161
109	THIRUVALLA	122	161	140	113	112
110	THRISSUR	252	330	294	251	253
111	THIRUVANANTHAPURAM	290	386	335	307	297
112	AMBIKAPUR	90	107	96	82	88
113	BALAGHAT	24	36	28	22	24
114	BHILAI	133	152	132	119	118
115	BHOPAL	398	545	455	401	396
116	BILASPUR CHH	136	174	144	125	131
117	CHHATARPUR	40	49	45	36	38
118	CHHINDWARA	64	79	71	56	60
119	GUNA	45	66	53	46	43
120	GWALIOR	158	211	186	168	160
121	INDORE	241	327	270	241	233
122	JABALPUR	200	260	229	194	192
123	JAGDALPUR	41	54	50	46	47
124	KHANDWA	60	80	67	60	59
125	KHARGONE	23	28	25	22	22
126	RAIGARH	31	44	38	32	36
127	RAIPUR	213	306	251	222	220
128	Ratlam	84	105	95	80	82
129	REWA	82	95	84	77	82
130	SAGAR MP	76	93	84	77	75
131	SATNA	51	66	54	49	51
132	SHAHNOL	52	65	54	47	53
133	UJJAIN	71	91	76	65	67
134	BETUL	31	33	31	28	28
135	AHMEDNAGAR	66	87	72	63	66
136	AKOLA	59	77	68	56	57
137	AMRAVATI	102	133	118	107	103
138	AURANGABAD	184	241	207	169	179
139	MUMBAI	1146	1478	1248	1117	1109
140	BULDHANA	21	29	27	18	16
141	CHANDRAPUR	48	59	47	43	42
142	DHULE	66	76	65	63	61
143	JALGAON	73	92	83	64	70
144	KALYAN	145	186	152	133	125
145	KOLHAPUR	112	152	120	110	109
146	LATUR	78	104	89	77	77
147	NAGPUR	360	468	386	336	338
148	NANDED	76	87	79	72	73
149	NASHIK	155	217	186	152	146
150	PARBHANI	56	78	64	57	59
151	PUNE	540	713	593	527	509

Sr. No.	EXAM CENTRE NAME	S1	S2	S3	S4	S5
152	RATNAGIRI	43	50	46	43	43
153	SANGLI	59	73	65	49	55
154	SATARA	64	80	69	64	63
155	SOLAPUR	116	155	123	107	104
156	THANE	249	314	255	233	221
157	WARDHA	51	65	52	43	50
158	NAVI MUMBAI	748	1012	843	751	709
159	IMPHAL	50	64	50	47	47
160	SHILLONG	20	38	24	23	20
161	TURA	10	11	10	8	9
162	AIZAWL	18	28	20	18	19
163	KOHIMA	18	20	19	18	15
164	MOKOKCHUNG	4	5	5	4	4
165	BALASORE	90	126	115	91	96
166	BERHAMPUR	81	115	105	84	90
167	BHAWANIPATNA	44	59	48	41	44
168	BHUBANESHWAR	478	646	531	467	461
169	CUTTACK	110	147	123	105	113
170	KORAPUT	45	55	50	48	44
171	ROURKELA	44	66	50	43	45
172	SAMBALPUR	112	151	129	111	113
173	ABOHAR	53	65	59	47	48
174	AMRITSAR	135	167	140	129	127
175	BHATINDA	149	198	170	144	152
176	FEROZEPUR	47	58	51	47	48
177	HOSHIARPUR	51	64	56	45	46
178	JALANDHAR	183	226	197	169	161
179	LUDHIANA	156	216	179	146	153
180	MANSA	73	95	84	73	79
181	PATHANKOT	88	112	95	85	80
182	PATIALA	90	115	100	88	90
183	SANGRUR	62	83	65	66	57
184	AJMER	100	129	114	97	97
185	ALWAR	94	122	104	95	91
186	BANSWARA	25	35	29	23	24
187	BHILWARA	81	105	90	83	81
188	BIKANER	131	149	135	127	130
189	SRI GANGANAGAR	126	171	139	127	125
190	JAIPUR	579	731	620	551	579
191	JAISALMER	30	33	29	24	24
192	JODHPUR	247	293	261	238	240
193	KOTA	195	237	219	199	190
194	SAWAI MADHOPUR	45	50	45	42	42
195	SIKAR	169	210	182	154	168
196	UDAIPUR	133	175	149	133	123
197	GANGTOK	16	23	17	18	16
198	COIMBATORE	263	382	313	263	260

Sr. No.	EXAM CENTRE NAME	S1	S2	S3	S4	S5
199	DHARMAPURI	76	100	84	72	73
200	ERODE	122	162	140	118	120
201	KARUR	84	121	97	79	83
202	CHENNAI	999	1229	1112	959	950
203	MADURAI	426	537	459	408	411
204	NAGERCOIL	103	146	118	96	103
205	OOTY	14	22	20	12	16
206	SALEM	196	262	220	183	187
207	THANJAVUR	139	186	167	140	139
208	TIRUCHIRAPPALLI	241	326	279	233	245
209	TIRUNELVELI	237	300	263	221	239
210	TIRUPPUR	103	137	109	94	96
211	VELLORE	132	166	143	127	131
212	AGARTALA	121	151	128	112	121
213	AGRA	300	422	345	307	306
214	ALIGARH	123	157	133	112	117
215	PRAYAGRAJ ALLAHABAD	226	314	259	233	233
216	AZAMGARH	91	119	102	92	95
217	BAREILLY	194	265	221	191	190
218	DEHRADUN	291	384	325	288	290
219	ETAH	31	45	42	33	33
220	ETAWAH	62	77	66	59	60
221	FAIZABAD	110	138	115	107	99
222	GHAZIABAD	292	393	330	287	299
223	GHAZIPUR	86	105	94	84	84
224	GONDA	100	126	112	99	97
225	GORAKHPUR	274	367	299	270	261
226	HARIDWAR	57	78	65	57	54
227	JAUNPUR	47	55	49	44	44
228	JHANSI	97	142	115	96	98
229	KANPUR	349	465	382	344	341
230	LUCKNOW	795	1028	884	781	768
231	MEERUT	171	229	194	166	172
232	MORADABAD	184	237	219	189	193
233	MUZAFFARNAGAR	73	99	80	70	76
234	NAINITAL	169	226	188	174	169
235	SAHARANPUR	47	62	53	45	43
236	SHAHJAHANPUR	113	137	119	110	111
237	VARANASI	318	406	353	315	324
238	ASANSOL	147	190	161	143	145
239	BARRACKPORE	135	200	157	137	136
240	BARDHAMAN	114	149	125	114	114
241	KOLKATA	783	1019	869	774	768
242	COOCH BEHAR	47	61	49	45	47
243	MALDA	100	131	123	105	107
244	MIDNAPORE	55	73	59	53	52

Sr. No.	EXAM CENTRE NAME	S1	S2	S3	S4	S5
245	SERAMPORE	127	162	137	121	114
246	SILIGURI	145	194	165	137	143
247	PORT BLAIR	17	21	19	18	16
248	CHANDIGARH	497	661	540	484	478
249	NEW DELHI	1201	1642	1353	1208	1215
250	MARGAO	59	92	72	59	59
251	PANAJI	115	142	120	103	105
252	PUDUCHERRY	170	205	189	167	164
253	VAPI	57	64	60	52	56
254	GAYA	98	131	117	96	102
255	KHARAGPUR	52	80	68	59	57
256	Mira Road	117	171	133	117	112
	Total	38,740	50,698	43,197	37,718	37,999