ANNEX A: PROPOSAL

Project Name:

RFP.TDT.2025.0006

Provision of Professional Services, Cloud Hosting Subscription, Support and Maintenance Services for the Implementation of AI Agents for Transformation of IBF Training Programme Accreditation

Name of Corporate Entity:

For Internal (IBF) Use only

Date Received:

Officer-in-charge:

USEFUL NOTES

(A) Submission of Proposal

To assist us in reviewing your proposal in the shortest time possible, please provide the requested information completely and accurately. If the space provided is insufficient, a separate sheet may be used. Where information is not yet available or not applicable, please indicate accordingly.

You are advised to contact us should you have any difficulties in completing the form or if you need any further information.

All proposals must be clearly marked as **"Implementation of AI Agents for Transformation of IBF Training Programme Accreditation (RFP.TDT.2025.0006)",** and addressed to:

The Institute of Banking & Finance
10 Shenton Way
#13-07/08, MAS Building
Singapore 079117
Email: procurement@ibf.org.sg

(B) Structure of the Proposal

The complete proposal consists of 6 parts:

Part I – Company Data

Part II – Details of Proposed Project

Part III – Project Costs & Fees

Part IV – References / Other Considerations

Part V – Non-disclosure and Undertaking (Third Parties)

Part VI – IBF IT Service Provider Checklist

(C) IBF reserves the right to conduct interviews and on-site visits during the review of the proposal.

(D) The Company in submitting this proposal undertakes not to divulge or communicate to any person or party any confidential information, including but not limited to any documents that may be forwarded from IBF to you subsequently, without having first obtained the written consent of IBF.

PART I – COMPANY DATA

1. GENERAL

(a) Company Name: _____

(b) Mailing Address: _____

2. OWNERSHIP: Information on Paid-Up Share Capital & Shareholders

3. CLIENTELE LIST

Please provide a list of your company's key clients. with at least two contactable client references for feedback on services delivered for related past projects.

4. SIGNIFICANT ACHIEVEMENTS, AWARDS & CERTIFICATIONS (where applicable)

Please indicate significant achievements, awards and certifications received by company or staff.

5. SUPPORTING DOCUMENTS REQUIRED

a) A copy of the latest updated ACRA search.

b) Full set of the latest audited financial / management report for the last 1 year.

c) Include CVs of key project personnel

d) Any other relevant reports or information available.

PART II – DETAILS OF PROPOSED PROJECT

A) Functional and Non-functional Specifications

S/No.	Specifications	Ability to Deliver (Yes / No)	If yes, please provide brief description and state any other relevant details	If no, please state reasons and proposed variations or alternatives
1.	**Requirements Gathering**			
1.1	Conduct user requirements gathering			
1.2	Develop a detailed project scope document outlining the AI Agents' functionalities and features			
1.3	Design user-friendly interfaces based on solicitation of user feedback and open dialog.			
1.4	Gather user feedback that provides impetus to the continuous improvement of the AI Agents.			
1.5	Institutionalise change management to manage any impact to people, processes and systems and provision for user education/training.			
2.	**Functional Requirements**			
2.1	Level 1 screening and sanity check for IBF Course Accreditation: (1) **Automate data preprocessing:** The AI Agent shall remove manual steps where IBF officers download application forms and supporting documents from the SSG-Training Partner Gateway (TPG) and email them to their IBF staff addresses for processing. The process shall be fully automated with zero manual handling of downloaded files. (2) **Automate file categorisation and renaming:** The AI Agent shall automatically categorise and			

S/No.	Specifications	Ability to Deliver (Yes / No)	If yes, please provide brief description and state any other relevant details	If no, please state reasons and proposed variations or alternatives
	rename application documents based on their contents, handling variations in file naming conventions used by TPs (e.g., "Lesson Plan" labelled as "Course Outline" or "Course Prospectus"). The system shall: (i)Correctly classify at least 95% of documents into the appropriate categories. (ii)Process multiple file formats, including PDF, Word, Excel, PowerPoint, and image files. (3) **Automate document completeness and coherence checks:** The AI Agent shall check each submission against the application document checklist and verify that information in the documents is coherent and consistent with the data declared in the application form. (4) **Automate content integrity screening:** The AI Agent shall: (i)Check for completeness of required information. (ii)Identify prohibited words or content. (iii)Verify authenticity and credibility of cited sources. (iv)Flag missing, misleading, or unacceptable information. (5) **Automate email notifications:** The AI Agent shall detect missing or contradictory information and generate a first-draft email to the TP, including: (i)Requests for missing documents. (ii)Notifications of contradictory, misleading, or non-credible content.			

S/No.	Specifications	Ability to Deliver (Yes / No)	If yes, please provide brief description and state any other relevant details	If no, please state reasons and proposed variations or alternatives
	(ii)Plagiarism violations based on external reference checks. (iii)Draft emails shall be available for human review before sending. (6) **Structured data conversion and pre-filling:** The AI Agent shall: (i)Extract application form data (including PDF formats) into a structured dataset for record-keeping in Excel. (ii)Autofill the internal reviewer checklist using relevant extracted content. (iii)Generate a summarised version of all documents. (iv)Auto-tagging of extracted content to support Level 2 checks.			
2.2	Level 2 screening and qualitative assessment: (1) **Automate Adult Educator (AE) CV verification:** The AI Agent shall automatically verify CVs of AEs assigned to the programme, ensuring that: (i)Assigned AEs on TPG have the required supporting documents. (ii)Supporting documents are consistent with the AE's assigned role(s). (iii)AEs meet IBF's requirements based on CVs, mapped against relevant funding schemes and (iv)A complete list of all applications previously assigned to the AE is available. (2) **Automate ITM and Skills Framework verification:** The AI Agent shall verify that the selected Industry Transformation Map (ITM) (e.g., Cluster: Modern Services; Sector: Financial Services; Sub-sector: Financial			

S/No.	Specifications	Ability to Deliver (Yes / No)	If yes, please provide brief description and state any other relevant details	If no, please state reasons and proposed variations or alternatives
	Services) in the application form is accurately referenced and exists within the Skills Framework for Financial Services (FS SFw). (3) **TSC and job role alignment:** The AI Agent shall: (i)Validate that the Technical Skills Competency (TSC) specified in the application exists in the FS SFw. (ii)Confirm alignment between the TSC and the selected job role. (iii)Verify that the course content aligns with the TSCs linked to the job role. (4) **Automate course content suitability assessment:** The AI Agent shall assess whether: (i)course title accurately reflects the course coverage. (ii)training content is relevant and contextualised to the Financial Services sector. (iii)The content is relevant to the identified job role(s). (5) **Knowledge and Abilities alignment:** Based on the TSC(s) declared by the TP, the AI Agent shall: (i)Identify content in the training and assessment materials that aligns with the Knowledge and Abilities statements of the specified TSC(s). (ii)Provide reasoning for the mapping, supported by explicit evidence references. (iii)Assess the degree of alignment of the courseware. (6) **Skills Competency Checklist verification:** The AI Agent shall be able to:			

S/No.	Specifications	Ability to Deliver (Yes / No)	If yes, please provide brief description and state any other relevant details	If no, please state reasons and proposed variations or alternatives
	(i)Use the mapping table ("Skills Competency Checklist") submitted by the TP to verify mapping (ii)Provide justification for validity or invalidity, with references to explicit evidence in the courseware. (7) **Gap analysis and reporting:** Following mapping and alignment evaluation, the AI Agent shall generate a gap analysis document detailing issues for TP follow-up. (8) **Questions generation:** The AI Agent shall generate relevant, contextual questions based on the submission of the application documents for the purpose of assisting the PO to query the TP with the set of questions.			
2.3	Continuous Review and Improvement: (1) **Presentation**: The AI Agent shall present the accreditation review outcomes specified in 5.2(a) and (b) in a user-friendly format for review by POs and AOs. (2) **Correction**: The AI Agent shall provide an avenue for the PO/AO to counter-propose review outcomes, and the AI Agent shall make the corresponding amendments to the email to TP and/or internal review checklist, where applicable. (3) **Performance Tracking**: The AI Agent shall keep a log of activities, including the interaction between the AI Agent and PO/AO specified in 5.3(c)(ii) of the main RFP paper, which shall be used to			

S/No.	Specifications	Ability to Deliver (Yes / No)	If yes, please provide brief description and state any other relevant details	If no, please state reasons and proposed variations or alternatives
	review or enhance the performance of the system. (4) **Audit Trail**: The log of activities shall be downloadable in csv format that facilitates further data analysis or auditing.			
3.	**Non-functional Requirements**			
3.1	**AI Agents and Large Language Models:** (1) The AI Agents in the platform shall leverage world-renowned LLMs in the market that possess advanced reasoning capabilities and should have auto-switch capability between the LLMs that is tailored for the different scenarios or processes to yield the best outcome. (2) Vendor shall justify their choice of foundational/base LLMs, considering factors such as accuracy, ability to fine-tune/customize, privacy, latency, inference efficiency, and SOC2/Enterprise SLAs. The approach to model optimization for cost and latency should be detailed. (3) Vendor shall detail the use of model training and adaptation techniques such as Retrieval Augmented Generation (RAG), Fine-tuning, Zero-Shot Learning, and Few-Shot Learning. (4) Vendor shall detail the implementation of memory systems for the AI Agents, distinguishing between short-term (instruction/conversation context) and long-term (knowledge base, vector database) memory, and potentially incorporating knowledge graphs for episodic			

S/No.	Specifications	Ability to Deliver (Yes / No)	If yes, please provide brief description and state any other relevant details	If no, please state reasons and proposed variations or alternatives
	memory and finite state machines for procedural memory. (5) The LLMs shall support multi-modality.			
3.2	**Cloud and Data Residency:** (1) The proposed license or service model must include cloud hosting services. (2) PDPA Compliant: The solution must ensure personal data does not leave Singapore and is data-resident in Singapore. (3) For LLMs or other components not physically residing in Singapore, the vendor must provide the exact geographical location (with physical address) and share the reason for selection. (4) The AI Agents and their associated data will eventually need to be hosted/transited over to IBF cloud (AWS) at a later phase and Vendor will need to account for this effort and costing in their proposal. (5) Vendor shall detail the proposed deployment infrastructure that is fully cloud-based with a clear strategy for managing any base LLM models API usage fees and optimizing inference costs. The strategies for load balancing, performance optimization (caching, async processing), monitoring, and health checks are required. (6) Vendor shall provide the development environment, including necessary tools and dependencies (e.g., Python,			

S/No.	Specifications	Ability to Deliver (Yes / No)	If yes, please provide brief description and state any other relevant details	If no, please state reasons and proposed variations or alternatives
	language model providers, vector databases for memory).			
3.3	**Integration Capabilities:** Vendor shall describe how tools (internal and external APIs, databases, web services, application services) will be integrated to extend the AI Agents capabilities: (i)Ability to download application forms and supporting documents from the SSG-TPG system (GSIB machine). (ii)Ability to do web search for sussing out data and information outside of IBF's intranet. (iii)Ability to interact with IBF machines or data pipelines for ingestion and processing activities. (iv)Ability to integrate with Outlook Mail for automated email communications to TPs.			
3.4	**User Experience (UI/UX):** The UI/UX and prompt design and tuning for the AI Agents must be user-friendly, intuitive, and easy-to-navigate.			
3.5	**Scalability:** The AI Agents architecture must be scalable to handle increasing volumes of applications and adapt to future demands, dynamically expanding or contracting capacity with workload.			
3.6	**Vendor and Product Performance**: (i)The vendor is responsible for the accuracy and performance of the AI Agents.			

S/No.	Specifications	Ability to Deliver (Yes / No)	If yes, please provide brief description and state any other relevant details	If no, please state reasons and proposed variations or alternatives
	(ii)The solution must demonstrate high precision and contextual relevance in its outputs. (iii)Response times should be optimized, aiming for rapid processing to meet the reduced TAT goal. This includes strategies for low-latency inference. (iv)The solution must demonstrably contribute to achieving the target (TAT) turnaround time of within 1-2 months for the accreditation process.			
3.7	**Best-of-breed traditional Machine Learning (ML) and Large Language Models (LLMs) or Small Language Models (SLMs):** (i) The AI Agents can leverage on best of breed traditional MLs and LLMs/SMLs for the solution design, implementation and maintenance, where Vendor find it suitable and effective to employ for optimum gains. (ii)The data models shall be regularly updated with new fresh data, files and information. (iii)By analysing the data, the AI Agents shall learn to adapt, respond and act effectively over time.			
3.8	**Security and Compliance**: (i)PDPA Compliance: Strict adherence to Singapore's Personal Data Protection Act (PDPA) is mandatory. This includes ensuring personal data does not leave Singapore and is data-resident in Singapore and implementing necessary safeguards to protect confidential			

S/No.	Specifications	Ability to Deliver (Yes / No)	If yes, please provide brief description and state any other relevant details	If no, please state reasons and proposed variations or alternatives
	data at all costs within the hosting environment. (i)Data Protection: Implement robust measures against memory poisoning, tool misuse, and privilege escalation. (ii)Input Validation and Sanitization: Implement rigorous input validation and sanitization to prevent malicious injections (iii) Access Control: Implement fine-grained access controls, including role-based access control (RBAC) and dedicated service accounts with minimal permissions. Ensure authentication and authorization mechanisms are in place for communication among agentic and procedural systems. (iv)Rate Limiting: Implement rate limiting to prevent misuse or large volume attacks. (v)Zero-Trust Architecture: Adhere to zero-trust principles, verifying every request, applying least privilege access, continuous monitoring, and dynamic access control. (vi)Prompt Engineering for Security: Design system prompts to resist manipulation and ensure agents adhere to their allowed capabilities. (vii)Continuous Monitoring and Logging: Implement comprehensive monitoring and logging for auditability and proactive issue detection.			

S/No.	Specifications	Ability to Deliver (Yes / No)	If yes, please provide brief description and state any other relevant details	If no, please state reasons and proposed variations or alternatives
	(viii)Incident Response: Outline a plan for detecting, containing, investigating, recovering from, and learning from security incidents. (ix)Ethical AI Safeguards: Integrate ethical considerations to prevent biases, promote fairness, and ensure accountability. Human-in-the-loop oversight is a critical safeguard. **LLM Masking**: (i) Implement LLM Masking to mask/hide sensitive Personally Identifiable PII like NRIC/FIN No./Passport No., Phone Numbers and Personal Name, etc. before sending text to LLM models, and then reintroduces the original data afterward for backward reference. This will prevent PII from being exposed to 3rd party services LLM services and minimise the chance of data breaches or unauthorised access to sensitive information. This will also ensure privacy, security and compliance with data protection laws like PDPA, GDPR, HIPAA and CCPA.			
4.	**Set-up, Design, Development, SIT and UAT**			
4.1	Set-up of secured Cloud hosting environment and services			
4.2	Design, develop and orchestrate the AI Agents by building the user interface, data pipeline,			

S/No.	Specifications	Ability to Deliver (Yes / No)	If yes, please provide brief description and state any other relevant details	If no, please state reasons and proposed variations or alternatives
	frameworks, tools use and integration, knowledge base, retrieval and memory management, etc.			
4.3	Evaluation, logging and fine-tuning			
4.4	Conduct SIT			
4.5	Conduct UAT			
4.6	Monitoring and governance			
4.7	Presentation(s) and demonstration(s) of proposed solution to IBF management and team leads for endorsement			
5.	**VAPT and Remediation**			
5.1	Conduct VAPT and remediation			
6.	**Change Management**			
6.1	(a) Identify all relevant stakeholders impacted by the AI Agents implementation, including but not limited to: (i)Staff (potential users e.g. Standards and Accreditation) (ii)Management (sponsors for the project) (iii)IT department (responsible for integration and maintenance) (b)Vendor shall l educate IBF users (POs and AOs) about the AI Agents' capabilities and limitations. (c)Vendor shall develop and execute comprehensive change management strategies and plans to ensure successful adoption of the AI Agents amongst users within IBF. (d)Vendor shall plan and coordinate communication efforts targeted at the different user profiles or roles to ensure users are sufficiently aware of the AI			

S/No.	Specifications	Ability to Deliver (Yes / No)	If yes, please provide brief description and state any other relevant details	If no, please state reasons and proposed variations or alternatives
	Agents' purpose, functionalities and benefits and build their desire towards supporting the change for the better. Vendor shall engage the different stakeholders including management to understand their concerns towards the change and ensure decentralised change messaging is coherent throughout. (e)Vendor shall have a good grasp of the change impact within the business domain and ensure that domain owners are adequately informed of scenarios where high change impact or risks are present so that appropriate risk mitigation measures can be taken. (f)Vendor shall work and collaborate with IBF-hired change management practitioner(s), if necessary, to ensure alignment with IBF's overall master change strategy. (g)Vendor shall monitor the progress of change initiatives, evaluate their effectiveness, and report on outcomes to IBF management and make adjustments as needed. Vendor shall seek and identify leading best practices for change management. (h)Vendor shall design and conduct training sessions for users to familiarise them with the AI Agents and support users in transiting into the new system / features. (i)Vendor shall develop a knowledge base with FAQs and			

S/No.	Specifications	Ability to Deliver (Yes / No)	If yes, please provide brief description and state any other relevant details	If no, please state reasons and proposed variations or alternatives
	troubleshooting guides for both users and support staff.			
6.2	User Education: Vendor will educate IBF users about the AI Agents' capabilities and limitations.			
6.3	Develop a communication plan to inform stakeholders about the AI Agents' purpose, functionalities, and benefits.			
6.4	Conduct training sessions for relevant staff to familiarise them with the AI Agents.			
6.5	Develop a knowledge base with FAQs and troubleshooting guides for both users and support staff.			
7.	**Client Environment Migration**			
7.1	When the AI Agents are to be migrated to IBF cloud environment, Vendor shall work with IBF in the planning and execution, and to ensure that appropriate security measures and governance processes are in place. This may include collaboration on data security practices, user access controls, and incident response protocols. All IBF data will be migrated over with proper testing and acceptance, and data measures to completely remove data from vendor's cloud will take place at no additional cost to IBF with formal certification as evidence that all IBF and user data are securely wiped out.			
7.2	The Vendor shall work with IBF and its appointed IT system vendor(s) to ensure seamless transition between the platform and the respective system(s) and all migrated data are to be fully			

S/No.	Specifications	Ability to Deliver (Yes / No)	If yes, please provide brief description and state any other relevant details	If no, please state reasons and proposed variations or alternatives
	verified with report submitted to IBF for acceptance.			
8.	**System Integration**			
8.1	The platform shall allow easy insert/configure hyperlink(s) to existing IBF website and any other websites that IBF deemed necessary.			
9.	**Governance and Oversight**			
9.1	Transparency: Vendor shall be transparent about the AI Agents' tools, technology, frameworks, capabilities and constraints. Vendor shall disclose the mechanism of the AI Agents' workings and the data they are trained on while protecting IBF's intellectual property.			
9.2	Accountability: Vendor shall be accountable for the development and operation of the AI Agents and take steps to ensure that the AI Agents are used in a safe and responsible manner.			
9.3	Alignment with Values: The AI Agents shall be governed by a set of well-defined values that promote safety, fairness, transparency and accountability. These values will be aligned with the principles of artificial intelligence ethics and responsible development. Vendor shall also take reference and use AI Verify's evaluation toolkits and governance testing framework, https://aiverifyfoundation.sg/#, and present their findings to IBF, where applicable.			
9.4	Human Oversight: The AI Agents shall be subject to human oversight to ensure they are used appropriately and in accordance			

S/No.	Specifications	Ability to Deliver (Yes / No)	If yes, please provide brief description and state any other relevant details	If no, please state reasons and proposed variations or alternatives
	with the values and guidelines as set out in para 5.6c of the main RFP paper.			
9.5	Data Security: Vendor shall implement appropriate security measures to protect user data from unauthorised access, disclosure, alteration, or destruction.			
9.6	Privacy: Vendor shall respect user privacy and comply with all applicable data privacy laws and regulations. Users will have control over their data and how it is used.			
9.7	Misuse Prevention: Vendor shall take steps to prevent the AI Agents from being used for malicious purposes, such as spreading misinformation or propaganda.			
9.10	Vulnerability Management: Vendor shall have a process in place to identify, assess, and address vulnerabilities in AI Agents.			
9.11	Incident Response: Vendor shall have a plan in place to respond to security incidents involving the AI Agents.			
9.12	Continuous Improvement: Vendor shall be committed to continuously improving the governance and security of the AI Agents and regularly review and update guidelines as necessary.			
9.13	Bias and Fairness: Vendor shall take steps to mitigate bias in the AI Agents' evaluation and responses.			
9.14	Explainability: Vendor shall ensure AI Agents' cognitive thinking and reasoning			

S/No.	Specifications	Ability to Deliver (Yes / No)	If yes, please provide brief description and state any other relevant details	If no, please state reasons and proposed variations or alternatives
	capabilities are easily understandable e.g. demonstrating Chain of Thought, or Tree of Thought.			
9.15	The platform shall be protected against all known security vulnerabilities inclusive of OWASP (Open Web Application Security Project) Top 10 web application security risks. System and Organization Controls Report (preferably SOC 2 Type 2 certification) and Outsourced Service Provider Audit Report (OSPAR) will have to be attached together with this submission.			
9.16	Vulnerability and Penetration testing (VAPT) conducted at least once a year with vulnerabilities remediated within reasonable timeframe and report to be submitted to IBF. For avoidance of doubt, VAPT report have to be submitted and accepted by IBF that all vulnerabilities are remediated prior to go-live of the system.			
9.17	All Data transmissions such as data-in-use, data-in-transit and data-at-rest shall be encrypted.			
10.	**Staff Training and User Guide**			
10.1	Preparation and confirmation of User Guide			
10.2	Users training			
10.3	Change communications plan			
11.	**Contract Duration**			
11.1	The initial contract period is SIX (6) calendar months (hereinafter referred to as the “Initial Contract Period”) with a provision to extend for another TWELVE (12) months on the condition that the outcome			

S/No.	Specifications	Ability to Deliver (Yes / No)	If yes, please provide brief description and state any other relevant details	If no, please state reasons and proposed variations or alternatives
	of the first SIX (6) months pilot run is successful (pls refer to Para 20 for the Exit Clause in the main RFP paper). Vendor shall provide quotes for service support charged on an annual basis or equivalent man hours. Vendor shall provide quotes for change request on platform configurations charged on equivalent man hours.			
12.	**Achieve Project Timeline**			
12.1	Ability to achieve project timeline within the 1st 2 months of pilot implementation followed by 4 months of pilot run			

B) System Requirements

S/N No.	Specifications	Ability to Deliver (Yes / No)	If yes, please provide brief description and state any other relevant details	If no, please state reasons and proposed variations or alternatives
1.	**System Requirements**			
1.1	The estimated transactions/applications to be catered for the AI Agents estimated based on mean return rate of applications to Training Provider of 2, is as follows: (i) Low Range: less than 15 transactions per week			

S/N No.	Specifications	Ability to Deliver (Yes / No)	If yes, please provide brief description and state any other relevant details	If no, please state reasons and proposed variations or alternatives
	(ii) Mid-Range: 30 transactions per week (iii) High Range: 45+ transactions per week			
2.	**Data Governance**			
2.1	IBF shall have full ownership of all transacted data, documents and reference materials on the platform, and any data used throughout the project. All data disclosure to third parties, data retention and disposal by Vendor shall be subjected to IBF's approval and compliance.			
2.2	Vendor shall ensure that the data is protected against loss, corruption, unauthorised access, use, amendments etc. and only authorised staff has access to the data in both UAT and PROD environments. All data migration must be approved by IBF.			
2.3	Vendor shall comply with all its obligations under the PDPA at its own cost.			
2.4	The Vendor shall only process, use or disclose IBF's Training Providers' Personal Data: i)strictly for the purposes [of fulfilling its obligations and providing the services required] under this Agreement; ii)with IBF's prior written consent; or iii)when required by law or an order of court but shall notify IBF as soon as practicable before complying with such law or order of court at its own costs.			

S/N No.	Specifications	Ability to Deliver (Yes / No)	If yes, please provide brief description and state any other relevant details	If no, please state reasons and proposed variations or alternatives
2.5	The Vendor shall not transfer IBF's Training Providers' Personal Data to a place outside Singapore without IBF's prior written consent. [If IBF provides consent, the Vendor shall provide a written undertaking to IBF that the Training Providers' Personal Data transferred outside Singapore will be protected at a standard that is comparable to that under the PDPA. If the Vendor transfers the Training Providers' Personal Data to any third party overseas, the Vendor shall procure the same written undertaking from such third party].			
2.6	The Vendor shall protect IBF's Training Providers' Personal Data in the Vendor's control or possession by making reasonable security arrangements (including, where appropriate, physical, administrative, procedural and information & communications technology measures) to prevent: i)unauthorised or accidental access, collection, use, disclosure, copying, modification, disposal or destruction of the Training Providers' Personal Data, or other similar risks; and ii)the loss of any storage medium or device on which personal data is stored.			
2.7	The Vendor shall only permit its authorised personnel to access IBF's Training Providers'			

S/N No.	Specifications	Ability to Deliver (Yes / No)	If yes, please provide brief description and state any other relevant details	If no, please state reasons and proposed variations or alternatives
	Personal Data on a need-to-know basis and access logs shall be furnished to IBF upon request.			
2.8	The Vendor shall provide IBF with access to the Training Providers' Personal Data that the Vendor has in its possession or control, as soon as practicable upon IBF's written request.			
2.9	Where IBF provides its Training Providers' Personal Data to the Vendor, IBF shall make reasonable effort to ensure that the Training Providers' Personal Data is accurate and complete before providing the same to the Vendor. The Vendor shall put in place adequate measures to ensure that the Training Providers' Personal Data in its possession or control remain or is otherwise accurate and complete. In any case, the Vendor shall take steps to correct any errors in the Training Providers' Personal Data, as soon as practicable upon the IBF's written request.			
2.10	The Vendor shall not retain IBF's Training Providers' Personal Data (or any documents or records containing the Training Providers' Personal Data, electronic or otherwise) for any period of time longer than is necessary to serve the purposes of this RFP.			
2.11	The Vendor shall also facilitate IBF to comply with the obligation			

S/N No.	Specifications	Ability to Deliver (Yes / No)	If yes, please provide brief description and state any other relevant details	If no, please state reasons and proposed variations or alternatives
	in Clause 7.3j of the main RFP paper to review and maintaining of the Training Provider's Personal Data database.			
2.12	The Vendor shall, upon the request of IBF: i)return to IBF, all of the Training Providers' Personal Data; or ii)delete all the Training Providers' Personal Data in its possession, and after returning or deleting all of the Training Providers' Personal Data, provide IBF with written confirmation that it no longer possesses any of the Training Providers' Personal Data. Where applicable, the Vendor shall also instruct all third parties to whom it has disclosed the Training Providers' Personal Data for the purposes of this Contract to return to the Vendor or delete the Training Providers' Personal Data.			
2.13	The Vendor shall immediately notify IBF with established communication channels e.g. email, phone calls, messaging apps without undue delay when the Vendor becomes aware of a breach of any of its obligations in Clauses [7.3d to 7.3l] in the main RFP paper or believe that a data breach has occurred in relation to personal data that the Vendor is processing on behalf of and for the purposes of another organisation.			
2.14	Vendor shall sign the Non-Disclosure and Undertaking			

S/N No.	Specifications	Ability to Deliver (Yes / No)	If yes, please provide brief description and state any other relevant details	If no, please state reasons and proposed variations or alternatives
	Agreement (NDA) not to access, use, share, divulge or retain data unless this is required by the Vendor's staff in discharging their duties during their employment. The NDA is binding even if the staff has resigned or is transferred to another project team or after the termination or expiry of the Contract. Non-compliance could result in legal action being taken against the Vendor by IBF and/or referred to relevant authorities.			
3.	**Availability**			
3.1	The System shall be available on a twenty-four (24) hours per day, seven (7) days per week, three hundred and sixty-five (365) days per year basis (24 X 7 X 365) except for scheduled routine system maintenance or downtime in which IBF is to be notified at least one (1) week in advance to inform users. The support hours for the platform are from Singapore Time 9.00 am to 6.00 pm from Mondays to Fridays (excluding public holidays in Singapore).			
4.	**Technical and User Support Requirements**			
	The Vendor shall provide offsite support (preferably local) for the System conforming to all IBF business hours. For all issues reported by the users or by IBF, Vendors should adhere to response time as prescribed by IBF. An issue or incident is			

S/N No.	Specifications	Ability to Deliver (Yes / No)	If yes, please provide brief description and state any other relevant details	If no, please state reasons and proposed variations or alternatives
	deemed resolved when the reporting party is notified and satisfied with the resolution steps taken by the Vendor.			

C) Project Schedule and Deliverables

S/N No.	Specifications	Ability to Deliver (Yes / No)	If yes, please provide brief description and state any other relevant details	If no, please state reasons and proposed variations or alternatives
	Project Deliverables: Accreditation AI Agents (to be deployed by the end of the 1st 2 months from the date of award of project)			
1.	**Stage 1 – Gathering of User Requirements**			
1.1	**Timeline – 2 weeks** a) User requirements gathering b) Develop a detailed project scope document outlining the AI Agents' functionalities and features. c) Prioritize requirements based on user needs and IBF's objectives. d) Gather user feedback that provides impetus to the continuous improvement of the AI Agents.			
2.	**Stage 2 – Set-up, Design, Development, SIT and UAT**			

S/N No.	Specifications	Ability to Deliver (Yes / No)	If yes, please provide brief description and state any other relevant details	If no, please state reasons and proposed variations or alternatives
2.1	**Timeline – 4 weeks** a) Set-up of secured Cloud hosting environment and services b) Design, develop and orchestrate the AI Agents by building the user interface, data pipeline, frameworks, tools use and integration, knowledge base, retrieval and memory management, etc. c) Evaluation, logging and fine-tuning d) Conduct SIT e) Conduct UAT f) Monitoring and governance g) Presentation(s) and demonstration(s) of proposed solution to IBF management and team leads for endorsement			
3.	**Stage 3 – VAPT and Remediation**			
3.1	**Timeline – 1 weeks** 1. Conduct VAPT and Remediation			
4.	**Stage 4 – Production Deployment**			
4.1	**Timeline – 1 week** 1. Production deployment of the AI Agents			
5.	**Stage 5 – Staff Training and User Guie**			
5.1	**Timeline – 3 Days** 1. Preparation and confirmation of User Guide 2. User training			

S/N No.	Specifications	Ability to Deliver (Yes / No)	If yes, please provide brief description and state any other relevant details	If no, please state reasons and proposed variations or alternatives
	3. Change communications plan			

PART III –PROJECT COSTS & FEES

Please provide information on the detailed applicable fees and any other applicable costs and payment schedule expected for the completion of this project.

Project Fee Quotation Template (Please submit in Excel format)

Item	SGD (exclude GST)
1. Professional services fee for pilot implementation of Accreditation AI Agents with a detailed breakdown based on the deliverables for user requirements gathering, platform configuration, design, data preparation, SIT, UAT, production deployment, staff training, change communications plan. 2. Base platform/subscription model fees or usage-based model fees for 1st 6 months of pilot implementation.	
2. **Optional** - Base platform/subscription model fees or usage-based model fees support and maintenance services on per month/annum basis for 1-year extension for production implementation – *this will be an option-to-exercise at the discretion of IBF depending on the successful outcome of the pilot implementation.*	
3. **Optional** - Professional services fee for transition to IBF Cloud with a detailed breakdown during the 1-year extension for production implementation – *this will be an option-to-exercise at the discretion of IBF depending on the successful outcome of the pilot implementation.*	
4. Service support a) Please state scope of services and estimated man-days for both office and non-office hours	
5. Ad hoc Change Requests a) Please state scope of services and man-day rate for both office and non-office hours	
6. Any other miscellaneous costs a) Please state clearly on intent and in man-hours/monthly/annual costs where applicable)	
Total Cost	

PART IV – REFERENCES / OTHER CONSIDERATIONS

Please indicate customer references (with contact details), reference or highlight any other useful factors you would like us to consider in reviewing your quotation.

PART V – NON-DISCLOSURE AND UNDERTAKING (THIRD PARTIES)

IMPORTANT NOTES

1. The Institute of Banking and Finance ("the **Organisation**") is legally required to comply with the provisions of the *Personal Data Protection Act* (No. 26 of 2012) ("the **Act**"). Failure to comply with the Act may result in penalties being issued against the Organisation.

2. To ensure compliance with the Organisation's internal policies in relation to the Act, all third-party contractors and/or service providers are required to sign this Undertaking.

3. This Undertaking shall be signed before the commencement of work and/or services for the Organisation.

A. SERVICE PROVIDER'S (AKA as the VENDOR) DETAILS

1.	**Name of Service Provider's Company ("Service Provider"):**	
2.	**Company UEN No:**	
3.	**Contact Number:**	
4.	**Address:**	
5.	**Email Address:**	
6.	**Nature of Work / Service provided to Organisation ("Purpose"):**	

B. UNDERTAKING

1. Access to Personal Data, non-public and sensitive information ("**Confidential Information**") may be required in the performance of the Service Provider's Purpose. "**Personal Data**" shall have the meaning given to it in the Act and refers to information about an identified or identifiable individual, where the individual refers to a natural person, whether living or deceased. It covers all forms of personal data, whether in electronic or non-electronic form.

2. Should the Service Provider have access to such Confidential Information, the Service Provider undertakes that it shall not under any circumstances, release or disclose such

Confidential Information to any third party or third-party organisation. The Service Provider shall protect such Confidential Information and will employ all reasonable efforts to maintain the confidentiality of such Confidential Information.

3. The Service Provider shall implement such security measures as are reasonably necessary to protect the Confidential Information against unauthorised access, collection, use, disclosure, copying, modification, disposal, or any other form of processing (as defined under the Act).

4. The Service Provider shall immediately notify the Organisation of any suspected or confirmed unauthorized access, collection, use, disclosure, copying, modification, disposal or any other form of processing (as defined under the Act) and/or misuse of Confidential Information. Without prejudice to any other rights and remedies that the Organisation may have, the Service Provider shall at its own expense render all necessary assistance to the Organisation to investigate, remedy and/or otherwise respond to such unauthorised access, collection, use, disclosure, copying, modification, disposal or any other form of processing (as defined under the Act).

5. The Service Provider shall immediately inform the Organisation if any Confidential Information is lost or destroyed or becomes damaged, corrupted, or unusable. Without prejudice to any other rights and remedies that the Organisation may have, the Service Provider shall restore such Confidential Information at its own expense.

6. Before the Service Provider discloses Personal Data of any third-party individuals to the Organisation, the Service Provider undertakes to obtain all necessary consents required under the Act for the Organisation to collect, use and/or disclose such personal data.

7. The Service Provider undertakes to comply with all obligations that apply to it under the Act and all subsidiary regulations that may be enacted from time to time under the Act.

C. CONSEQUENCES OF BREACH OF UNDERTAKING

The Service Provider acknowledges that:

1. In the event of any breach or neglect of its obligations under this Undertaking, the Organisation may exercise its right to refuse the Service Provider access to the Organisation's premises and facilities.

2. If the Service Provider should breach any provisions of this Undertaking, the Organisation may suffer immediate and irrevocable harm for which damages may not be an adequate remedy. Hence, in addition to any other remedy that may be available in law, the Organisation is entitled to injunctive relief to prevent a breach of this Undertaking.

3. Without prejudice to any other clause(s) in this Undertaking, the Service Provider shall bear all liability and shall fully indemnify the Organisation against any and all actions, claims, proceedings (including proceedings before the Personal Data Protection Commission ("**PDPC**")), costs (including costs of complying with any remedial directions and/or financial penalties that may be imposed by the PDPC on the Organisation), damages, legal costs and/or other expenses incurred by the Organisation or for which the Organisation may become liable due to any failure by the Service Provider or its employees or agents to comply with any of its obligations under this Undertaking.

4. Even after the Service Provider ceases its Purpose at the Organisation, it agrees that the obligations herein shall continue.

Name of Service Provider:	_____
Service Provider's Company Stamp:	_____
Name of Representative of Service Provider:	_____
Signature of Representative of Service Provider:	_____
Date:	_____

PART VI: IBF IT SERVICE PROVIDER CHECKLIST

Name of Service Provider _____

Date Completed _____

Name of Respondent _____

Designation / Title _____

Contact Number _____

Email Address _____

Signature _____

Company Stamp _____

For The Institute of Banking and Finance ("IBF") use only:

Name of Reviewer

Designation / Title	
Contact Number	
Email Address	
Type of Outsourcing	Material / Non-Material[1]

[1] For non-material outsourcing, Service Provider Checklist is applicable if the service is classified under category 2A where the service provider will be hosting or handling personal sensitive data or classified data ("Confidential" or higher), or the services is assessed to have potential medium or above impact to IBF

Instructions

1. This service provider checklist should be completed by personnel who have direct knowledge of the information systems and operations. The information provided in this checklist should be reviewed.

2. For each guideline description, place an “X” in the appropriate column to indicate whether the service provider is fully compliant, partially compliant, or not compliant. Otherwise, place an “X” in the NA column.

3. If full compliance has not been achieved, explain in the Comments column why, and how and when remedial action would be made.

4. Please attached evidence (e.g. SOC-2 Type 2, most recent penetration test report) that service is validated for security assurance and adequate protection measures are in place.

5. IBF IT team may require the service provider to furnish further evidence if the submission details are incomplete.

S/N	Risk Category	Full Compliance	Partial Compliance	Non-Compliance	N.A.	Comments
1	**Service/Product Information**					
1.1	Brief Service/Product Description:					
1.2	For hosted services, is the data hosted only in Singapore region? If no, please state the countries or cities where the data will reside					
2	**Service Assurance**					
2.1	Does the Service Provider commit to a service level agreement (SLA)? If yes, please provide either the SLA document/details or website URL of the service agreement.					
2.2	Service Provider has a disaster recovery plan and has tested the contingency plan, backup restoration and service recovery?					
2.3	Does the service agreement make reasonable provisions for confidentiality protection clause(s), right to access audit reports, sub-contractors obligations (if sub-contracted), termination clause(s) with sufficient advanced notice?					
2.4	Has the Service Provider attained security-related compliance (SOC-2 Type 2 (preferred) or other equivalent)? Attach the necessary report to show the security assurance.					

S/N	Risk Category	Full Compliance	Partial Compliance	Non-Compliance	N.A.	Comments
	Otherwise, please provide supporting information that the necessary security controls are in place. (e.g. audit opinions). Examples of security-related compliance: A. ISO/IEC (27001 / 27002 / 27017 / 27018) B. SOC (Type 1 / Type 2 / Type 3) C. PCI DSS (Level 1 / 2 / 3 /4) D. CSA Star (Level 1 / 2 / 3) E. NIST (800-53 / 800-144) F. OWASP ASVS (Level 1 / 2 / 3) G. MTCS SS584 H. Outsourced Service Provider Audit Report (OSPAR)					

S/N	Risk Category	Full Compliance	Partial Compliance	Non-Compliance	N.A.	Comments
2.5	Service Provider to support and assist in audit activity by providing necessary documents/reports stated in 2.4 upon request.					
2.6	In the event of negative comments or potential auditor concerns in the reports (e.g. incomplete controls), the Service Provider shall make the necessary corrective follow-up actions to address the concern.					
2.7	Service Provider has an incident management process and will notify customer promptly for major incident or when there is a cybersecurity data breach in the service.					
2.8	Service Provider has not suffered any significant breaches in the last 5 years.					
3	**Data Security**					
3.1	As part of the service engagement, no personally identifiable information ('PII') or other personal data should be stored in the vendor's endpoint devices e.g. laptop and mobile					
3.2	Service provider undertakes to protect the confidentiality and security of IBF's sensitive or confidential information					

S/N	Risk Category	Full Compliance	Partial Compliance	Non-Compliance	N.A.	Comments
	and will comply with applicable data protection laws and regulations e.g. PDPA, GDPR?					
3.3	Does the Service provider implement backup of critical information on a regular basis and periodically validate the recovery process?					
3.4	Is data segregated between customers (if hosted) and controls put in place to protect customer data from unauthorised access, modification or leakage?					
3.5	Are data at rest and in transit encrypted using strong encryption algorithm?					
3.6	Are customers' data securely erased from the systems and environment (including backup media) after the termination of the contract?					
4	**General Security Controls**					
4.1	Does the service provider follow secure software development lifecycle practices?					
4.2	Does the service provider enforce change management procedures to ensure changes does not affect services?					

S/N	Risk Category	Full Compliance	Partial Compliance	Non-Compliance	N.A.	Comments
4.3	Does the service provider regularly patch and review the system configurations met its security hardening baselines?					
4.4	Is the service validated regularly for potential security vulnerabilities and findings tracked till closure? If yes, please attach evidence (most recent penetration test reports performed by CREST-accredited penetration tester or equivalent).					
4.5	Is the service resilient to Distributed Denial-of-Service (DDoS) attacks and common application attacks?					
4.6	Are network security controls (e.g. firewall restriction) implemented to protect and detect network resources from unauthorized access?					
4.7	Does the service provide strong authentication controls (e.g. MFA) before service can be accessed?					
4.8	If password is used as the primary means of authentication, is the service able to enforce password complexity requirements, password expiration and account lockout policies					

S/N	Risk Category	Full Compliance	Partial Compliance	Non-Compliance	N.A.	Comments
4.9	Does the application support role-based access control (RBAC) to segregate distinct functions and roles such as for end-users and administrators?					
4.10	Does the service support ease of review or automated handling of inactive/dormant accounts?					
4.11	Is audit logging or reports turn on (e.g. timestamp, login, logout, user actions performed) and the audit logs or reports accessible/retrievable?					
4.12	Is the privilege access management controls enforced in the service provider operations i.e. privileged activities are controlled, monitored and independently reviewed?					
4.13	Segregation of duties should be enforced to prevent any single individual for making critical changes to the system or data without oversight.					
4.14	Does the service provider monitor the security of the system on a 24x7x365 basis?					
5	**Peripheral Supporting Services (If applicable)**					
5.1	If there are peripheral services (e.g. ticketing system) associated with this engagement that keep personal or confidential data from IBF or IBF customers, are the same					

S/N	Risk Category	Full Compliance	Partial Compliance	Non-Compliance	N.A.	Comments
	security controls are in place as above? If not, state what controls are missing and any mitigation measures (e.g. system is not internet facing)					