ANNEX A: PROPOSAL

Project Name:

RFP.TDT.2024.0009

Provision of Professional Services, Subscription, Support and Maintenance for GenAI-Powered Chatbot

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 **"Proposal – Provision of Professional Services, Subscription, Support and Maintenance for GenAI-Powered Chatbot (**RFP.TDT.2024.0009**)",** 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 (Excel version provided)

A) Functional and Non-functional Specifications

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.	**User Requirements Gathering**			
1.1	Conduct User requirements gathering			
1.2	Develop a detailed project scope document outlining the chatbot's functionalities and features.			
1.3	Prioritize requirements based on user needs and IBF's objectives.			
1.4	Design user interface mock-ups for user feedback and refinement.			
1.5	Establish clear communication channels for ongoing user feedback and continuous improvement of the JTM Chatbot.			
1.6	Establish change management to manage any impact to stakeholders and cater to user education/training.			
1.7	Following the business user requirement gathering process, the collected information will be analysed and used to: (i) Develop a detailed project scope document outlining the chatbot's functionalities and features. (ii) Prioritise requirements based on user needs and IBF's objectives. (iii) Design user interface mock-ups for user feedback and refinement.			

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
	(iv) Establish clear communication channels for ongoing user feedback and continuous improvement of the JTM Chatbot.			
2.	**Functionality**			
2.1	Interactive Guidance: The chatbot will guide users through the relevant JTM based on their initial input, with: (i) Ability to understand Sustainable Finance and Generative AI industry JTM and IBF provided documents and be able to act as an interactive virtual career advisor to the users. (ii) Ability to understand and respond to user queries in natural language (iii) Support for multi-turn conversations with context retention (vi) Support for uploaded documents to be in format of word (e.g. docx), excel (e.g. xlsx) and PDF (vii) Personalization capabilities to tailor responses			

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
	based on user profile and historical interactions. (vi) Provide individuals with insights on how emerging skills will affect their careers with the JTM study serving as the data foundation for the chatbot's responses with minimally the following: • Welcome and Introduction - The chatbot greets the user and introduces itself and briefly explains its purpose, i.e. informing users about the impact of emerging skills on their careers • User Input - Asks the user for their current job title or a brief description of their role. Prompts the user to select relevant emerging skills or job roles they're interested in (e.g., sustainable finance, generative AI) from a pre-defined list or allows them to type their own. • Analyses the user's current job title/description and selected skills in relation to the JTM study findings. Generates a tailored response using GenAI's natural language processing for			

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
	potential impact of the chosen skills on the user's current job such as increased automation or job displacement risks (if applicable) or opportunities for upskilling or using the skills to enhance current tasks; and relevance of the skills for future job prospects such as demand for these skills in related or entirely new job fields.			
2.2	Accurate Responses: Responses will be based solely on published JTMs and IBF data, ensuring high accuracy and relevance with no hallucination			
2.3	Personalised Recommendations: The chatbot will prompt users for basic information (industry, career goals) to personalize responses and recommend training programs (based on IBF-accredited programs).			
2.4	CV Upload Function: Users can upload CVs and chatbot will be able to distil it into skills to perform a hyper-personalised skills gap analysis and provide tailored training program recommendations with reference to IBF sources such as IBF Programme Finder (https://www.ibf.org.sg/home/for-individuals/skills-and-jobs-development/upskill/programme-finder) or any relevant sources informed by IBF. This CV Upload			

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
	function should preferably be ready by 1 September 2024, otherwise the vendor shall ensure delivery of this CV upload function no later than 4 weeks from the chatbot's launch on 1 September 2024, with explanation subjected to IBF's review.			
2.5	Report for Users: At the end of the conversation with the chatbot, it should prompt the user on whether they require a summary/report of the conversation to be emailed to the user for record/reference, and the email shall be captured in the system for IBF administrators to follow-up with the user if necessary.			
2.6	Feedback Mechanism: A user survey will be integrated at the end of the conversation to gather feedback for continuous improvement and machine learning. To include contactable information such as email when necessary.			
2.7	Future JTM Support: The chatbot shall have functionality to allow seamless uploading of future JTM studies supported by vendor and subjected to review and acceptance by IBF administrator and users for continued functionality and scalability.			
2.8	Data Analytics: The vendor will provide analytics and reports on usage volume, top queries,			

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
	chatbot responses, feedback, and other key metrics for continuous improvement.			
2.9	Ability for IBF administrators to: (i) upload documents to be used by chatbots as reference for responses (ii) draw up a workflow on how the chatbots should manage the input and outputs to the users (iii) fine-tune the parameters to allow more targeted and specific responses			
2.10	IBF have the flexibility to partake in the training and fine tuning of the chatbot and the vendor shall guide and assist IBF at no additional costs			
3.	**Technical Specifications**			
3.1	Cloud Environment: Deployment and maintenance of the chatbot in a public cloud environment provided by the vendor, ensuring scalability, reliability, and security.			
3.2	Model: The Large Language Model used must have MMLU (Massive Multitask Language Understanding) above 80			
3.3	Scalability: to accommodate fluctuations in user traffic and workload demands.			
3.4	Text Processing: The chatbot should be able to handle text input up to 250 words.			

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
3.5	Large Language Model (LLM): The chatbot will leverage renowned LLM(s) residing in a geographically disclosed location outside of Singapore. The vendor must provide justification for the chosen LLM(s). (i) Domain-specific knowledge: Expertise in the employment and skills training domain would be beneficial. (ii) Multilingual capabilities: If the target audience includes users with varying language proficiency, multilingual support might be required. (iii) Safety and security features: The LLM should have built-in safeguards against bias and offensive language generation. (iv) Ability for learning and correction, and to include any fine-tuning based on user feedback			
3.6	Natural Language Processing (NLP): The chatbot should utilise robust NLP techniques to: (i) Understand user queries with high accuracy, even with typos or informal language.			

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) Generate natural and engaging responses that mimic human conversation.			
3.7	Dialogue Management: The chatbot should employ a dialogue management system to: (i) Maintain context throughout the conversation and avoid irrelevant responses. (ii) Guide the conversation flow based on user intent and provide appropriate follow-up questions.			
3.8	Machine Learning (ML): The chatbot should leverage ML for continuous improvement: (i) By analysing user interactions, the chatbot can learn to personalise responses more effectively over time. (ii) The ML model should be regularly updated with new JTM data and training information.			
3.8	Data Security: (i) PDPA compliance with consent, and to ensure sensitive user data remains within Singapore. (ii) Security measures to prevent misuse and large-volume attacks.			

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
	(iii) Guardrails to ensure ethical and accurate responses.			
4.	**Development**			
4.1	Design, train, and validate the chatbot using robust industry metrics for GenAI chatbots, such as accuracy, fluency, and user satisfaction.			
4.2	Develop and implement Response Attribute Grammatical Error (RAG) correction, prompt engineering, and fine-tuning techniques for accuracy.			
4.3	Integrate the chatbot with the IBF website (www.ibf.org.sg) or any IBF related services.			
5.	**Change Management**			
5.1	Identify all relevant stakeholders impacted by the GenAI chatbot implementation, including but not limited to: (i) Employees (potential users e.g. Career Advisors) (ii) HR department (responsible for training and communication) (iii) IT department (responsible for integration and maintenance) (iv) Management (sponsors for the project)			
5.2	User Education: Vendor will educate IBF users about chatbot's capabilities and limitations.			

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
5.3	Develop a communication plan to inform stakeholders about the chatbot's purpose, functionalities, and benefits.			
5.4	Conduct training sessions for relevant staff to familiarise them with the chatbot and how to direct user inquiries.			
5.5	Develop a knowledge base with FAQs and troubleshooting guides for both users and support staff.			
6.	**Client Environment Migration (Option)**			
6.1	In the event that the chatbot is to be migrated to IBF cloud environment, Vendor will 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.			
6.2	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/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
	verified with report submitted to IBF for acceptance.			
7.	**System Integration**			
7.1	The chat shall be able to integrate with IBF-determined systems such as the IBF website such that users can easily start a conversation via their internet devices.			
7.2	The platform shall allow easy insert/configure hyperlink(s) to existing IBF website and any other websites that IBF deemed necessary.			
7.3	The platform shall be able to support web links where possible to IBF's reference sites, partner sites, financial training providers and financial institutions.			
8.	**Governance and Security**			
8.1	Ability to adhere to governance and security measures			
8.2	Vendor shall submit a report to IBF with satisfactory results and accepted by IBF before the launch of the platform, and thereafter on a yearly basis: • To provide the latest report on the Vulnerability Assessment and Penetration Testing (VAPT) performed by an independent CREST-certified party conducted on the platform; and • To diligently rectify any identified security gaps that comes to IBF's attention.			
8.3	Vendor shall ensure the platform hosting services meet all industry security 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
8.4	Vendor shall ensure the data security fulfils PDPA requirements.			
8.5	Vendor shall provide SOC 2 compliance of the Cloud Service Provider, especially Type 2 reporting, demonstrating a dedication to data protection			
9.	**Staff Training and Change Management**			
9.1	Preparation and confirmation of User Guide			
9.2	Users training			
9.3	Change communications plan and management			
10.	**Contract Duration**			
10.1	The initial contract period is twelve (12) calendar months (hereinafter referred to as the “Initial Contract Period”). 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.			
11.	**Achieve Project Timeline**			
11.1	Ability to achieve project timeline to go-live on 1 Sep 2024			

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 interaction to be catered for the chatbot estimated based on monthly usage as following: (i) Low Range: 5,000 - 10,000 interactions per month (ii) Mid Range: 10,000 - 20,000 interactions per month (iii) High Range: 20,000+ interactions per month.			
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	The Vendor shall sign the Non-Disclosure and Undertaking Agreement (NDA) not to access, use, share, divulge or retain			

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
	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.			
2.4	Vendor shall comply with all its obligations under the PDPA at its own cost.			
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.			
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
1.	**Project Deliverables: Phase 1 - Sustainable Finance GenAI Chatbot(to be deployed by 1 Sept 2024)**			
1.1	**Timeline – 2 weeks** 1. User requirements gathering 2. Develop a detailed project scope document outlining the chatbot's functionalities and features. 3. Prioritize requirements based on user needs and IBF's objectives. 4. Design user interface mock-ups for user feedback and refinement. 5. Establish clear communication channels for ongoing user feedback and continuous improvement of the JTM Chatbot.			

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.	**Stage 2 – Design, Development, Usability Testing, fine-tuning and UAT**			
2.1	**Timeline – 2 weeks** 1. Setup of secured cloud hosting 2. Design and development of Chatbot based on IBF's requirement 3. Conduct Usability Testing 4. Fine-tuning of chat responses 5. Presentation(s) and demonstration(s) of proposed solution to IBF management and team leads for endorsement			
3.	**Stage 3 – Integration with IBF Website**			
3.1	**Timeline – 1 weeks** 1. Integration with IBF website 2. Conduct SIT and UAT 3. Conduct VAPT and remediation			
4.	**Stage 4 – Production Deployment**			
4.1	**Timeline – 1 weeks** 1. Production deployment of the Chatbot			
5.	**Stage 5 – Staff Training and Change Management**			
5.1	**Timeline – 3 Days**			

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. Preparation and confirmation of User Guide 2. User training 3. Change communications plan and management			
6.	**Project Deliverables: Phase 2 – Other JTMs**			
6.1	**After Sept 2024** 1. Other JTM studies to be uploaded to the model			

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	Year 1 (in SGD $) (exclude GST)
1. Professional services fee Please provide a detailed breakdown based on the deliverables for user requirements gathering, platform configuration, design, data preparation, SIT, UAT, integration production deployment, staff training, change communications plan, optional items as mentioned in the RFP and any other project overheads broken down by phased implementation.	
2. Platform, hosting, model subscription fees on per annum basis including implementation with detailed breakdown based on following: (i) Low Range: up to 5,000 interactions per month (ii) Mid Range: 5,000 - 10,000 interactions per month (iii) High Range: 10,000+ interactions per month.	
3. Service support a) Please state scope of services and estimated man-days for both office and non-office hours	
4. Ad hoc Change Requests a) Please state scope of services and man-day rate for both office and non-office hours	
5. Any other miscellaneous costs a) Please state clearly on intent and in man-hours/monthly/annual costs where applicable)	
6. **Optional** cost with detailed breakdown on the migration of the chatbot back to IBF cloud environment at a later date	
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	

Instructions

1. This security checklist should be completed by senior officers who have direct knowledge of the information systems and operations. The information provided in this checklist should be reviewed by their superiors.

2. For each guideline description, place an “X” in the appropriate column to indicate whether the financial institution 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. Evidence of Vulnerability Assessment and Penetration Testing, Configuration Assessment for Cloud systems, and Incident Management Plan to be attached together with this submission.

5. System and Organization Controls Report (preferably SOC 2 plus) and Outsourced Service Provider Audit Report (OSPAR) will have to be attached together with this submission.

S/N	Risk Category	Full Compliance	Partial Compliance	Non-compliance	N.A.	Comments
1	**Usage Risk**					
1.1	TLS 1.2 or latest version is implemented to provide communication security. (Adopted from MAS TRM E.2.5)					
1.2	Application(s) and database(s) are physically hosted in Singapore.					
1.3	The Service Provider has established a disaster recovery contingency framework which defines its roles and responsibilities for documenting, maintaining and testing its contingency plans and recovery procedures. (Adopted from MAS TRM 5.1.7)				N.A	
1.4	A data backup strategy is developed for the storage of critical information on a regular basis. (Adopted from MAS TRM 8.4.1)					
1.5	Periodic testing and validation of the recovery capability of backup media is carried out. (Adopted from MAS TRM 8.4.3)					
1.6	Service Provider provides logging details via download or through a web application for:					
	User to role/privilege mapping					
	User activity					
	Administrative activity					
1.7	Service Provider has achieved compliance certifications. (please indicate certification, e.g. PCI Compliance, STAR, SAS70/SSAE16-3)					

1.8	Service Provider has completed the Cloud Security Alliance (CSA) self-assessment or Consensus Assessments Initiative Questionnaire (CAIQ).					
1.9	Service Provider conforms to a specific industry standard security framework, e.g. NIST Cyber Security Framework or ISO 27001.					
1.10	Service Provider has a dedicated Information Security office or staff.					
1.11	Service Provider has not suffered any significant breaches in the last 5 years.					
1.12	All components of the disaster recovery plan are reviewed at least annually and updated as needed.					
1.13	Service Provider has a formal incident response plan.					
2	**Application Risk**					
2.1	Mobile and Desktop application do not store data on devices. (e.g. PII, confidential data)					
2.2	Service Provider complies with GDPR and PDPA.					
2.3	Annual Vulnerability Assessment and Penetration Test (VAPT) is performed and provides annual report.					
2.4	Penetration testing is conducted prior to the commissioning of a new modules/enhancements which offers internet accessibility and open network interfaces. (Adopted from MAS TRM 6.2.4)					
2.5	Application supports role-based access control (RBAC) for end-users.					
2.6	Application and infrastructure support role-based access control (RBAC) for system administrators.					
2.7	Application and infrastructure support password/passphrase aging.					

2.8	Audit logs minimally include the following: login, logout, actions performed, and source IP address.					
2.9	Service Provider has existing policies and/or procedures guiding how security risks are mitigated until patches can be applied.					
2.10	Vulnerabilities discovered in the systems or applications are remediated prior to release.					
3	**Data Security Risk**					
3.1	Data resides physically in Singapore.					
3.2	Service Provider to promptly remove or destroy data stored at the Service Provider's systems and backups in the event of contract termination and provide a certification. (Adopted from MAS TRM 5.2.4)					
3.3	The data loss prevention strategy and encryption takes into consideration the following: (Adopted from MAS TRM 9.1.2)					
	a) Data at endpoint - Data which resides in notebooks, personal computers, portable storage devices and mobile devices;					
	b. Data in motion - Data that traverses a network or that is transported between sites; and					
	c. Data at rest - Data in computer storage which includes files stored on servers, databases, back-up media and storage platforms.					
3.4	Service Provider do not have access to IBF's data (unless specifically authorised by IBF Management on a case-by-case basis).					
3.5	The Service Provider is able to isolate and clearly identify IBF's data and other information system assets for protection. (Adopted from MAS TRM 5.2.3)					

3.6	Measures are implemented to protect sensitive or confidential information such as personal, account and transaction data which are stored and processed in systems. (Adopted from MAS TRM 9.0.2)					
3.7	IBF is properly authenticated before access to online transaction functions and sensitive personal or account information is permitted. (Adopted from MAS TRM 9.0.2)					
3.8	Only encryption algorithms which are of well-established international standards are adopted. (Adopted from MAS TRM 12.1.3)					
3.9	Monitoring or surveillance systems are implemented so that the organisation can be alerted of any abnormal system activities, transmission errors or unusual online transactions. (Adopted from MAS TRM 12.1.5)					
3.10	Service Provider has a data privacy policy.					
3.11	Sensitive data is encrypted in transit (e.g. system to client).					
3.12	Sensitive data is encrypted in storage (i.e. at rest).					
3.13	The database supports encryption of specified data elements in storage.					
3.14	Service Provider has an existing documented media handling process covering, but not limited to, end-of-life, repurposing, and data sanitisation procedures.					
3.15	Service Provider owns the physical hosting location (e.g. data centre) where IBF's data will reside.					
3.16	Service Provider has obtained Systems and Organisation Controls (SOC) 2 Type II certification for the hosting location.					

3.17	Service Provider has implemented a physical barrier in the hosting location to fully enclose the physical space preventing unauthorised physical contact with any of the devices inside.					
3.18	Service Provider has physical security controls and policies in place to protect the hosting location.					
3.19	Employees of Service Provider are not allowed or able to take home any assets in any form (including any hardware, software or data) belonging to IBF.					
4	**IT Service Management**					
4.1	Service Provider provides Service Level Agreement (SLA).					
4.2	Service Provider to support and assist in audit activity by providing necessary documents upon request. (Adopted from MAS TRM 5.1.3)					
4.3	The Service Provider is required to employ a high standard of care and diligence in its security policies, procedures and controls to protect the confidentiality and security of IBF's sensitive or confidential information, such as personal data, computer files, records, object programs and source codes. (adopted from MAS TRM 5.1.4)					
4.4	IBF is kept informed of any major incident. (Adopted from MAS TRM 7.3.9)					
4.5	IBF is kept informed of any enhancement to the system.					
4.6	A root-cause and impact analysis is performed for major incidents which result in severe disruption of IT services. (Adopted from MAS TRM 7.3.10)					
4.7	Employees of Service Provider are subjected to close supervision, monitoring and access restrictions. (Adopted from MAS TRM 11.1.2)					

4.8	Service Provider's access privileges to support/maintain the system are regularly reviewed to verify that privileges are granted appropriately and according to the 'least privilege' principle. (Adopted from MAS TRM 11.1.4)					
4.9	Service Provider has a documented and currently followed change management process (CMP).					
4.10	Service Provider has monitoring in place for Next-Generation Persistent Threats (NGPT).					
4.11	Service Provider monitors for intrusions on a 24x7x365 basis.					
4.12	A separate management network is used for the administration of the system or service.					