ANNEX A: PROPOSAL

Project Name:

RFP.CE.2022.0080
Provision of IBF Virtual Career Platform Services

Name of Corporate Entity:

For Internal (IBF) Use only
Date Received:
Officer-in-charge:

USEFUL NOTES

(A) Submission of Quotation

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 **"**Provision of IBF Virtual Career Platform Services **(**RFP.CE.2022.0080**)",** and addressed to:

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

(B) Structure of the Quotation

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.

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) Any other relevant reports or information available.

PART II – DETAILS OF PROPOSED PROJECT

A) 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.	**Base Services**			
1.1	Provide Virtual Career Fair Platform Services for two (2) years to host up to six (6) virtual career fairs.			
1.2	Provide platform training and user guide and how to videos for IBF administrators and partners			

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.	**Security Measures**			
1.1	Contractor shall submit a report to IBF before the launch of the platform, and thereafter on a yearly basis: (i) Vulnerability Assessment and Penetration Testing (VAPT) White box testing performed by an independent, CREST certified party conducted on the platform; and (ii) Rectification of all			

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
	identified security gaps. (iii) Source code scan			
1.2	Contractor shall propose appropriate BCP and data backup measures and frequency to ensure minimum disruption and data loss to business operations.			
1.3	The Contractor shall ensure it has sufficient security controls in place and met ISO 27001, ISO 27017 and ISO 27018, SOC2, NIST or any other relevant security framework. Contractor shall ensure that data in transit and at rest is protected/encrypted. Transport Layer Security (TLS) version 1.2 or later shall be implemented for secure transmission of data online via major browsers.			
1.4	Ensure that certificates used are of minimum SHA256 algorithm.			
1.5	The Contractor shall conduct configuration management review on regular basis and validated by external auditor and provide report to IBF for review.			
2.	**Data Governance**			

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	IBF has full ownership of all customer data and reference materials in the CMS. All data disclosure to third parties, retention and disposal by Contractor shall be subjected to IBF's approval.			
2.2	The Contractor 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 Contractor shall sign the Non-Disclosure and Undertaking Agreement (NDA) not to access, use, share, divulge or retain data unless this is required by the Contractor's staff in discharging their duties during their employment. The NDA is binding even if the personnel 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			

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
	Contractor by IBF and/or will be referred to relevant authorities.			
3.	**Availability**			
3.1	The online platform shall be required to run continuously for 24 hours a day, during the stipulated event period including Saturdays, Sundays, and Public Holidays. The Service Availability Level shall not be less than 99.5% for each calendar month, except during the time when the online platform is shut down for maintenance. Such maintenance shall be planned and subjected to approval by IBF.			
3.2	The online platform shall provision for up to 100GB for the hosting of the resources to be published on the online platform by IBF and its partner.			
3.3	Ability to meet required response time as per stated in para 4.18 in requirements 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
4.	**Technical and User Support Requirements**			
4.1	The Contractor shall provide Helpdesk support (preferably local) for the online platform conforming to all IBF business hours. For all issues reported by the users or by IBF, Contractor should adhere to response time as prescribed by IBF. An issue or incident is deemed resolved when the reporting party is notified and satisfied with the resolution steps taken by the Vendor.			
5.	**Multi Devices and Browsers Support**			
5.1	The Contractor shall provide online platform to be compatible with the most widely adopted browsers and mobile devices (e.g., Android, iOS, and Windows) and is capable of rendering contents and pages for proper display and access from different users' devices such as mobile phones, laptops etc			

c) Optional Services

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
1.1	Provide design services to create the entire event platform with six (6) different thematic templates for virtual career fairs			
1.2	Provide gamification proposal for each VCF based on project needs			

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 – Base Services

Item	Fee Quote in S$ (Mandatory to quote, optional for IBF to purchase)			
	Year 1	Year 2	Year 3	Year 4
1. Provide Virtual Career Fair Platform Services for two (2) years to host up to six (6) virtual career fairs. a) Please provide cost for each event as contractor will be paid upon completion of each VCF.				
2. Provide platform training and user guide for IBF administrators				
3. Provide pre-event briefing and user guide to all participating partners				

4. Provide technical support services				
5. Hosting fees (if applicable)				
6. License fee (if applicable)				
7. Subscription fee (if applicable)				
8. Any other costs a) Please state clearly on intent and in manhours/monthly/annual costs where applicable)				
Total Cost				

Project Fee Quotation Template – Optional Services

Item	Fee Quote in S$ (Mandatory to quote)		Fee Quote in S$ (Mandatory to quote, optional for IBF to purchase)	
	Year 1	Year 2	Year 3	Year 4
1. Provide design services to create the entire event platform with six (6) different thematic templates for virtual career fairs a) Please provide cost of each event as contractor will be paid only upon utilisation				
2. Provide gamification proposal for each VCF a) Please provide breakdown if 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 Contractor s 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 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.

3. 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.

4. 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).

5. 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).

6. 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.

7. 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.

8. 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	Recent released version of Transport Layer Security (minimally TLS version 1.2 or later) is implemented to provide communication security. (Adopted from MAS TRM E.2.5)					
1.2	Application and database 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)					
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)					

S/N	Risk Category	Full Compliance	Partial Compliance	Non-compliance	N.A.	Comments
1.6	Service provider provide logging is available to IBF 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.					

S/N	Risk Category	Full Compliance	Partial Compliance	Non-compliance	N.A.	Comments
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.					
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)					

S/N	Risk Category	Full Compliance	Partial Compliance	Non-compliance	N.A.	Comments
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.					

S/N	Risk Category	Full Compliance	Partial Compliance	Non-compliance	N.A.	Comments
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 take 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 does not have access to IBF's data.					
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)					

S/N	Risk Category	Full Compliance	Partial Compliance	Non-compliance	N.A.	Comments
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)					

S/N	Risk Category	Full Compliance	Partial Compliance	Non-compliance	N.A.	Comments
3.10	Service Provider has a data privacy policy.					
3.11	Sensitive data is encrypted in transit (e.g. system to client).					
3.12	Service Provider has an existing documented media handling process covering, but not limited to, end-of-life, repurposing, and data sanitisation procedures.					
3.13	Service Provider owns the physical hosting location (e.g. data centre) where IBF's data will reside.					
3.14	Service Provider has obtained Systems and Organisation Controls (SOC) 2 Type II certification for the hosting location.					
3.15	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.					
3.16	Service Provider has physical security controls and policies in place to protect the hosting location.					

S/N	Risk Category	Full Compliance	Partial Compliance	Non-compliance	N.A.	Comments
3.17	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)					

S/N	Risk Category	Full Compliance	Partial Compliance	Non-compliance	N.A.	Comments
4.5	IBF is kept informed of any enhancement to the system.					
4.6	A root-cause and impact analysis are 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).					

S/N	Risk Category	Full Compliance	Partial Compliance	Non-compliance	N.A.	Comments
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.					