PUBLIC DOCUMENT

REQUEST FOR PROPOSAL

Project Name:

Provision of Managed Services
RFP.TDT.2025.001

The Institute of Banking & Finance
10 Shenton Way
#13-07/08 MAS Building
Singapore 079117
Tel: 62208566
Fax: 62244947
Email: procurement@ibf.org.sg

CONTENTS

1. INTRODUCTION

1.1 The Institute of Banking and Finance ("IBF") is issuing this Request for Proposal ("RFP") to identify suitable entity(ies) (hereinafter referred to as the "Vendor") to submit proposals for Provision of Managed Services.

2. BACKGROUND

2.1 The Institute of Banking and Finance Singapore (IBF) was established in 1974 as a not-for-profit industry association to foster and develop the professional competencies of the financial industry. IBF represents the interests of close to 200 financial institutions including banks, insurance companies, securities brokerages and asset management firms. In partnership with the financial industry, government agencies, training providers and the trade unions, IBF is committed to equip practitioners with capabilities to support the growth of Singapore's financial industry.

2.2 IBF is the national accreditation and certification agency for financial industry competency in Singapore under the IBF Standards, which were developed in partnership with the industry. The IBF Standards set out the functional skills required for job roles in the financial industry, guiding IBF's accreditation of structured skills training programmes. Individuals who complete the IBF-accredited skills training programmes and meet the relevant criteria may apply for IBF Certification.

2.3 Since 2018, IBF has been the appointed programme manager for the administration of career conversion programmes for the financial industry. As programme manager, IBF will partner financial institutions to re-skill employees for expanded roles and opportunities in growth areas.

2.4 IBF also provides personalised career advisory and job matching services to locals exploring a new role in, or career switch into the financial industry, under IBF Careers Connect.

3. SCOPE OF SERVICES

Provide both online and onsite (resource will be onsite as part of IBF's IT team) end user support at IBF offices (IBF main office and IBF Assessment Center (IAC)) for all user requests. The 1st point of call shall be provided by the online services, failing which or if the situation requires onsite support, the onsite staff shall be activated. The service includes Level 1 support services such as basic troubleshooting of audio & visual equipment, application and IT devices, laptop provisioning/migration, service request processing, user access and asset management, service management as well as assisting IBF IT staff in event/incident management.

3.1 Vendors are invited to quote for the provision of Managed Services in End-User Computing area to meet IBF's requirements as stated below.

a. Services provision

Vendor will deliver Level 1 support services in the following areas:

i. Basic Troubleshooting, Laptop Provisioning and Migration

- Device Issues: Troubleshoot and resolve basic hardware and network connectivity issues, such as mobile, desktops, laptops and projectors and audio devices.
- Software Issues: Resolve common software problems such as operating systems, office applications, and email clients.
- Laptop Provisioning: Prepare the new laptop by installing all the necessary software on one new laptop and sent to the vendor for cloning. This exercise will be conducted 2 times a year.
- Laptop Replacement/Migration: Assist IBF employees on replacing and migrating their old laptop to new laptop and guide them on the data backup and migration process.
- Ensure secure wiping and reimaging of laptops and devices returned by staff, ensuring all data is completely removed and devices are ready for redeployment without compromising data security.

ii. Service Request Fulfilment

- Processing Requests: Handle service requests such as software installations, password resets, and access permissions.
- Request Tracking: Track and manage service requests to ensure timely fulfilment.

iii. User Access Management

- User Account Management: Create, modify, unlock and deactivate user accounts as per organizational policies.
- Permissions Management: Manage approved user access changes and permissions for applications and data.
- Documentation Management: Ensure processes are in line with IT policy and comply with audit requirements.

iv. Asset Management

- Maintain an accurate and up-to-date inventory of all IT assets, including hardware, software, and licenses and reported to IBF.
- Monitor the physical location, usage, and performance of IT assets, enabling quick identification of issues or inefficiencies and reported to IBF.
- Ensure routine maintenance is performed, with proactive support to prevent downtime and address any asset-related issues swiftly.

- Work with vendor to ensure secure disposal or degaussing of assets, especially those containing sensitive data, in compliance with data protection regulations to prevent data breaches.
- Batch replacement of laptops will be done for up to 2 times per year.
- Issuance or replacement of laptops for new employees or those experiencing issues.

v. Escalation Management

- Escalation Process: Identify incidents and requests that are beyond L1 support and escalate to L2 support in IBF’s IT Team or vendor L2 support accordingly.

vi. Service Management

- Diagnosis: Perform diagnosis and resolve the incident using standard procedures.
- Resolution and Recovery: Resolve incidents within the scope of Level 1 capabilities, otherwise, escalate to Level 2 support.
- Communication: Keep users informed about the status of their incidents.
- Logging and Categorization: Record all support incidents reported by end users, categorize them based on priority and impact, and document resolution for closure.

vii. Reporting

- Incident and Request Reports: Generate monthly reports on incidents and service requests, including resolution times based out of the provided ticketing system.
- Monthly meeting to discuss on service management with IBF.
- Knowledge Base Maintenance: Maintain and update a knowledge base of common issues and solutions.

b. Ticketing System Provision

I. Vendor will provide a case/service management system for enhanced tracking, status update, resolution and closure using a publicly available SaaS platform hosted in Singapore. The case management system will be accessible over web and provided to all the IBF staff to log cases. The IBF L2 IT staff will be provided with a higher user access which allow them to update the cases.

II. Ticket creation to have multiple options (e.g. email, browser or phone calls)

III. Necessary security controls (e.g. MFA and audit trail etc) must be implemented to ensure that access controls are effective and vulnerabilities (on ticketing system) are managed appropriately.

IV. Provide evidence on an annual basis that comprehensive Vulnerability Assessment and Penetration Testing (VAPT) are performed by certified independent vendor and personnel (CREST, etc) and all vulnerabilities are remediated promptly.

c. Service Hours

i. Online Support

- Mondays to Fridays: 0830hrs to 1800hrs (Singapore Time) exclude Singapore public holidays.
- The support will be provided over a local hotline, email or Microsoft Teams call.

ii. One Onsite Support (to be residing in IAC during exam sessions else will be in IBF office)

- Mondays to Fridays from 0830hrs to 1800hrs (Singapore Time) exclude Singapore public holidays
- Replacement of staff if assigned staff is on leave or MC.

d. Service Levels and Performance Metrics

The following support SLAs will be provided for:

S/N	**Type of Service**	**SLA**
1	Response to tickets	Within 1 hr
2	Case resolution time	Within 3 days (approval for extension by IBF on a case-by-case basis)
3	Creation of user account	3 days upon approval
4	Unlock of user account	Within 30 mins
5	Onboarding and Access Change Request	Minimum 1 week before the staff come onboard or require access changes
6	Removal of user account	To be performed on the last day of employment of user

Refer to **Annex 1 Part II – Requirement Specifications** for the detailed project requirements.

3.2 Assumptions

- There is a total of 140 end user devices which are required to be supported.
- Estimated 30 cases per month which are needed to be supported and more than 80% of these cases can be resolved remotely by L1.
- The case management system will be a publicly available SaaS platform

- IBF will provide the office space for the onsite staff support who will be part of IBF IT team
- IBF will provide access rights to Vendor's staff to relevant systems to provide L1 support
- IBF will provide laptop/VPN and/or remote access to the relevant systems to provide L1 support
- There is no migration of any reports or data from current L1 ticketing system
- Subjected to security clearance for the Managed Services onsite staff

3.3 The Vendor is required to submit a proposal with reference to **'Submission Details' under Paragraph 5**, using the template under **Annex 1: Proposal Template**.

4. EVALUATION CRITERIA

4.1 The following are the criteria and weightage (%) used to evaluate all proposals received by IBF for this RFP:

a) Ability to provide a proposal that fulfils IBF's project objectives, timeline and scope of services (40%);
b) Vendor's experience and track record (20%);
c) Price competitiveness (40%).

4.2 IBF may evaluate based on the proposals submitted by Vendors and any other information provided by Vendors at the request of IBF, pursuant to the proposal submission.

4.3 As part of the evaluation process, shortlisted Vendors may be required to present their credentials, proposals to IBF management and to provide an online demonstration of their proposed solution.

5. SUBMISSION DETAILS

5.1 The submitted proposal shall comprise:

a) An executive summary of the Vendor's understanding of IBF's project objectives and scope of services and how the Vendor's proposals will address IBF's requirements.
b) An illustrated detailed explanation of how the proposal will fulfil each requirement outlined in **Annex 1 Part II – Requirement Specifications**.
c) Details of proposal including project planning, execution, and reporting.
d) Experience and track record:
    i. Provide a brief on the company's demonstrated experience and track record on related projects to improve or optimise a client's enterprise architecture.
    ii. Provide two client references for feedback on services delivered for related past projects.
    iii. Provide a brief on the qualifications, relevant certifications and experiences of the staff assigned to the project and describe their respective roles in the project team. Please

provide the curriculum vitae (“CV”) of the assigned staff as supporting documents to the brief.

iv. Provide assurance that the assigned staff must be able to communicate fluently in English and be physically located in Singapore.

e) Proposed fees:

i. Provide quotations for fees using the ‘Proposal Template’ under **Annex 1 Part III – Project Costs & Fees**.

ii. Fees quoted shall be in Singapore Dollars only and exclude GST. All fees quoted shall be final and shall include the cost of patches and after-sales services, and all fees shall remain the same throughout the Initial Contract Period.

f) Signed **‘Non-Disclosure and Security Awareness Undertaking’** under **Annex 1 Part VI** as confidential information may be provided by IBF during the RFP process.

g) Fully completed and signed **‘IBF IT Service Provider Checklist’ under Annex 1 Part VII**.

5.2 The submitted proposal shall include the reference **‘RFP.TDT.2025.001’** and must be clearly marked as **‘Provision of Managed Services’.**

5.3 Soft copy (in PDF format) of the proposal submission to be duly completed shall reach IBF **no later than 28 Feb 2025, 5pm**. Please send the proposal submission to the following email address:

Attention: IBF Procurement
Email: procurement@ibf.org.sg (do not cc/bcc any other IBF emails)

5.4 All proposals submitted will remain confidential. IBF reserves the right not to accept late submissions.

5.5 In the event that IBF seeks clarifications on the proposal, the Vendor shall provide full and comprehensive responses within three (3) days of notification.

5.6 IBF reserves the right to cancel or modify in any form, this RFP for any reason, without any liability to IBF.

6. RIGHTS TO THE PROJECT DELIVERABLES

6.1 Materials, findings, studies, and reports arising from work on the various tasks in this project are strictly and solely the properties and rights of IBF. Reproduction, in whole or in part, of any of these materials, findings, studies and reports by the successful Vendor, its associates, representatives or any third party deemed to be connected to the successful bid, in any context is strictly prohibited and liable to legal action by IBF.

7. EXPENSES

7.1 The Vendor shall bear all out-of-pocket expenses incurred.

7.2 Withholding tax or taxes of any nature, if any, shall be borne by the successful Vendor.

8. PAYMENT

8.1 The appointed Vendor shall comply with the following payment schedule outlined by IBF:

8.1.1 **Quarterly Payment Structure**

The payment for the IT Managed Services shall be structured into quarterly instalments to align with the service delivery periods.

- **Billing Schedule**
  The Vendor shall issue invoices at the beginning of each quarter, specifically on the following dates: 1st January 1st April 1st July and 1st October.

- **Billing Frequency**
  The total contract value for the 3-year term shall be divided into equal quarterly payments, where possible.

- **First and Last Invoices**
  If the contract start date does not coincide with the start of a quarter, the Vendor shall issue the first invoice covering the period from the contract start date to the end of that quarter. Likewise, if the contract end date does not coincide with the end of a quarter, the final invoice shall cover the period from the start of the final quarter to the contract end date.

  All other invoices will adhere to the standard quarterly schedule as follows: Q1: January–March, Q2: April–June, Q3: July–September, Q4: October–December.

8.1.2 **Provisions for Adjustments**

- Adjustments to payments may be made based on any agreed changes in the scope of services or SLAs.
- Any additional ad-hoc services beyond the scope shall be invoiced separately with prior approval.

8.1.3 **Termination Clause**

In the event of early contract termination, payments shall be prorated to reflect services rendered up to the termination date, subject to the terms outlined in the agreement.

9. CONFIDENTIALITY

9.1 The Vendor shall ensure the absolute confidentiality of the data and information provided by IBF or any other organisation identified by IBF for this project and shall not, under any circumstances, release or communicate through any means, in whole or in part, any information to any third parties. All correspondence and communication with all external parties, pertaining to matters relating to this project, shall be made only through IBF. The Vendor will be required to sign **a 'Non-Disclosure and Security Awareness Undertaking' under Annex 1 Part VI**.

9.2 IBF may require an unsuccessful Vendor to return all materials that IBF provided during the period from the issue of this RFP to the acceptance of the successful proposal.

10. DATA GOVERNANCE

10.1 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.

10.2 The 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.

10.3 The Vendor shall comply with all its obligations under the PDPA at its own cost.

10.4 The Vendor shall only process, use or disclose IBF's Customer Personal Data:

- strictly for the purposes of fulfilling its obligations and providing the services required under this Agreement;
- with IBF's prior written consent; or
- 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.

10.5 The Vendor shall not transfer IBF's Customer 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 IBF's Customer Personal Data transferred outside Singapore will be protected at a standard that is comparable to that under the PDPA. If the Vendor transfers IBF's Customer Personal Data to any third party overseas, the Vendor shall procure the same written undertaking from such third party.

10.6 The Vendor shall protect IBF's Customer 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:

- unauthorised or accidental access, collection, use, disclosure, copying, modification, disposal or destruction of IBF's Personal Data, or other similar risks; and
- the loss of any storage medium or device on which personal data is stored.

10.7 The Vendor shall only permit its authorised personnel to access IBF's Customer Personal Data on a need-to-know basis and access logs shall be furnished to IBF upon request.

10.8 The Vendor shall provide IBF with access to IBF's Customer Personal Data that the Vendor has in its possession or control, as soon as practicable upon IBF's written request.

10.9 Where IBF provides its Customer Personal Data to the Vendor, IBF shall make reasonable effort to ensure that the Customer 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 Customer 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 Customer Personal Data, as soon as practicable upon IBF's written request.

10.10 The Vendor shall not retain IBF's Customer Personal Data (or any documents or records containing IBF's Customer Personal Data, electronic or otherwise) for any period of time longer than is necessary to serve the purposes of this RFP.

10.11 The Vendor shall also facilitate IBF to comply with the obligation to review and maintain the Customer personal data database.

10.12 The Vendor shall, upon the request of IBF:

- return to IBF, all of IBF's Customer Personal Data; or
- delete all IBF's Customer Personal Data in its possession, and after returning or deleting all of IBF's Customer Personal Data, provide IBF with written confirmation that it no longer possesses any of IBF's Customer Personal Data. Where applicable, the Vendor shall also instruct all third parties to whom it has disclosed IBF's Customer Personal Data for the purposes of this Contract to return to the Vendor or delete, such IBF's Customer Personal Data.

10.13 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 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.

10.14 Vendor shall sign the Non-Disclosure and Undertaking 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.

11. SECURITY CLEARANCE

The Vendor shall subject all their personnel who will be involved in the performance of the Services to security clearance by IBF before commencing their work. IBF reserves the right to reject any of the Vendor's personnel and the Vendor is responsible for finding replacements immediately and at the Vendor's own expense.

The Vendor shall observe the secure usage and handling of all IBF's information. All the Vendor's personnel shall sign an Undertaking to Safeguard Official Information to protect IBF's information against unauthorised disclosures by the Vendor's personnel during the course of their work.

All the Vendor's personnel shall fully comply with any written instructions from IBF regarding security matters.

12. INDEMNITY AGAINST A THIRD PARTY

12.1 The Vendor shall indemnify and hold harmless IBF and its partners and employees from and against any foreseeable loss, expense, damage or liabilities (or actions that may be asserted by any third party) that may result from any third party, claims arising out of or in connection with the project or any use by the Vendor of any deliverable item under this project and will reimburse IBF for all costs and expenses (including legal fees) reasonably incurred by IBF in connection with any such action or claim.

13. ACCEPTANCE OR NON-ACCEPTANCE OF PROPOSAL

13.1 IBF shall be under no obligation to accept the lowest or any proposal received. It generally does not correspond with any Vendor regarding the reasons for non-acceptance of a proposal.

13.2 IBF reserves the right to award the contract in parts or in full.

13.3 The issue of a Letter of Acceptance by IBF accepting the proposal or part of the proposal submitted by a Vendor shall create a binding contract on the part of the Vendor to supply the specified deliverables in the proposal to IBF. The awarded Vendor shall provide a Master Purchase Agreement to be reviewed and agreed upon by both parties.

14. TERMINATION

14.1 IBF shall, after giving 7 days written notice to the Vendor, have the right to suspend or terminate this Contract if IBF is affected by any state of war, act of god or other circumstances seriously disrupting public safety, peace or good order of the Republic of Singapore. Neither party shall be liable to the other by reason of such suspension nor termination save that IBF pay the Vendor the price of the Goods or Services that have been performed and accepted by IBF. The Vendor shall refund the balance of any payments or deposits made after deducting any outstanding sums owing by IBF to the Vendor by reason of this Clause 14.

14.2 In addition to any other rights to terminate this Contract or any rights to cancel parts of the Services under this Contract, IBF shall have the unilateral right to terminate this Contract without assigning any reasons whatsoever by giving the Vendor 30 days' written notice. For the avoidance of doubt, the Vendor shall not be entitled to any compensation or damages whatsoever in relation to such a termination. The Vendor shall only be entitled to payment for any Services provided and accepted up to the end of the 30-day notice period.

15. NOTIFICATION OF UNSUCCESSFUL BID

15.1 Notification will not be sent to unsuccessful Vendors.

16. ENQUIRIES

16.1 All enquiries about this RFP may be addressed to the following email: tech@ibf.org.sg and cc procurement@ibf.org.sg with the following email subject starting with "**[RFP.TDT.2025.001]**"

ANNEX 1: PROPOSAL TEMPLATE

The Institute of Banking & Finance Singapore

Project Name:

Provision of Managed Services

RFP.TDT.2025.001

Name of Corporate Entity:

<u>For Internal (IBF) Use only</u>

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.

(B) Structure of the Quotation

The complete proposal consists of 6 parts:

Part I – Company Data

Part II – Requirement Specification

Part III – Project Costs & Fees

Part IV – Acceptance of Terms and Conditions

Part V – References / Other Considerations

Part VI – Non-disclosure and Security Awareness Undertaking (Third Parties)

Part VII – 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 copy of the latest updated ACRA search.
- Full set of the latest audited financial / management report for the last 1 year.
- Any other relevant reports or information available.

PART II – REQUIREMENT SPECIFICATIONS

In addition to the proposal, Vendors shall complete the table below.

S/No	Proposal Details	Able to Deliver? (Yes/No)	If Yes, please provide brief description and cite the relevant section of your proposal here	If No, please provide the reasons
A	**SERVICE PROVISION OVERVIEW AND TICKETING SYSTEM IMPLEMENTATION**			
	Services provision **Vendor shall deliver Level 1 support services in the following areas:**			
(i)	Basic Troubleshooting, Laptop Provisioning and Migration			
1	Device Issues: Troubleshoot and resolve basic hardware and network connectivity issues, such as mobile, desktops, laptops and projectors and audio devices.			
2	Software Issues: Resolve common software problems such as operating systems, office applications, and email clients.			
3	Laptop Provisioning: Prepare the new laptop by installing all the necessary software on one new laptop and sent to the vendor for cloning. This exercise shall be conducted 2 times a year.			
4	Laptop Replacement/Migration: Assist IBF employees on replacing and migrating their old laptop to new laptop and guide them on the data backup and migration process.			
5	Ensure secure wiping and reimaging of laptops and devices returned by staff, ensuring all data is completely removed and devices are ready for redeployment without compromising data security.			
(ii)	Service Request Fulfilment			
6	Processing Requests: Handle service requests such as software installations, password resets, and access permissions.			
7	Request Tracking: Track and manage service requests to ensure timely fulfilment.			
(iii)	User Access Management			
8	User Account Management: Create, modify, unlock and deactivate user accounts as per organisational policies.			
9	Permissions Management: Manage approved user access changes and permissions for applications and data.			
10	Documentation Management: Ensure processes are in line with IT policy and comply with audit requirements.			
(iv)	Asset Management			
11	Maintain an accurate and up-to-date inventory of all IT assets, including hardware, software, and licenses and reported to IBF.			
12	Monitor the physical location, usage, and performance of IT assets, enabling quick identification of issues or inefficiencies and reported to IBF.			
13	Ensure routine maintenance is performed, with proactive support to prevent downtime and address any asset-related issues swiftly.			
14	Work with vendor to ensure secure disposal or degaussing of assets, especially those containing sensitive data, in compliance with data protection regulations to prevent data breaches.			
15	Batch replacement of laptops shall be done for up to 2 times per year.			
16	Issuance or replacement of laptops for new employees or those experiencing issues.			
(v)	Escalation Management			
17	Escalation Process: Identify incidents and requests that are beyond L1 support and escalate to L2 support in IBF's IT Team accordingly.			
(vi)	Incident Management			
18	Diagnosis: Perform diagnosis and resolve the incident using standard procedures.			
19	Resolution and Recovery: Resolve incidents within the scope of Level 1 capabilities, otherwise, escalate to Level 2 support.			
20	Communication: Keep users informed about the status of their incidents.			
21	Logging and Categorization: Record all incidents reported by end users, categorise them based on priority and impact, and document resolution for closure.			
(vii)	Reporting			

S/No	Proposal Details	Able to Deliver? (Yes/No)	If Yes, please provide brief description and cite the relevant section of your proposal here	If No, please provide the reasons
22	Incident and Request Reports: Generate monthly reports on incidents and service requests, including resolution times based out of the provided ticketing system			
23	Monthly meeting to discuss on service management with IBF			
24	Knowledge Base Maintenance: Maintain and update a knowledge base of common issues and solutions.			
	Ticketing System Provision			
25	Vendor shall provide a case management system for enhanced tracking, status update, resolution and closure using a platform hosted in Singapore. The case management system shall be accessible over the web and provided to all the IBF staff to log cases. The IBF L2 IT staff shall be provided with higher user access which allow them to update the cases.			
26	Ticket creation to have multiple options (e.g. email, browser or phone calls)			
27	Necessary security controls (e.g. MFA and audit trail etc) must be implemented to ensure that access controls are effective, and vulnerabilities (on the ticketing system) are managed appropriately.			
28	Provide evidence on an annual basis that comprehensive Vulnerability Assessment and Penetration Testing (VAPT) are performed by certified independent vendor and personnel (CREST, etc) and all vulnerabilities are remediated promptly.			
B	**SERVICE HOURS**			
	Online Support			
29	Mondays to Fridays: 0830hrs to 1800hrs (Singapore Time) exclude Singapore public holidays.			
30	The support shall be provided over a local hotline, email or Microsoft Teams call.			
	Onsite Support			
31	Mondays to Fridays from 0830hrs to 1800hrs (Singapore Time) exclude Singapore public holidays			
32	Replacement of staff if assigned staff is on leave or MC			
C	**SERVICE LEVELS AND PERFORMANCE METRICS**			
33	Response to tickets Within 1 hr			
34	Case resolution time Within 3 days (approval for extension by IBF on a case-by-case basis)			
35	Creation of user account: 3 days upon approval			
36	Unlock of user account: Within 30 mins (during office hours)			
37	Onboarding and Access Change Request: Before staff come onboard or require access changes			
38	Removal of user account: To be performed by the last day service of user			

PART III – PROJECT COSTS & FEES

It is **mandatory** to quote for all items stated below, N.A. or zero will be required if item is not required or available. Vendors shall complete the table below. All costs must be quoted in Singapore Dollars excluding GST.

		Pricing in SGD (exclude GST)			
S/No	**Item Description**	**One-Time Cost (if any)**	**Year 1**	**Year 2**	**Year 3**
1.	Managed Services Listed in **Annex 1 Part II - Requirement Specifications**				
2.	Ad-hoc services beyond the scope				
	Total Costing				

PART IV – ACCEPTANCE OF TERMS AND CONDITIONS

Should your firm require any exceptions to any specifications, terms, or conditions of this RFP or offer substitutions, please explicitly state the exception(s), reasons(s), and language substitute(s) (if any) in this section of the proposal response.

Failure to take exception(s) shall mean that the proposer accepts the conditions, terms, and specifications of the RFP. If your firm takes no exception to the specifications, terms, and conditions of this RFP, please indicate so.

Signed By: ______________________

Name: ______________________

Title: ______________________

Date: ______________________

PART V – REFERENCES / OTHER CONSIDERATIONS

Please indicate reference or highlight any other useful factors you would like us to consider in reviewing your quotation.

PART VI – NON-DISCLOSURE AND SECURITY AWARENESS 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. VENDOR / SERVICE PROVIDER'S DETAILS

1.	**Name of Vendor / 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 any and 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 VII – 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]

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 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 (Ticketing System) attained security-related compliance (SOC-2 Type 2 (preferred) or					

S/N	Risk Category	Full Compliance	Partial Compliance	Non-Compliance	N.A.	Comments
	other equivalent)? Attach the necessary report to show the security assurance. 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	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.					
2.7	Service Provider has not suffered any significant breaches in the last 5 years.					
3	**Data Security (applicable to Ticketing System)**					
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 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?					

S/N	Risk Category	Full Compliance	Partial Compliance	Non-Compliance	N.A.	Comments
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 (applicable to Ticketing System)**					
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?					
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 (e.g. most recent penetration test reports).					

S/N	Risk Category	Full Compliance	Partial Compliance	Non-Compliance	N.A.	Comments
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 unauthorised access?					
4.7	Does the service provide strong authentication controls (e.g. MFA) before service can be accessed?					
4.8	Does the application support role-based access control (RBAC) to segregate distinct functions and roles such as for end-users and administrators					
4.9	Does the service support ease of review or automated handling of inactive/dormant accounts?					
4.10	Is audit logging turn on (e.g. login, logout, actions performed) and the security logs accessible/retrievable or can be sent to SIEM?					
4.11	Does the service provider monitor the security of the system on a 24x7x365 basis?					