**PUBLIC DOCUMENT**

**REQUEST FOR PROPOSAL**

**Project Name:**

**Provision of Robotic Process Automation Solution (Automation Anywhere) Maintenance and Professional Services**

**RFP.IT.2023.0030**



**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 3](#_Toc142921027)

[2. BACKGROUND 3](#_Toc142921028)

[3. SCOPE OF SERVICES 4](#_Toc142921029)

[4. EVALUATION CRITERIA 4](#_Toc142921030)

[5. SUBMISSION DETAILS 5](#_Toc142921031)

[6. BRIEFING 6](#_Toc142921032)

[7. RIGHTS TO THE PROJECT DELIVERABLES 6](#_Toc142921033)

[8. INTELLECTUAL PROPERTY 7](#_Toc142921034)

[9. EXPENSES 7](#_Toc142921035)

[10. PAYMENT 7](#_Toc142921036)

[11. CONFIDENTIALITY 7](#_Toc142921037)

[12. SECURITY CLEARANCE 7](#_Toc142921038)

[13. INDEMNITY AGAINST A THIRD PARTY 8](#_Toc142921039)

[14. ACCEPTANCE OR NON-ACCEPTANCE OF PROPOSAL 8](#_Toc142921040)

[15. NOTIFICATION OF UNSUCCESSFUL BID 8](#_Toc142921041)

[16. ENQUIRIES 9](#_Toc142921042)

[ANNEX 1: PROPOSAL TEMPLATE 10](#_Toc142921043)

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 a Automation Anywhere Robotic Process Automation solution (hereinafter referred to as the “AA RPA”) and associated professional services (hereinafter referred to as the “Services”).

1.2 The objective is to is to continue the services of the current IBF AA RPA solution to increase operational efficiency for selected business processes over a period of twenty-four (24) months (hereinafter referred to as the “Initial Contract Period”).

1.3 IBF shall have the option to extend the Initial Contract Period by one or more periods to be determined at IBF’s sole discretion provided always that the cumulative period of extension(s) shall not exceed twelve (12) calendar months in total, on the same terms and conditions, and any other terms that may be mutually agreed by the IBF and the Vendor in writing. IBF shall exercise such option by giving written notice to the Vendor at any time before the expiry of the Initial Contract Period or any extensions thereof.

1. 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 12 industry segments and more than 50 jobs 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.

* 1. Under Workforce Singapore’s Adapt and Grow initiative, IBF is the appointed programme manager for the administration of professional 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. IBF also provides personalised career advisory and job matching services to Singapore Citizens and Singapore Permanent Residents exploring a new role in, or career switch into the financial industry, under IBF Careers Connect.
	3. IBF has onboarded AA RPA since 2019 and recently in Feb 2023, the AA RPA platform was upgraded from v11 to Automation 360 and hosted on-premises. It is mainly used by Training Grant & Finance Division (“TGF”) for Account Receivables (“AR”) automation, and Workforce & Talent Development Division (“WTD”) for Technology in Finance Immersion Programme (“TFIP”) and Wealth Management Accelerator Programme (“WMAP”) automation.

# 3. SCOPE OF SERVICES

3.1 Vendors are invited to quote for the provision of AA RPA and related services to meet IBF needs as stated above.

3.2 Vendors shall propose AA RPA solution only.

3.3 Vendors may propose generative AI and the relevant licences required.

3.4 Vendor may review the current IBF AA RPA processes and propose the addition of generative AI for improvement.

3.5 The Vendor is required to submit a proposal with reference to ‘[Submission Details’](#_6._SUBMISSION_DETAILS) under Paragraph 5, and using the template under [**Annex 1: Proposal Template**](#_ANNEX_2:_PROPOSAL).

4. EVALUATION CRITERIA

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

1. Ability to provide a proposal that fulfils IBF’s project objectives and scope of services (10%);
2. System and data security, access controls, risk management and scalability plans (5%);
3. Vendor’s experience and track record (5%);
4. Quality of support and maintenance services (10%);
5. Price competitiveness (70%).

4.2 IBF may evaluate based on the proposals submitted by Vendors and also 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 and proposals to IBF management.

# 5. SUBMISSION DETAILS

5.1 The submitted proposal shall comprise:

1. **An executive summary of the company’s understanding of IBF’s project objectives and scope of services**
2. **Details of proposal** including project planning, execution and reporting
3. **Experience and track record**:
	1. Provide a brief on the qualifications, relevant certifications (e.g. AA certification) 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.
	2. The assigned staff must be able to communicate fluently in English and be physically located in Singapore.
	3. Provide a brief on the company’s demonstrated experience and track record with projects that used AA RPA tool/solution to improve or optimise a client’s business processes.
	4. Provide two client references for feedback on services delivered for past projects that used AA as a RPA tool/solution.
4. **Proposed fees:**
	1. Provide quotations for fees using the **‘Proposal Template’** under [**Annex 1**](#_ANNEX_2:_PROPOSAL).
	2. 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.
5. Signed ‘Non-Disclosure and Security Awareness Undertaking’ under [**Annex 1**](#_ANNEX_2:_PROPOSAL) **Part V** as confidential information may be provided by IBF during the RFP process.

5.2 The submitted proposal shall include the reference **‘RFP.IT.2023.0030’** and must be clearly marked as **‘Provision of Robotic Process Automation Solution (Automation Anywhere) Maintenance and Professional Services’**.

5.3 One (1) soft copy (in PDF format) of the proposal submission shall reach IBF **no later than 27 Sep 2023, 5pm.** Please send the proposal submission to the following email address:

**Attention:** IBF Procurement

**Email:** procurement@ibf.org.sg

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 one (1) day 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. BRIEFING

6.1 Companies that are interested to bid for this project will be invited to attend a briefing session. Please email procurement@ibf.org.sg to indicate interest **no later than 07 Sep 2023, 5pm**. The interested Vendor may submit a list of questions for clarification during the briefing.

6.2 The briefing session will be held on **11 Sep 2023, 3pm** via web conferencing and meeting details will be sent upon receipt of interest.Vendors shall indicate the number of people attending the briefing, their names, designations, and contact details.

6.3 Signed ‘Non-Disclosure and Security Awareness Undertaking’ under [Annex 1 Part V](#_Toc376944064) to be duly completed and submitted via email by **12 Sep 2023, 5pm** to receive list of current IBF eServices inventory.

# 7. RIGHTS TO THE PROJECT DELIVERABLES

7.1 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.

# 8. INTELLECTUAL PROPERTY

8.1 All related codes and logic generated during this project shall remain as the intellectual property of IBF.

# 9. EXPENSES

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

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

# 10. PAYMENT

10.1 IBF shall work out the payment schedule with the appointed Vendor.

# 11. CONFIDENTIALITY

11.1 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**](#_ANNEX_2:_PROPOSAL) **Part V**.

11.2 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.

# 12. SECURITY CLEARANCE

12.1 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.

12.2 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. The Vendor shall ensure that all its personnel and subcontractors are informed that failure to comply with the undertaking would be a criminal offence.

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

# 13. INDEMNITY AGAINST A THIRD PARTY

13.1 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.

# 14. ACCEPTANCE OR NON-ACCEPTANCE OF PROPOSAL

14.1 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.

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

14.3 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.

# 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:

Khoo Chee Huat, Senior Manager, IT

Email: cheehuat@ibf.org.sg

# ANNEX 1: PROPOSAL TEMPLATE



**Project Name:**

Provision of Robotic Process Automation Solution (Automation Anywhere) Maintenance and Professional Services

RFP.IT.2023.0030

**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.

**(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 Security Awareness 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**
	1. Company Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
	2. Mailing Address: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
2. **OWNERSHIP: Information on Paid-Up Share Capital & Shareholders**
3. **CLIENTELE LIST**

 Please provide a list of your company’s key clients.

1. **SIGNIFICANT ACHIEVEMENTS, AWARDS & CERTIFICATIONS** (where applicable)

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

1. **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 – Details of Proposed Project**

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 reasons** |
| --- | --- | --- | --- | --- |
| **1** | **Ability to provide a proposal that fulfils IBF’s project objectives and scope of services** |  |  |  |
| A | Proposal demonstrates understanding of IBF's project objectives and scope of services |  |  |  |
| B | Provision of AA RPA tool/solution on Automation 360 and/or leverage on Generative AI to improve the accuracy of automation processes. |   |  |  |
| C | Professional services for:i. System installation and configuration.ii. While it is mandatory for the Vendor to quote for this additional scope of services, IBF shall have the option to decide whether it will proceed with the additional scope of services and when it will embark on it.  |   |  |  |
| D | Provision of reporting and analytics on the automated processes |   |  |  |
| E | Provision of all documentation and user guides during each project phase:i) All processes and discussions during each project phase are to be documented with the provision of all associated documents (i.e. meeting minutes, user guides, functional specifications, technical documentation etc.). |   |  |  |
| **2** | **System and data security, access controls, risk management and scalability plans** |  |  |  |
| A | Incorporate system and data security, access controls for the AA RPA bot, risk management procedures for all risk scenarios such as a breakdown of the AA RPA bot, and provide plans on how to scale the AA RPA bot across to IBF’s other business processes |  |  |  |
| **3** | **Vendor's experience and track record** |  |  |  |
| A | Credentials of project team members |  |  |  |
| B | Company’s demonstrated experience and track record with projects that used AA RPA tool/solution to improve or optimise a client’s business processes |  |  |  |
| C | Feedback provided by references on services delivered for past projects that used AA RPA tool/solution:i) Please provide two client references with the contact numbers and email addresses of the referees cited |  |  |  |
| **4** | **Quality of support and maintenance services** |  |  |  |
| A | Vendor shall propose a Service Level Agreement (“SLA”) for the provision of support and maintenance services. This shall include but is not limited to contingency plans which cover downtime so that the AA RPA tool can continue to function without disruptions to IBF’s business operations, until the issue is completely resolved. |  |  |  |

**Part III – Project Costs & Fees**

It is mandatory to quote for all items stated below. Vendors shall complete the table below.

|  |  |  |
| --- | --- | --- |
| **S/No** | **Item Description** | **Pricing (to quote in Singapore Dollars only and exclude GST)** |
| **1** | **Licence and Maintenance** | **Year 1** | **Year 2** | **Year 3 (Optional for IBF to purchase)** |
| A | Provision of AA RPA tool/solution on Automation 360 platform, with minimum version 29:i. 1 Control Roomii. 3 Bot Creatorsiii. 1 Unattended Bot Runneriv. 1 Attended Bot Runnerv. 10 Analytical Usersvi. 1 Bot Insight Platform*Current Automation 360 licence is expired in Dec 2023* |   |   |   |
| B | Provision of IQ Bot: Up to 25,000 pages |   |   |   |
| C | Provision of support/maintenance services:Vendor shall propose a Service Level Agreement (“SLA”) for the provision of support and maintenance services. This shall include but is not limited to contingency plans which cover downtime so that the AA RPA tool can continue to function without disruptions to IBF’s business operations, until the issue is completely resolved. |   |   |   |

|  |  |  |
| --- | --- | --- |
| **2** | **Other Professional Services (Mandatory to quote, optional for IBF to purchase)** | **Pricing (to quote in Singapore Dollars only and exclude GST)** |
|  |  | **Year 1** | **Year 2** | **Year 3** |
| A | Man-day rate for professional services **(mandatory to quote, optional for IBF to purchase)** |  |  |   |

|  |  |  |
| --- | --- | --- |
| **3** | **Other Optional Item(s)** | **Pricing (to quote in Singapore Dollars only and exclude GST)** |
|  |  | **Year 1** | **Year 2** | **Year 3** |
| A | Generative AI for AA RPA |  |  |   |

**Part IV – REFERENCES / OTHER CONSIDERATIONS**

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

**Part V – 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. CONTRACTOR / SERVICE PROVIDER’S DETAILS**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |  |  |
| --- | --- | --- |
|  | **Name of Contractor / Service Provider’s Company (“Service Provider”):** |  |
|  | **Company UEN No:** |  |
|  | **Contact Number:** |  |
|  | **Address:** |  |
|  | **Email Address:** |  |
|  | **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 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 system and Incident management plan to be attached together with this submission.

5. System and Organization Controls Report (preferably SOC 2) 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 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) |  |  |  |  |  |
| 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. |  |  |  |  |  |
| 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) |  |  |  |  |  |
| 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. |  |  |  |  |  |