PUBLIC DOCUMENT

INVITATION TO QUOTE

Project Name:
IBF EMAIL MARKETING PLATFORM

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

CONTENTS

1. INTRODUCTION

1.1 The Institute of Banking and Finance ("IBF") is issuing this Invitation to Quote ("ITQ") to identify suitable entity(ies) (hereinafter referred to as the "Vendor") to submit proposals for the provision of IBF Email Marketing Platform.

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 over 250-member 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 Skills Framework for Financial Services, which were developed in partnership with the industry. Individuals who complete the IBF-accredited skills training programmes and meet the relevant criteria may apply for IBF Certification.

2.3 Since 2018, IBF is the appointed programme manager for the administration of career conversion programmes for the financial industry supported by Workforce Singapore. 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 to Singapore Citizens and Singapore Permanent Residents exploring a new role in, or career switch into the financial industry, under IBF Careers Connect. Since mid-October 2020, IBF has been appointed by the National Jobs Council as the Jobs Development Partner for the financial industry.

3. OBJECTIVE

3.1 The organisation intends to replace its existing Email Marketing Platform as part of efforts to enhance the effectiveness, scalability, and integration of its digital communication initiatives. The new platform is expected to better support the organisation's objectives in customer engagement, lead generation, and brand building.

3.2 The replacement platform should offer improved functionality in campaign management, automation, audience segmentation landing page, and performance analytics. It will also enable seamless integration with existing websites and ensure compliance with prevailing data protection regulations. Ultimately, the platform should facilitate more targeted, timely, and impactful communication with both prospective and existing stakeholders.

4. PROJECT SPECIFICATIONS AND REQUIREMENTS

4.1 The Service Provider is to provide the Email Marketing Platform according to the requirements below.

Project Item	Requirement
Compliance with Functional Requirements	The Service Provider should be able to support IBF's core email marketing requirements, including contact segmentation, automation, email templates, lead generation, landing pages, analytics, data migration, and compliance with data protection regulations.
User Experience and Interface	The platform should be user-friendly for both technical and non-technical users, offering an intuitive dashboard, drag-and-drop tools, and easy setup for campaigns and landing pages.
Integration and Compatibility	The platform should also be able to integrate with IBF's existing website forms to facilitate lead generation for the mailing list.
Value-Added Feature/Innovation	The platform should offer unique innovations or features. This may include AI-driven capabilities, smart automation tools, A/B testing, or additional integrations that enhance lead generation and campaign performance.
Data Security and Compliance	The service provider must submit the latest Vulnerability Assessment and Penetration Testing (VAPT) report with satisfactory results. The platform must be compliant with relevant regulations and standards, including PDPA/ GDPR and SOC 2.
Service Provider Support	The service provider should provide responsive local support (initial response between 1-4 hours), a dedicated account manager, and regular relevant training for users.
Track Record	The vendor's experience working with similar organisations will also be favorably considered.

4.2 IBF requires the vendor to provide the service for a duration of two years. The vendor is to provide a breakdown of the costing in Annex B.

5. PROJECT DELIVERABLES & SCHEDULE

5.1 The Service Provider shall deliver the following based on the timelines below unless otherwise instructed by IBF.

Date	Item
Mid Aug 2025	a) Data migration – Transferring data from the current Email Marketing Platform to the new platform.
3rd week of August 2025	a) Rolling out the new Email Marketing Platform for initial use and configuration. b) Final UAT for the new platform before using the new Email

	Marketing Platform.
End Aug 2025	a) Service Provider to provide comprehensive training to 9 IBF users on the new Email Marketing Platform b) Preparation of a step-by-step user guide for the new Email Marketing Platform.

6. EVALUATION CRITERIA

6.1 The following are the criteria used for the evaluation of all proposals received by IBF for this ITQ and its weightage (%):

S/N	Evaluation Criteria	Weightage
1	Compliance with Functional Requirement	10%
2	User Experience and Interface	10%
3	Integration and Compatibility	10%
4	Value-Added Feature/Innovation	10%
5	Data Security and Compliance	20%
6	Service Provider Support	5%
7	Track record	5%
Q-score		**70%**
8	Price Competitiveness	30%

6.2 In the event that IBF seeks clarification upon any aspect of the proposal, the Service Provider shall provide full and comprehensive responses within three (3) working days of notification.

7. SUBMISSION DETAILS

7.1 The submitted proposal shall comprise:

a) An executive summary of vendor's understanding of IBF's project objectives and scope of work and how vendor's proposal will address IBF's requirements.

b) All vendors are required to complete the attached "Proposal Template" in Annex A.

c) Proposed fees:
   i. Provide quotations for fees using the "Fee Schedule" in Annex B
   ii. Fees quoted shall be in Singapore Dollars only and exclude GST. All fees quoted shall be final and remain the same through the contract period.

7.2 All Vendors are required to provide one (1) soft copy (PDF format) of the proposal to IBF **before 5pm, on 4 Augst 2025**. All proposals must be clearly marked as **"**IBF Email Marketing Platform" and addressed to:

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

7.3 The IBF reserves the right not to accept late submissions. The IBF also reserves the right to cancel, or modify in any form, this Request for Proposal for any reason, without any liability to IBF. All proposals submitted will remain confidential.

8. CONFIDENTIALITY

8.1 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.

8.2 The Vendor shall submit, together with their proposals, an undertaking to safeguard the confidentially of all information revealed to them.

9. Data Governance

9.1 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.

9.2 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.

9.3 The Vendor shall comply with all its obligations under the GDPR/PDPA at its own cost.

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

9.5 strictly for the purposes of fulfilling its obligations and providing the services required under this Agreement;

9.6 with IBF's prior written consent; or

9.7 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.

9.8 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 GDPR/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.

9.9 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:

a) unauthorised or accidental access, collection, use, disclosure, copying, modification, disposal or destruction of IBF's Personal Data, or other similar risks; and

b) the loss of any storage medium or device on which personal data is stored.

9.10 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.

9.11 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.

9.12 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.

9.13 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.

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

9.15 The Vendor shall, upon the request of IBF:

a) return to IBF, all of IBF's Customer Personal Data; or

b) 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.

9.16 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.

9.17 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.

10. INDEMNITY AGAINST A THIRD PARTY

10.1 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 and will reimburse IBF for all costs and expenses (including legal fees) reasonably incurred by IBF in connection with any such action or claim.

11. NOTIFICATION OF UNSUCCESSFUL BID

11.1 Notification will not be sent to unsuccessful Vendors by IBF.

12. ENQUIRIES

12.1 All enquiries pertaining to this Request for Proposal may be directed to tiffany@ibf.org.sg and cc events@ibf.org.sg

Annex A – Proposal Template

All vendors must complete table below and indicate if they are able to fulfill these requirements. Supplementary information on how vendor can meet these requirements can be provided in a separate detailed proposal.

Project Item	**Submission**	**Vendor Response** (Full Compliance – Provide details, or indicate reference in detailed proposal)	**Vendor Response** (Non-Compliance – Provide reasons)
Compliance with Function Requirements	*Please describe how your platform meets the following core email marketing functions:* • *Contact segmentation* • *Marketing automation* • *Customisable email templates* • *Lead generation tools and form* • *Landing page creation* • *Campaign analytics and reporting*		
User Experience and Interface	*Please provide a description of the user interface. Demonstrate how the platform is intuitive for both technical and non-technical users. Include screenshots or demo access if available. Key features to highlight include:* • *Dashboard usability* • *Drag-and-drop design tools* • *Campaign and landing page setup*		
Integration and Compatibility	*Please confirm and detail how your platform integrates with external website forms, especially for mailing list lead generation. Include supported platforms and CMS (e.g., WordPress, custom-built sites).*		
Value-Added Feature / Innovation	*Please outline any unique features or innovations your platform offers. This may include AI-driven capabilities, smart automation tools, A/B testing, or additional integrations that enhance lead generation and campaign performance.*		
Data Security and Compliance	*Please submit the most recent Vulnerability Assessment and Penetration Testing (VAPT) report by a CREST certified vendor showing*		

	satisfactory results. Additionally, confirm compliance with relevant data protection and security standards, such as: • *PDPA / GDPR* • *SOC 2 Type 2*		
Service Provider Support	*Please provide details on the level of support that will be provided, including:* • *Number of hours of **local support** available per week (including business hours and after-hours support, if any)* • *Response time for support requests (e.g., critical issues, general inquiries)* • *Availability of an **assigned account manager** as a dedicated point of contact* • *Scope and frequency of **training sessions** provided for 4 IBF staff (e.g., onboarding, advanced features, refresher training)*		
Track Record	*Please share your experience working with organisations of similar scale and nature, particularly in the financial sector, government, or regulatory bodies. For at least **three past or current clients**, provide the following:* • *Name of organisation* • *Nature of services provided* • *Duration of engagement* • *Contact person (optional) or reference availability* • *Any relevant outcomes, case studies, or performance indicators demonstrating platform effectiveness*		

Annex B – Price Schedule

S/No	Item	Description	Pricing in SGD (exclude SG)	
			Year 1	Year 2
1	Base Database Pricing	*Cost for supporting up to 120,000 contacts*	<Provide both monthly and annual options if available>	<Provide both monthly and annual options if available>
2	Incremental Database Pricing *(IBF current database is at 120,000. Provide Quotation based on this)*	*Pricing for each additional 20,000 contacts beyond the initial tier (or based on pricing structure of vendor)*	<Provide both monthly and annual options if available>	<Provide both monthly and annual options if available>
3	Additional Database Pricing	*Indicate if there are any limits or additional cost for sending volume tied to database size*		
4	Service Support	*Indicate no. of manhours provided. Provide total cost and breakdown for per manhour cost.*		
5	Implentation Cost	*This should be a one-time cost.*		-
6	Other Costs	*Indicate there are any other costs beyond what is listed above*		
		Total Costing		

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)- include as Appendix I
Part VI – IBF IT Service Provider Checklist – include as Appendix II

Appendix I: – 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

1.	**Name of Contractor / 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: _____

Annex II – IBF IT Service Provider Checklist (SPC)

Name of Service Provider	
Date Completed	
Name of Respondent	
Designation / Title	
Contact Number	
Email Address	
Signature	
Company Stamp	

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

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

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

Instructions

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

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

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

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

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

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

S/N	Risk Category	Full Compliance	Partial Compliance	Non-Compliance	N.A.	Comments
	G. MTCS SS584 H. Outsourced Service Provider Audit Report (OSPAR)					
2.5	Service Provider to support and assist in audit activity by providing necessary documents/reports stated in 2.4 upon request.					
2.6	In the event of negative comments or potential auditor concerns in the reports (e.g. incomplete controls), the Service Provider shall make the necessary corrective follow-up actions to address the concern.					
2.7	Service Provider has an incident management process and will notify customer promptly for major incident or when there is a cybersecurity data breach in the service.					
2.8	Service Provider has not suffered any significant breaches in the last 5 years.					
3	**Data Security**					
3.1	As part of the service engagement, no personally identifiable information ('PII') or other personal data should be stored in the vendor's endpoint devices e.g. laptop and mobile					
3.2	Service provider undertakes to protect the confidentiality and security of IBF's sensitive or confidential information and will comply with applicable data protection laws and regulations e.g. PDPA, GDPR?					
3.3	Does the Service provider implement backup of critical information on a regular basis and periodically validate the recovery process?					
3.4	Is data segregated between customers (if hosted) and controls put in place to protect customer data from unauthorised access, modification or leakage?					
3.5	Are data at rest and in transit encrypted using strong encryption algorithm?					

S/N	Risk Category	Full Compliance	Partial Compliance	Non-Compliance	N.A.	Comments
3.6	Are customers' data securely erased from the systems and environment (including backup media) after the termination of the contract?					
4	**General Security Controls**					
4.1	Does the service provider follow secure software development lifecycle practices?					
4.2	Does the service provider enforce change management procedures to ensure changes does not affect services?					
4.3	Does the service provider regularly patch and review the system configurations met its security hardening baselines?					
4.4	Is the service validated regularly for potential security vulnerabilities and findings tracked till closure? If yes, please attach evidence (most recent penetration test reports performed by CREST-accredited penetration tester or equivalent).					
4.5	Is the service resilient to Distributed Denial-of-Service (DDoS) attacks and common application attacks?					
4.6	Are network security controls (e.g. firewall restriction) implemented to protect and detect network resources from unauthorized access?					
4.7	Does the service provide strong authentication controls (e.g. MFA) before service can be accessed?					
4.8	If password is used as the primary means of authentication, is the service able to enforce password complexity requirements, password expiration and account lockout policies					
4.9	Does the application support role-based access control (RBAC) to segregate distinct functions and roles such as for end-users and administrators?					
4.10	Does the service support ease of review or automated handling of inactive/dormant accounts?					

S/N	Risk Category	Full Compliance	Partial Compliance	Non-Compliance	N.A.	Comments
4.11	Is audit logging or reports turn on (e.g. timestamp, login, logout, user actions performed) and the audit logs or reports accessible/retrievable?					
4.12	Is the privilege access management controls enforced in the service provider operations i.e. privileged activities are controlled, monitored and independently reviewed?					
4.13	Segregation of duties should be enforced to prevent any single individual for making critical changes to the system or data without oversight.					
4.14	Does the service provider monitor the security of the system on a 24x7x365 basis?					
5	**Peripheral Supporting Services (If applicable)**					
5.1	If there are peripheral services (e.g. ticketing system) associated with this engagement that keep personal or confidential data from IBF or IBF customers, are the same security controls are in place as above? If not, state what controls are missing and any mitigation measures (e.g. system is not internet facing)					