PUBLIC DOCUMENT

REQUEST FOR PROPOSAL

Project Name:

Provision of Security Information Event Management with Managed Security Services

RFP.IT.2020.0014

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 entities (hereinafter referred to as the “Vendor”) to submit quotations for the provision of a security information event management (“SIEM”) with Managed Security Services (“MSS”).

1.2 The initial contract period is twenty-four (24) calendar months.

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 twenty-four (24) 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.

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 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 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.

2.4 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. OBJECTIVE

3.1 To implement SIEM with MSS for both IBF office and web portal. Service shall include analysing of log and event data in real time to provide threat monitoring, correlation with other sources of information to allow pre-emptive actions to defend against or nullify potential threats. The SIEM will also support and coordinate incident response.

Vendor shall also implement a centralised log depository of various logs files from servers, endpoints and networking devices for each of the above two sites.

3.2 To provide IBF with timely and relevant intelligence on cyber threats.

3.3 The appointed Vendor is expected to ensure all works and tests conform to guidelines and measures issued by the Ministry of Health (MOH), Ministry of Manpower (MOM), Ministry of Trade and Industry (MTI) and other relevant Singapore government agencies for containing the spread of diseases such as COVID-19.

4. SCOPE OF SERVICES

4.1 Vendors are invited to quote for the implementation of centralised log depository to be hosted in IBF office integrating with SIEM with MSS and related services to meet IBF needs.

4.2 Vendors are to take note that the scope shall cover both IBF office (located in IBF registered office address) and IBF portal (located in IBF data center).

4.3 The Vendor is required to submit a proposal with reference to 'Submission Details' under Paragraph 5 Project Deliverables & Schedule and using the template under Annex A: Proposal Template.

IBF will provide a **detail list of servers and devices** to be covered under this project. Vendors will first need to **complete the "Non-disclosure and Security Awareness Undertaking"** attached in **Annex C** and email to the person-in-charged stated in paragraph 16 Enquiries. Once verified, we will provide you with the list shortly.

Do send in the completed form early for you to prepare the proposal.

5. PROJECT DELIVERABLES & SCHEDULE

5.1 The Vendor shall complete the project deliverables based on the stipulated timeline:

Phase	Description	Timeline
1	1. Review the organisational security posture and identify critical devices/applications/servers to be monitored. 2. Propose processes on alerting, escalation and incident handling. 3. Propose project plan.	2 weeks
2	1. Perform baselining on the logs analysed and work with IBF to determine on setting the respective processes and security policies. 2. Implement and trial on various processes defined in Phase 1.	1-2 months
3	1. Continuous fine-tuning security policies and processes to handle new threats. 2. Provide 24x7x365 monitoring, detecting and alerting of security incidents. 3. Support the incident response process which include analysis, containment, eradication, recovery of systems and producing investigation reports. 4. Provide IBF with up-to-date threat intel on the cyber security landscape.	On-going

6. EVALUATION CRITERIA

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

(a) Ability to provide a solution that achieves IBF's project objectives and scope of services (50%);

(b) Vendor's experience and track record (10%)

(c) Ability to meet project timeline (10%); and

(d) Price Competitiveness (30%).

6.2 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.

6.3 As part of the evaluation process, shortlisted Vendors may be required to present their credentials and proposals to IBF management.

7. SUBMISSION DETAILS

7.1 The submitted proposal shall comprise:

a) An executive summary of the company's understanding of IBF's project objectives and scope of services

b) Details of proposal including project planning, execution and reporting

c) Experience and track record:

   i. Provide a brief on the qualifications, relevant certifications (e.g. incident response management 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.

   ii. The assigned staff must be able to communicate fluently in English and be physically located in Singapore.

   iii. Provide a brief on the company's demonstrated experience and track record with projects similar to IBF's scope.

   iv. Provide two client references for feedback on services delivered for past projects implementing on SIEM with MSS.

d) Proposed fees:

   i. Provide quotations for fees using the 'Proposal Template' under Annex A.

   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.

e) Signed 'Non-Disclosure and Security Awareness Undertaking' under Annex A Part V as confidential information may be provided by IBF during the RFP process.

7.2 The submitted proposal shall include the reference 'RFP.IT.2020.0014' and must be clearly marked as 'Provision of Security Information Event Management with Managed Security Services'.

7.3 One (1) soft copy (in PDF format) of the proposal submission shall reach IBF no later than 9 Dec 2020, 5pm. Please send the proposal submission to the following email address:

Attention: IBF Governance
Email: procurement@ibf.org.sg

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

7.5 In the event that IBF seeks clarifications on the proposal, the Vendor shall provide full and comprehensive responses within one (1) day of notification.

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

8. RIGHTS TO THE PROJECT DELIVERABLES

8.1 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 Vendor, in any context is strictly prohibited and liable to legal action by 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. SECURITY CLEARANCE

11.1 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.

11.2 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.

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

12. CONFIDENTIALITY

12.1 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.

12.2 IBF may require an unsuccessful Vendor to return all materials that IBF provided during the period between the issuance of the RFP and the acceptance of the successful quotation.

12.3 All Vendors shall submit, together with their quotations, an undertaking to safeguard the confidentiality of all information revealed to them.

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 QUOTATION

14.1 IBF shall be under no obligation to accept the lowest or any quotation received. It does not normally enter into correspondence with any Vendor regarding the reasons for non-acceptance of a quotation.

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

14.3 IBF reserves the right, unless the Vendor expressly stipulates to the contrary in its proposal, to accept such portion of each contract as IBF may decide.

14.4 The issue by IBF of a Letter of Acceptance 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 to the IBF the specified deliverables in the proposal.

15. NOTIFICATION OF UNSUCCESSFUL BID

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

16. ENQUIRIES

16.1 All enquiries pertaining to this RFP may be directed to:

Mr Tris Tan
Manager, IT
Email: tris@ibf.org.sg

The Institute of Banking & Finance Singapore

ANNEX A: PROPOSAL

Project Name:

Provision of Security Information Event Management with Managed Security Services

RFP.IT.2020.0014

Name of Corporate Entity / Individual:

____

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

Date Received:

Officer-in-charge:

USEFUL NOTES

(A) Submission of Quotation

To assist us in reviewing your quotation in the shortest time possible, please provide the requested information completely and accurately. If the space provided is insufficient, a separate sheet may be used. Where information is not yet available or not applicable, please indicate accordingly.

You are advised to contact us should you have any difficulties in completing the form or if you need any further information.

A soft copy (PDF format) of the proposal shall reach IBF **no later than 9 Dec 2020, 5PM**. All proposals must be clearly marked as "Provision of Security Information Event Management with Managed Security Services (RFP.IT.2020.0014)", and sent via email to:

procurement@ibf.org.sg

(B) Structure of the Quotation

The complete proposal consists of 6 parts:

Part I – Company / Individual Data

Part II – Details of Proposed Project

Part III – Project Costs & Fees

Part IV – References / Other Considerations

Part V – Declaration

Part VI – Annex B: 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 or individual 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 / INDIVIDUAL DATA

1. GENERAL

(a) Company / Individual 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. SIGNICANT 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 business registration document
- Full set of the latest audited financial / management report for the last 3 years.
- Any other relevant reports or information available

PART II – DETAILS OF PROPOSED PROJECT

1 Project Methodology & Approach

[Describe your overall approach to the following task areas. Your response to this form should not exceed three pages.]

- How would you go about gathering requirement?
- How would you go about gathering information from us?
- How would you approach this project?
- What would be the major things you would do in this project?

2 Project Schedule and Workplan

Provide a detailed project implementation plan that includes:

- A Gantt chart showing beginning and end dates of all tasks (the actual project start date will be determined during contract negotiations)
- A table listing vendor staff assignments and proposed labour hours for all tasks

- A brief description of each task and its work products
- A description of each proposed deliverable

3. Key Project Staff Members

[Complete the following table for each of the key project staff members. Use your word processor's copy and paste commands to create additional copies of this table as necessary. Please allow one page for each table.

At a minimum, key staff must include your proposed project manager and key contributors to this project.

Staff member name	
Position in the company	
Length of time in position	
Education	
Previous work experience	
Technical skills and qualifications for the project position	

5. Vendor's experience and track record

Summarise your firm's qualifications and how your firm is uniquely qualified to undertake this project.

Your proposal summary is not to exceed two pages. You are also allowed to provide one work sample showing substantially similar work to demonstrate your credentials for this work.

6. Client Reference

Please list 2 contactable clients for whom you have provided services relevant to this RFP.

Client name	
Company name	
Project reference/title	
Phone number	
Email addresses	

7. Scope of Services

No.	Requirement	Compliance (Y/N)	Remarks if no
Logging & Monitoring			
1	The vendor’s service must provide a solution that will automatically accept events and start to monitor devices without any administrator intervention.		
2	The vendor’s service must provide the ability to analysing and correlating activity with minimum configuration setting. The service must assist security analysts by reducing false positives automatically without requiring significant configuring of rules or filters to do so.		
3	The vendor’s service must provide the ability to reduce compliance auditing efforts by monitoring and alerting on compliance failures in real-time and provide the necessary reports and dashboards to assist auditors in gathering the necessary data, alleviating staff from being taken off their regular tasks during an audit.		
4	The vendor’s service must normalise all collected event data into a consistent format suggested by NIST 800-92. This prepares the data in advance to real-time correlation or ad hoc reporting and allows the data from heterogeneous event sources to be viewed in one consistent manner.		
5	Any failures of the event collection infrastructure must be detected immediately and operations personnel must be notified. Health monitoring must include the ability to validate that original event sources are still sending events.		
6	The vendor’s service must be capable of correcting event time for systems with incorrect timestamps. This allows integrity for forensic analysis to determine the original time on the event source and what the system time was for each vendor component processing the event.		
7	Vendor may offer cloud-based log storage with online or near-online log retention.		
8	The vendor’s log management system search performance must be capable of searching through millions of structured (indexed) and unstructured log messages in an acceptable amount of time.		
9	Log retention hosted at vendor’s premise must not be more than 3 months.		
Detection, Forensic and Investigation			
10	The vendor’s correlation engine must provide many correlation rules to automate the incident detection and workflow process.		

11	The vendor’s service must be capable of correlating activity across multiple devices to detect authentication failures, perimeter security, worm outbreaks and operational events in real-time without the need to specify particular device types.		
12	The vendor’s service must be capable of monitoring attack history against critical asset or by particular users (internal or external).		
13	The vendor’s solution must provide the ability to correlate DHCP, VPN and Active Directory events to provide session tracking for every user in the network.		
14	The vendor’s service must be able to correlate event data against static lists of items that IBF either allows or doesn’t allow on the network (i.e. list of insecure protocols). Additionally, lists should be automatically populated by the system for tracking things such as attacks, user sessions and other policy violations.		
15	The vendor’s solution must provide the ability to model incoming event data into logical groups such as domains, networks, applications, criticality of target devices, etc. This data modelling should then be available to assist in filtering and logically segregating data from view.		
16	The vendor’s solution must be capable of leveraging information pertaining to a targeted device and alter the criticality of the event based on the target’s susceptibility to an attack.		
17	The system must be capable of detecting patterns of activity that would otherwise go unnoticed by real-time correlation.		
18	The vendor’s service must be capable of efficiently presenting categorised data to the correlation engine to allow real-time detection and response.		
19	The vendor service must provide the ability to allow rules to be triggered in a series, matching various correlation activity before an alert is generated.		
20	The vendor’s solution must provide an integrated case management system which allows investigators to collaborate on incidents without ticketing system administrators viewing case information. This feature supports the separation of duties that the security or forensic teams must have to conceal internal investigations.		
21	The vendor’s solution must provide a complete audit trail and accountability during the incident handling or forensic investigation process.		
22	The vendor’s solution must provide the ability to synchronise with authentication directories to collect information regarding user roles and responsibilities and correlate this data with all user activity.		

23	The vendor’s solution must be able to track user activity and ultimately bind an individual to an action.		
24	The vendor’s solution must be able to detect suspicious activity, such as printing or copying large numbers of files outside of business hours, emailing large attachments to personal email accounts or the clearing of system audit logs to cover up malicious activity.		
25	The vendor’s service must be capable of allowing investigators to restore a year’s worth of historical log files to a single appliance (extracting from IBF on-premise log depository) and then perform complex pattern searches and reporting against terabytes of data in a short period of time.		
26	The vendor’s service must capture IP addresses from suspected bad actors including known abusive attackers, malware propagators, spammers, and command and control sites.		
27	The vendor’s service must correlate data about the source and destination of external IP addresses to provide higher resolution on the risk of certain security events. This should be applied to inbound attacks and outbound traffic that could represent a calling home or data exfiltration behaviour.		
28	The vendor’s service must collect intelligence data from reliable sources and update their database frequently.		
29	The vendor’s service must monitor the security events on a 24x7x365 day basis and investigate, prioritise, and alert as necessary.		
30	Critical security events require rapid response and the vendor's service must provide analysis of such events within 30 minutes.		
31	Security Alerts and SOC Analyst communications should be in the context of actionable data enabling the customer to understand what is happening, why it is important and how best to respond.		
32	Alerts and Escalations must be customised to ensure they reach the right person using a preferred channel.		
33	Event data and follow up must be captured and retained in a case management system.		
34	Vendor should prioritise, categorise, and apply rules to assets and users to enable customised business context modelling.		
35	Please provide an overview of your customer notification and escalation process. Include details on how often a customer is notified of a security event, and the methods of notification.		
36	Vendor may offer features like User Event Behavioural Analysis (UEBA) and Security Orchestration and Automation (SOAR)		

PART III – PROJECT FEES

1. Please provide information on fees in Singapore dollars (SGD) as per the following table taking reference from paragraph 5 Project Deliverables & Schedule (Phase 1 to 3).

Professional Services		Pricing (exclude GST)			
		Year 1	Year 2	(Mandatory to quote, optional for IBF to purchase)	
[redacted]				Year 3	Year 4
A	One-time charges (e.g. Professional services required during setup and implementation)				
B	Monthly/Yearly recurring cost (e.g. licenses)				

Ad-hoc Services (Mandatory to quote, optional for IBF to purchase)		Pricing (exclude GST)			
		Year 1	Year 2	Year 3	Year 4
A	Man day/hour rate for consultation services required beyond the project scope				

PART IV – REFERENCES / OTHER CONSIDERATIONS

1. Please indicate reference or highlight any other useful factors (if any) you would like us to consider in reviewing your proposal.

PART V – DECLARATIONS

1. I declare that the information provided by me in this proposal and the accompanying documents are true and accurate to the best of my knowledge, and that the company is free from any litigation pertaining to the project in Singapore or overseas.

2. I agree that IBF shall have the absolute discretion to accept or reject the proposal made without being liable to give any reason thereof.

3. I agree to 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 submission of this proposal.

4. I undertake to safeguard the confidentiality of all information provided or revealed to me by IBF in relation to this RFP or project.

____

Signature (CEO / MD or equivalent for corporate Entity) #

____

Name (IN BLOCK LETTERS)

_________________________________ ____________________

Company Stamp Date

<u>CONTACT PERSON</u>

Name: ________________________________Designation: ___________________________

Telephone No.: _________________________

Email: __________________________________

# Please delete / indicate accordingly

ANNEX B: IBF IT SERVICE PROVIDER CHECKLIST

Name of Service Provider ______________________________

Date Completed ______________________________

Name of Respondent ______________________________

Designation / Title ______________________________

Contact Number ______________________________

Email Address ______________________________

Signature ______________________________

Company Stamp ______________________________

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

Name of Reviewer ______________________________

Designation / Title ______________________________

Contact Number ______________________________

Email Address ______________________________

Instructions

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

2. For each guideline description, place an “X” in the appropriate column to indicate whether the

financial institution is fully compliant, partially compliant, or not compliant. Otherwise, place an “X” in the NA column.

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

4. Evidence of Vulnerability Assessment and Penetration Testing, Configuration Assessment for Cloud systems, and Incident Management Plan to be attached together with this submission.

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

S/N	Risk Category	Full Compliance	Partial Compliance	Non-compliance	N.A.	Comments
1	**Usage Risk**					
1.1	Recent released version of Transport Layer Security (minimally TLS version 1.2 or later) is implemented to provide communication security. (Adopted from MAS TRM E.2.5)					
1.2	Application and database are physically hosted in Singapore.					
1.3	The service provider has established a disaster recovery contingency framework which defines its roles and responsibilities for documenting, maintaining and testing its contingency plans and recovery procedures. (Adopted from MAS TRM 5.1.7)					
1.4	A data backup strategy is developed for the storage of critical information on a regular basis. (Adopted from MAS TRM 8.4.1)					
1.5	Periodic testing and validation of the recovery capability of backup media is carried out.					

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

S/N	Risk Category	Full Compliance	Partial Compliance	Non-compliance	N.A.	Comments
1.11	Service Provider has not suffered any significant breaches in the last 5 years.					
1.12	All components of the disaster recovery plan are reviewed at least annually and updated as needed.					
1.13	Service Provider has a formal incident response plan.					
2	**Application Risk**					
2.1	Mobile and Desktop application do not store data on devices. (e.g. PII, confidential data)					
2.2	Service Provider complies with GDPR and PDPA.					
2.3	Annual Vulnerability Assessment and Penetration Test (VAPT) is performed.					
2.4	Penetration testing is conducted prior to the commissioning of a new modules/enhancements which offers internet accessibility and open network interfaces. (Adopted from MAS TRM 6.2.4)					

S/N	Risk Category	Full Compliance	Partial Compliance	Non-compliance	N.A.	Comments
2.5	Application supports role-based access control (RBAC) for end-users.					
2.6	Application and infrastructure support role-based access control (RBAC) for system administrators.					
2.7	Application and infrastructure support password/passphrase aging.					
2.8	Audit logs minimally include the following: login, logout, actions performed, and source IP address.					
2.9	Service Provider has existing policies and/or procedures guiding how security risks are mitigated until patches can be applied.					
2.10	Vulnerabilities discovered in the systems or applications are remediated prior to release.					
3	**Data Security Risk**					
3.1	Data resides physically in Singapore.					

S/N	Risk Category	Full Compliance	Partial Compliance	Non-compliance	N.A.	Comments
3.2	Service Provider to promptly remove or destroy data stored at the service provider's systems and backups in the event of contract termination and provide a certification. (Adopted from MAS TRM 5.2.4)					
3.3	The data loss prevention strategy and encryption take into consideration the following: (Adopted from MAS TRM 9.1.2)					
	a) Data at endpoint - Data which resides in notebooks, personal computers, portable storage devices and mobile devices;					
	b. Data in motion - Data that traverses a network or that is transported between sites; and					
	c. Data at rest - Data in computer storage which includes files stored on servers, databases, back-up media and storage platforms.					
3.4	Service Provider does not have access to IBF's data.					
3.5	The Service Provider is able to isolate and clearly identify IBF's data and other information system assets for protection.					

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

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

S/N	Risk Category	Full Compliance	Partial Compliance	Non-compliance	N.A.	Comments
3.17	Employees of Service Provider are not allowed or able to take home any assets in any form (including any hardware, software or data) belonging to IBF.					
4	**IT Service Management**					
4.1	Service Provider provides Service Level Agreement (SLA).					
4.2	Service Provider to support and assist in audit activity by providing necessary documents upon request. (Adopted from MAS TRM 5.1.3)					
4.3	The Service Provider is required to employ a high standard of care and diligence in its security policies, procedures and controls to protect the confidentiality and security of IBF's sensitive or confidential information, such as personal data, computer files, records, object programs and source codes. (adopted from MAS TRM 5.1.4)					
4.4	IBF is kept informed of any major incident. (Adopted from MAS TRM 7.3.9)					

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

S/N	Risk Category	Full Compliance	Partial Compliance	Non-compliance	N.A.	Comments
4.11	Service Provider monitors for intrusions on a 24x7x365 basis.					
4.12	A separate management network is used for the administration of the system or service.					

IBF The Institute of Banking & Finance Singapore

ANNEX C: 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: ______________________________