PUBLIC DOCUMENT

REQUEST FOR PROPOSAL

Project Name:

CyberArk Cloud Subscription with Migration

RFP.IT.2025.004

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

CONTENTS

1. INTRODUCTION

1.1 The Institute of Banking and Finance ("IBF") is issuing this Request for Proposal ("RFP") to identify suitable entity(ies) (hereinafter referred to as the "Vendor") to submit proposals for **CyberArk Cloud Subscription with Migration**.

2. BACKGROUND

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

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

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

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

2.5 The current CyberArk is a self-hosted on-premise version. IBF intends to migrate this service to the cloud (CyberArk Identity Security Privilege Cloud) by 31 December 2025. The current on-premise setup is based on the following:

Current CyberArk:
Current Infrastructure: 1xPSM, 1xPVWA, 1xEPV, 1xDRRep, 2xCPM, 1xDREPV, 1xPTA
Current Users: 35 User Licenses
# of CyberArk Safes: ~ 15 safes
RDS Cal License for 10x Windows Remote Desktop
The current implementation is a small-range implementation of <1000 managed passwords and up to 5 maximum capacity for Privilege Session Manager (PSM).

3. SCOPE OF SERVICES

3.1 Vendors are invited to quote for the **CyberArk Cloud Subscription with Migration** to meet IBF's requirements as stated below.

a. Provide the CyberArk Identity Security Privilege Cloud (SaaS Subscription) for 35 users for a period of 4 years based on firm purchase of 2 years with option to extend another 2 years

b. Provide the Microsoft RDS 2025 CAL Perpetual License for 10 users

c. Provide CyberArk Identity Security Platform capabilities for securing remote IT Admin/Ops access. Includes vault, credential protection, session isolation & monitoring, Secure Browser, MFA, SSO, automation & access to work loads with Zero Standing Privileges. Phase 1 must be completed by 31 Dec 2025 and Phase 2 by 30 April 2026

Project Phase	Description	Target Completion Date
Phase 1 – On-Premise	• Migrate self-hosted CyberArk to the CyberArk Identity Security Privilege Cloud • Setup on-premise connector for existing IT infrastructure • Ensure CyberArk Identity Security Privilege Cloud is fully operational to take over all existing PAM workflows and configurations	By 31 Dec 2025
Phase 2 – AWS	• Setup new connector for AWS cloud workloads • Configure and on-board cloud workloads • Configure any new enhancements supported by CyberArk Identity Security Privilege Cloud	By 30 April 2026

*Details for scope of work will be in Annex 1: Proposal Template.

Deliver professional services (during Office Hours) to implement the CyberArk Privilege Cloud and perform migration of on-premises CyberArk set up to CyberArk Cloud. This will also include any customization services for the CyberArk Privileged Access Manager (CPM) plugin and Privilege Session Manager (PSM) plugin

d. Provide software service maintenance (e.g. technical support for issues with platform or connector, technical guidance etc.) ensuring timely resolution for up to 2 x CyberArk Incidents. The proposal must indicate clearly the committed service levels (e.g. 24x7 unlimited call or email for technical support with 4 hours response onsite/remote). The response should be no more than 4 hours for any critical issues encountered.

e. Provide optional add-on user subscription licenses based on a minimum order quantity of 5 users

f. Provide quotation for optional change requests on the system or platform configurations based on equivalent man-day rates

g. Refer to Annex 1 Part II – Compliance for the detailed project requirements.

3.2 The new CyberArk Identity Security Privilege Cloud subscription shall only commence on the successful cutover to SaaS from on-premise, prior cutover activities should be supported by any implementation or trial license and switch to actual subscription on the cutover date or 5 Jan 2026 whichever comes earlier.

3.3 Phase 1 of the Project must complete cutover before the expiry of the on-premise license by 5 Jan 2026, failing which the vendor must provide bridging license at no additional cost to support our on-premise setup until successful cutover. i.e. No outage due to migration activities overrun.

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

4. EVALUATION CRITERIA

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

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

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

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

5. SUBMISSION DETAILS

5.1 The submitted proposal shall comprise:

a) **An executive summary of the vendor's understanding of IBF's project objectives and scope of services and how the vendor's proposals will address IBF's requirements.**

b) **An illustrated detailed explanation of how the implemented system will fulfil each requirement outlined in** Annex 1 Part II – Compliance.

c) **Details of proposal** including project planning, execution, and reporting.

d) **Experience and track record**:

   i. Provide a brief on the company's demonstrated experience and track record on related projects to improve or optimise a client's enterprise architecture.

   ii. Provide two client references for feedback on services delivered for related past projects.

   iii. Provide a brief on the qualifications, relevant certifications (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.

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

e) **Proposed fees:**

   i. Provide quotations for fees using the **'Proposal Template'** under **Annex 1**.

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

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

g) Fully completed and signed 'IBF IT Service Provider Checklist' under **Annex 1 Part VIII.**

5.2 The submitted proposal shall include the reference **'RFP.IT.2025.004'** and must be clearly marked as **'CyberArk Cloud Subscription with Migration'.**

5.3 Soft copy (in PDF format) of the proposal submission to be duly completed shall reach IBF **no later than 17 Jul 2025, 5pm**. Please send the proposal submission to the following email address:

Attention: IBF Procurement
Email: procurement@ibf.org.sg **(Do not copy any other IBF e-mail addresses)**

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

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

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

6. AUDITS

6.1 The Vendor shall cooperate with and provide all support, information and assistance necessary for the conduct of the audits (e.g. SOC-2 Type 2 report, ISO27001 certification, etc.) at no additional cost to the Customer. The Vendor shall also, at its own cost, answer all queries resulting from the audit or inspection and take measures to rectify all identified shortcomings within such period as may be required by the IBF. IBF shall have the right to conduct spot checks or walkthroughs on the Vendor to verify that all identified shortcomings are indeed rectified.

7 COORDINATION WITH OTHER VENDORS

7.1 IBF may engage other vendors to undertake work, supply software, hardware or services related to the Systems. The Vendor shall work closely with IBF-appointed vendors to ensure proper integration and interoperability of the Systems with the work, supply software, hardware, or services provided. The Vendor shall also keep the IBF informed of all relevant actions and interactions with other vendors and seek approval from IBF before implementing system changes or new integrations.

7.2 The Vendor, together with the IBF and IBF-appointed vendors, shall meet as often as required to discuss operational issues and other problems that may be encountered during the Contract Period. All meeting outcomes and decisions requiring changes to the system or new implementations shall be documented and approved by IBF before execution.

7.3 For any required changes to the existing system(s) because of the implementation of the new Systems, the Vendor shall be the single point of contact for the IBF and shall be responsible for working with the vendor(s) managing the existing systems and providing status updates to the IBF. The Vendor shall obtain approval from IBF for any changes or updates before implementation.

7.4 The Vendor shall take full ownership of all problems related to the Systems, regardless of whether the cause is related to software, hardware, application, or data. For problems that require investigations and rectifications from other third-party vendors (such as software vendors, service providers, and IBF's Facility Management (FM) provider), the Vendor shall act as a single point of contact and follow through with the third-party vendors to identify the root cause of the problem and ensure that the problem is resolved within the stipulated turnaround time. All actions taken shall be reported to the IBF and approved by IBF if they involve system changes or new implementations. Such support from the Vendor shall be part of the base maintenance services for the Systems and hence carried out at no additional cost 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 bid, 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 The appointed Vendor shall comply with the following payment schedule outlined by IBF:

a) Upon successful cutover from on-premise to CyberArk Identity Security Privilege Cloud SaaS	100% for Year 1's CyberArk Identity Security Privilege Cloud License, Microsoft RDS 2025 CAL License and Cyberark Software Service Maintenance
b) Upon successful delivery of Phase 1 (On-Premise) CyberArk Professional Services with successful cutover to SaaS	50% for Professional Services and Year 1's CyberArk Professional Services
c) Upon successful delivery of Phase 2 (AWS) CyberArk Professional Services with signed off acceptance by IBF	50% for Professional Services and Year 1's CyberArk Professional Services
d) Subsequent years	100% annual up-front payment at the start of each subscription year i.e. based on annual billing scheme for the CyberArk Identity Security Privilege Cloud SaaS Subscription and Software Service Maintenance

The payment schedule for optional items will be subject to an agreement between the Vendor and IBF.

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 Part VII.**

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 DATA GOVERNANCE

12.1 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.

12.2 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.

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

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

- strictly for the purposes of fulfilling its obligations and providing the services required under this Agreement;
- with IBF's prior written consent; or
- when required by law or an order of court but shall notify IBF as soon as practicable before complying with such law or order of court at its own costs.

12.5 The Vendor shall not transfer IBF's Customer Personal Data to a place outside Singapore without IBF's prior written consent. If IBF provides consent, the Vendor shall provide a written undertaking to IBF that IBF's Customer Personal Data transferred outside Singapore will be protected at a standard that is comparable to that under the PDPA. If the Vendor transfers IBF's Customer Personal Data to any third party overseas, the Vendor shall procure the same written undertaking from such third party.

12.6 The Vendor shall protect IBF's Customer Personal Data in the Vendor's control or possession by making reasonable security arrangements (including, where appropriate, physical, administrative, procedural and information & communications technology measures) to prevent:

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

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

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

12.9 Where IBF provides its Customer Personal Data to the Vendor, IBF shall make reasonable effort to ensure that the Customer Personal Data is accurate and complete before providing the same to the Vendor. The Vendor shall put in place adequate measures to ensure that the Customer Personal Data in its possession or control remain or is otherwise accurate and complete. In any case, the Vendor shall take steps to correct any errors in the Customer Personal Data, as soon as practicable upon IBF's written request.

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

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

12.12 The Vendor shall, upon the request of IBF:

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

12.13 The Vendor shall immediately notify IBF with established communication channels e.g. email, phone calls, messaging apps without undue delay when the Vendor becomes aware of a breach of any of its obligations or believe that a data breach has occurred in relation to personal data that the Vendor is processing on behalf of and for the purposes of another organisation.

12.14 Vendor shall sign the Non-Disclosure and Undertaking Agreement (NDA) not to access, use, share, divulge or retain data unless this is required by the Vendor's staff in discharging their duties during their employment. The NDA is binding even if the staff has resigned or is transferred to another project team or after the termination or expiry of the Contract. Non-compliance could result in legal action being taken against the Vendor by IBF and/or referred to relevant authorities.

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 TERMINATION

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

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

16 NOTIFICATION OF UNSUCCESSFUL BID

16.1 Notification will not be sent to unsuccessful Vendors.

17 ENQUIRIES

17.1 All enquiries about this RFP may be addressed to the following:

To: Tech (IBF)

Email: tech@ibf.org.sg

CC:

IBF Procurement

Email: procurement@ibf.org.sg

ANNEX 1: PROPOSAL TEMPLATE

Project Name:

CyberArk Cloud Subscription with Migration

RFP.IT.2025.004

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 8 parts:

Part I – Company Data

Part II – Compliance

Part III – System Implementation Details

Part IV – Project Costs & Fees

Part V – Summary Price Schedule (Mandatory to quote)

Part VI – References / Other Considerations

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

Annex 2 – IBF IT Service Provider Checklist

(C) IBF reserves the right to conduct interviews and on-site visits during the review of the proposal.

(D) The Company in submitting this proposal undertakes not to divulge or communicate to any person or party any confidential information, including but not limited to any documents that may be forwarded from IBF to you subsequently, without having first obtained the written consent of IBF.

PART I – COMPANY DATA

1. GENERAL

(a) Company Name: _____

(b) Mailing Address: _____

2. OWNERSHIP: Information on Paid-Up Share Capital & Shareholders

3. CLIENTELE LIST

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

4. SIGNIFICANT ACHIEVEMENTS, AWARDS & CERTIFICATIONS (where applicable)

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

5. SUPPORTING DOCUMENTS REQUIRED

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

PART II – COMPLIANCE

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

S/No	Proposal Details	Vendor Response (FC – Full Compliance / NC – Non-Compliance)	If NC, please provide the reasons
1	**Information Gathering and Design**		
1.1	The vendor shall provide kick off meeting to discuss pre-requisites and action plan for migration from on-premise CyberArk to CyberArk Privilege Cloud.		
1.2	The vendor shall provide pre-requisite information and firewall rules (a) Phase 1 - VM connector (x1) to service on-premise IBF Office and IBF Portal server targets (b) Phase 2- AWS Cloud connector (x2) to service IBF AWS Cloud workload and application targets		
1.3	The vendor shall provide consultation on project requirements and RBAC design		
1.4	The vendor shall review the environment and migration data		
1.5	The vendor shall ensure design covers backup vault data and component files. Data from existing on-premise CyberArk can be recovered when required.		
1.6	The vendor shall ensure that the new design should be no worst off in terms of service coverage compared to existing on-premise CyberArk (e.g. PTA will be replaced with AI powered identity security intelligence (ISI) or equivalent)		
2	**Desired Outcomes**		
2.1	The design shall be endorsed by CyberArk with their best practice and recommendations. The design must be secure and resilient to cyber intrusions.		
2.2	The CyberArk Cloud platform must be set to Singapore region (ap-southeast-1)		
2.3	The user login to the platform must be secured by MFA (e.g. Microsoft Entra ID with MS Authenticator, CyberArk Identity etc.)		
2.4	The login to the platform must be restricted to only specific authorized IP ranges or locations. This is to prevent an intruder login from unknown location from overseas.		
2.5	The proposal shall demonstrate clearly how review of privilege activities can be performed easily (e.g. via AI)		
2.6	The CyberArk Cloud connectors must be set to be automatically patched, updated and fully managed to ensure security vulnerabilities are addressed in a timely manner		
2.7	The completed installation shall demonstrate the full capability of the platform and include sample implementation and guide on performing AI powered identity security intelligence, Just In Time Access, passwordless authentication and how-tos for the various identities supported by the platform		
2.8	The solution must be able to prevent password visibility to administrator for out of band use, or to be able to automatically update the credential after approved usage to reduce exposure.		
3	**Installation and Integration**		
3.1	The vendor shall provide and verify relevant prerequisites and firewall ports		
3.2	The vendor shall provide CyberArk recommendations on the installation.		
3.3	The vendor shall provide installation and integration activities over 2 phases: (a) Phase 1 (by end Dec 2025) - to migrate existing on-premise CyberArk to CyberArk Privilege Cloud (b) Phase 2 (by end Apr 2026) - to setup new AWS connector to manage privilege credentials in the AWS Cloud workloads and applications Note: Phase 1 has a deadline to complete migration by 31 December 2025 (prior expiry of the on-premise license on 5 Jan 2026), failing which the vendor must provide bridging license **at no additional cost** to support our on-premise setup until successful cutover. i.e. No outage due to migration activities overrun.		
3.4	New CyberArk Privilege Cloud subscription shall only commence on the successful cutover of Phase 1, prior cutover activities should be supported by any implementation or trial license and switch to actual subscription on the cutover date or 5 Jan 2026 whichever comes earlier.		
3.5	The vendor will need to install and configure 3x Secured tunnels		

S/No	Proposal Details	Vendor Response (FC – Full Compliance / NC – Non-Compliance)	If NC, please provide the reasons
3.6	The vendor will need to install and configure 3x Privilege Cloud connectors (Phase 1: 1x Onprem DC, Phase 2: 2x AWS) to manage secrets in the respective environments.		
3.7	The vendor will need to install and configure 3x Secure Infrastructure Access (SIA) connectors for lightweight secure remote access. The installation shall be on the same machine as the Privilege Cloud Connector to reduce footprint.		
3.8	The vendor will need to install and configure up to 3x Identity Connector for integration with Active Directory/LDAP		
3.9	The vendor will provide integration with external IDP with EntraID		
3.10	The vendor will provide integration with SIEM to send logs to our SIEM service provider		
3.11	The vendor will generate certificate request and installation of SSL cert for CyberArk connectors only (if any). The vendor will upload CA cert to CyberArk backend		
3.12	The vendor will configure HTML5 gateway connection		
3.13	The vendor will configure MFA and password complexity policies		
3.14	The vendor will configure up to 10x ISI rules		
4	**Migration On-Premises to Privilege Cloud**		
4.1	The vendor shall migrate all relevant on-premises data to CyberArk Privilege Cloud		
4.2	The vendor shall re-create local user for safe migration and access matrix		
4.3	The vendor shall disable password rotation and CPM services during the migration transition period		
4.4	The vendor will migrate configurations: (a) Master policy configuration (b) File category migration (c) Local CyberArk vault user migration (d) PSM connection components migration (e) Platform migration (f) Migrate ALL CPM and PSM plugins (g) Migrate existing PTA or related configurations to flag suspicious events		
4.5	The vendor will perform data migration: a) Export Safe data and permissions (b) Import Safe data and permissions (c) Validate data imported in Privilege Cloud (d) Export password objects data (username, address etc) (e) Import password objects data (username, address etc)		
4.6	The vendor will ensure that all existing workflows and features are migrated successfully.		
4.7	The vendor shall provide, install and apply the Microsoft RDS CAL license required by the new setup		
5	**Knowledge Transfer**		
5.1	The vendor shall provide up to 2x knowledge transfer session for administrators and users (a) Phase 1 for on-premise administrators and users (b) Phase 2 for AWS cloud administrators and users		
6	**User Acceptance Testing**		
6.1	The vendor shall perform sampling verification of onboarded account in each platform created. (a) The vendor shall verify the (hashed) passwords stored in vault is correct. (b) the system shall provide the seamless login to the target devices, without the users having sight of their passwords to the devices (c) system shall change the passwords immediately upon the completion of each session and also periodically as configured.		
6.2	The vendor shall perform Password Management and reconciliation for at least 1 onboarded account in each platform (a) The vendor shall verify the password can be reconciled and changed successfully		
6.3	The vendor shall perform verification for target devices connection and session recording functionalities for x1 onboarded account in each platform (a) Connect to target devices and verify the connection established successfully (b) Verify the session recording notification pop out and started		
6.4	The vendor shall perform user verification assessment		

S/No	Proposal Details	Vendor Response (FC – Full Compliance / NC – Non-Compliance)	If NC, please provide the reasons
	(a) Validate that user can login to CyberArk Privilege Cloud web portal with relevant rights and permissions		
6.5	The vendor shall provide search and review capability for session recording: (a) Search session recording based on filters: time, keyword, user, username, hostname/ip etc (b) Verify key event capture in the session recording (c) Verify skip idle function is working (d) Highlight suspicious events (or those flagged by ISI) in filtered query timeframe (e.g. monthly) via dashboard or report for review purposes		
7	**Documentation**		
7.1	The vendor shall provide the operational and UAT documentation		
8	**Project Management**		
8.1	The vendor shall formulate execution plans, draft detailed SOW, implementation timeline		
8.2	The vendor shall review integration risks and impacts based on existing IT infrastructure		
8.3	The vendor shall provide weekly project updates, manage milestone deliverables		
9	**Vendor's experience and track record**		
9.1	The vendor shall provide credentials of project team members		
9.2	The vendor shall provide company's demonstrated experience and track record with projects that has performed the CyberArk Cloud Migration		
9.3	The vendor shall provide feedback by references on services delivered for past projects that used CyberArk Identity Security Privilege Cloud		
9.4	The vendor shall provide two client references with the contact numbers and email addresses of the referees cited		
10	**Software Service Maintenance**		
10.1	The vendor shall provide unlimited direct phone and email assistance by technical support specialists for Software problem resolution, bug reporting, documentation clarification and technical guidance, coverage 24 hours a day, 7 days a week		
10.2	The vendor shall provide no more than 4 hours onsite or remote session response by a Certified Engineer upon receipt of customer's request when critical issues are encountered		

PART III – PROPOSAL DETAILS

Vendors shall furnish relevant details not limited to the Part II Compliance, this may include supporting documents / website references but not limited to:

Solution Details

- Full solution features supported by the Platform
- Proposed High-Level Project Timeline
- Proposed Solution Architecture
- Security Trust Assurance for the Platform e.g. SOC-2 Type 2, ISO27001, FedRamp etc.
- Service SLA for the Platform
- Integration with Other Systems e.g. SIEM, LDAP
- Furnish relevant online guides and “How-To” articles to demonstrate type of identity coverage

Professional Services

- Installation, Configuration, Licensing and updates
- Migration approach
- Customisation Activities

Software Maintenance Services

- Support arrangements, hotline to call etc.
- Proposed Service Level Agreements

PART IV – PROJECT COSTS & FEES

It is mandatory to quote for all items stated below. Vendors shall complete the table below. All costs must be quoted in Singapore Dollars.

1. **CyberArk Identity Security Privilege Cloud (SaaS Subscription for 35 users)**

S/No	Item Description	Qty (a)	Unit Price (b)	Amount (a) x (b) = (c)	Discount (d)	Net Price (c) – (d) = (e)	Any Assumptions/Comments
Year 1							
Year 2							
Year 3 (mandatory to quote, optional for IBF to purchase)							
Year 4 (mandatory to quote, optional for IBF to purchase)							
	Total						

2. **Microsoft RDS 2025 CAL Perpetual License (based on 10 users)**

S/No	Item Description	Qty (a)	Unit Price (b)	Amount (a) x (b) = (c)	Discount (d)	Net Price (c) – (d) = (e)	Any Assumptions/Comments
Year 1							
	Total						

3. **CyberArk Professional Services - Project Implementation (including CPM and PSM plugin customization)**

S/No	Item Description	Qty (a)	Unit Price (b)	Amount (a) x (b) = (c)	Discount	Net Price (c) – (d) = (e)	Any Assumptions/Comments
One-Time Cost							
	Total						

* during Singapore Office Hrs (9 am to 6pm, Monday to Friday)

4. **CyberArk Software Service maintenance, up to 2 incidents, 24x7 support, no more than 4 hours response**

S/No	Item Description	Qty (a)	Unit Price (b)	Amount (a) x (b) = (c)	Discount (d)	Net Price (c) – (d) = (e)	Any Assumptions/Comments
Year 1							
Year 2							
Year 3 (mandatory to quote, optional for IBF to purchase)							
Year 4 (mandatory to quote, optional for IBF to purchase)							
	Total						

5. **Optional: CyberArk Identity Security Privilege Cloud Add-On License (based on MOQ of 5 users)**

S/No	Item Description	Qty (a)	Unit Price (b)	Amount (a) x (b) = (c)	Discount (d)	Net Price (c) – (d) = (e)	Any Assumptions/Comments
Year 1 (mandatory to quote, optional for IBF to purchase)							
Year 2 (mandatory to quote, optional for IBF to purchase)							
Year 3 (mandatory to quote, optional for IBF to purchase)							

Year 4 (mandatory to quote, optional for IBF to purchase)							
	Total						

6. **Optional: Change Request/ Service Request Costing**

S/No	**Item Description**	**Man-Days** (a)	**Per Man-Day Costing** (b)	**Amount** (a) x (b) = (c)	**Discount** (d)	**Net Price** (c) – (d) = (e)	**Any Assumptions/Comments**
	Total						

PART V – SUMMARY PRICE SCHEDULE (MANDATORY TO QUOTE)

Costing to be listed in readable Excel Format

S/No	Item Description	Pricing in SGD (exclude GST)				
		One-Time Cost	Year 1	Year 2	(Mandatory to quote, optional for IBF to purchase) Year 3	Year 4
1	CyberArk Identity Security Privilege Cloud (SaaS Subscripion) for 35 users*	-				
2	Microsoft RDS 2025 CAL License for 10 users	-				
3	CyberArk Professional Services - Project Implementation (including CPM and PSM plugin customization)		-	-	-	-
4	CyberArk Software Service Maintenance (e.g. technical support for issues with platform or connector, technical guidance etc.) , up to 2 incidents, 24x7 direct phone and email assistance, no more than 4 hours response remote session or onsite upon request	-				
5	Optional: CyberArk license add-on, Annual Subscription **(mandatory to quote based on minimum order qty of 5 users, optional for IBF to purchase)**	-				
6	Optional: Change Request/ Service Request Costing (**mandatory to quote, optional for IBF to purchase)**					
	Total Costing					

* New CyberArk Privilege Cloud subscription shall only commence on the successful cutover to SaaS from on-premise, prior cutover activities should be supported by any implementation or trial license and switch to **actual subscription on the cutover date or 5 Jan 2026 whichever comes earlier**. Project is expected to complete cutover before the expiry of the on-premise license by 5 Jan 2026, failing which the vendor must provide bridging license **at no additional cost** to support our on-premise setup until successful cutover. i.e. No outage due to migration activities overrun.

PART VI – REFERENCES / OTHER CONSIDERATIONS

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

PART VII – 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 2 – 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 _____

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.					

S/N	Risk Category	Full Compliance	Partial Compliance	Non-Compliance	N.A.	Comments
	Otherwise, please provide supporting information that the necessary security controls are in place. (e.g. audit opinions). Examples of security-related compliance: A. ISO/IEC (27001 / 27002 / 27017 / 27018) B. SOC (Type 1 / Type 2 / Type 3) C. PCI DSS (Level 1 / 2 / 3 /4) D. CSA Star (Level 1 / 2 / 3) E. NIST (800-53 / 800-144) F. OWASP ASVS (Level 1 / 2 / 3) G. MTCS SS584 H. Outsourced Service Provider Audit Report (OSPAR)					
2.5	Service Provider to support and assist in audit activity by providing necessary documents/reports stated in 2.4 upon request.					

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

S/N	Risk Category	Full Compliance	Partial Compliance	Non-Compliance	N.A.	Comments
3.4	Is data segregated between customers (if hosted) and controls put in place to protect customer data from unauthorised access, modification or leakage?					
3.5	Are data at rest and in transit encrypted using strong encryption algorithm?					
3.6	Are customers' data securely erased from the systems and environment (including backup media) after the termination of the contract?					
4	**General Security Controls**					
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).					

S/N	Risk Category	Full Compliance	Partial Compliance	Non-Compliance	N.A.	Comments
4.5	Is the service resilient to Distributed Denial-of-Service (DDoS) attacks and common application attacks?					
4.6	Are network security controls (e.g. firewall restriction) implemented to protect and detect network resources from 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?					
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?					

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