SINGAPORE CENTRE FOR CHINESE LANGUAGE
565 Balestier Road, #05-05, Singapore 329927
Tel: 64675667

Invitation to Quote

Date of Invitation: 5/11/2026 **ITQ Ref No. ITQ-FY27-08-000022**

To:

Address:

Tel No:

1) Please let us have your quotation (***exclusive of GST***) for the services specified below in your company letterhead and returning it to us by 17:00 (Time) on 18/11/2026 (Closing Date).
2) Where applicable, please attach brochures/catalogue/samples when submitting your quotation.
3) The quotation shall remain valid for 30 days from the closing date as stated above. On expiry of the offer, the vendor shall, if SCCL so requires, extend the validity of offer for a further period of 60 days from the aforesaid date of expiry.
4) SCCL reserves the right not to accept the lowest or any proposal and shall not be bound to assign any reason for the rejection. SCCL also reserves the right to award full quotation or part thereof and shall not be bound to assign any reason for the award.
5) Please note the possible risks of sending your quotation through the fax.

S/N	Description	Unit Price S$	Total Amount S$
1	Pls refer to the "Request for Quotation.pdf" Other requirement: Payment: 30 Days Credit Term upon satisfactory completion of the project and service delivery.		
		Total amount (exclude GST)	

If you have any queries, please email Mr Cillin Tio at it_support@sccl.sg or Mr Tay Yong Xiang at yongxiang.tay@sccl.sg for clarifications. Thank you.

Request for Quotation

The Singapore Centre for Chinese Language ("SCCL") invites you to submit a formal proposal for the provision of Privilege Access Management (PAM) Solution Services (hereinafter referred to as the "Services") for SCCL, as detailed below:

1. Introduction

1.1 This is a Request for Quotation (RFQ) for the design and implementation of PAM cybersecurity solution to control, monitor, and audit the use of privileged (administrator-level) accounts across SCCL IT critical systems, with the objective of reducing misuse, account comprise, and insider threat.

2. Scope of RFQ

2.1 A comprehensive plan which include project management, milestones, schedules, work breakdown structure and testing activities from the point of contract award.

2.2 Plan shall include requirements gathering, design, implementation, fall back plans, mitigation strategies, manpower and any other resources to ensure smooth and effective service delivery.

2.3 Plan shall also include a detailed, industry-standard Service Level Agreement (SLA), specifying key performance indicators (KPIs), response/resolution times, and availability targets to ensure optimal service performance and reliability.

2.4 Privilege Access Management (PAM) Solution Services (3 Years)

2.4.1 The Awarded Supplier shall provide the following requirements:

A) Configuration and Deployment

1. The PAM solution must support deployment as a virtual appliance and/or hardware appliance where required.

2. The PAM solution must provide a fully redundant architecture and capability to operate in High Availability (HA) and Disaster Recovery (DR) failover modes.

3. The PAM solution must expose APIs to support integration with other third-party solutions.

4. The PAM solution must ensure that all communications between PAM components are encrypted.

5. The PAM solution shall support time synchronization to ensure accurate session and audit timestamps.

6. The vendor shall supply, install, configure, test, and commission the PAM solution, including all required licences and software components, for operation in SCCL's environment.

7. The PAM solution must support at least 3 IT administrators.

8. The PAM solution must support at least 6 targets, including 4 Windows Servers and 2 Microsoft SQL Server database.

9. The vendor shall conduct system testing and User Acceptance Testing (UAT) prior to commissioning of the PAM solution.

B) Credential Vaulting and Password Management

1. The PAM solution shall securely store privileged credentials in an encrypted vault, including Windows Server Administrator accounts and Microsoft SQL Server accounts.

2. The PAM solution shall ensure that users do not need to know or view target credentials to launch privileged sessions.

3. The PAM solution must support scheduled automatic password rotation for privileged accounts on target systems.

4. The PAM solution shall enforce configurable password complexity rules that comply with the SCCL Password Construction Standard for passwords it generates and rotates on target systems,

5. The PAM solution shall provide configurable password expiry settings and proactively notify designated responsible users of upcoming password expiration via email and audit logs.

6. The PAM solution shall allow secrets and privileged credentials to be organized into folders with granular access permissions.

7. The PAM solution's vault must support multiple target and credential types.

C) Privileged Access Control

1. The PAM solution must support Role-Based Access Control (RBAC).

2. The PAM solution must support a configurable multi-level approval workflow before privileged access is granted.

3. The PAM solution must support exclusive credential check-in/check-out mechanisms to prevent concurrent use of a privileged credential.

4. The PAM solution must support emergency ("break-glass") privileged access with full auditing and traceability.

5. The PAM solution must support Multi-Factor Authentication (MFA) for privileged access, with support for integration with SCCL's existing Microsoft Active Directory accounts where possible.

6. The PAM solution must support SSH command-level filtering.

7. The PAM solution must support Just-in-Time (JIT) privileged access.

D) Privileged Session Monitoring, Auditing and Compliance

1. The PAM solution shall record full privileged sessions and retain session recordings for audit, review, and export.

2. The PAM solution shall support live monitoring ("over-the-shoulder" monitoring) of active privileged sessions and provide authorised administrators with the ability to terminate active sessions when required.

3. The PAM solution shall provide comprehensive audit logs of all privileged activity and support export/forwarding to external systems.

4. The PAM solution shall capture keystrokes, commands, mouse activities/clicks, and other relevant privileged session activities where supported by the applicable access protocol.

5. The PAM solution shall provide configurable email alerts for security-relevant events, including high-severity alerts and activation of emergency ("break-glass") access.

6. The PAM solution shall provide audit reports suitable for security review and compliance purposes.

E) Access Methods, Protocols and Integration

1. The PAM solution shall support browser-based, agentless privileged access to target systems without requiring client software where applicable.

2. The PAM solution shall support client-based privileged access using supported native and/or third-party client applications.

3. The PAM solution shall integrate with enterprise identity providers for Single Sign-On (SSO) and automated user lifecycle management.

4. The PAM solution shall support integration with SCCL's existing Microsoft Active Directory environment for authentication and privileged access management.

F). Training, Documentation and Knowledge Transfer

1. The vendor shall provide knowledge transfer and administrator training sessions for SCCL administrators and relevant personnel.

2. The vendor shall provide comprehensive system documentation covering, at minimum, solution architecture, system configuration, administration procedures, operational procedures, backup and recovery procedures where applicable, and troubleshooting and maintenance procedures.

3. The vendor shall provide relevant configuration records and operational documentation necessary for SCCL to administer and maintain the PAM solution after implementation.

G) Post-Implementation Support, Maintenance and Warranty

1. The vendor shall provide post-implementation technical support for the proposed PAM solution.

2. The vendor shall provide maintenance and warranty services covering the proposed solution, including the supplied software/hardware, and associated components as applicable.

3. The vendor shall provide support for troubleshooting, defect resolution, configuration issues, and other technical issues relating to the implemented PAM solution during the contracted support and maintenance period.

Scope of work to be completed before **26 February 2026 (Friday)**.

3. Experience of the Supplier

3.1 The Awarded Supplier shall possess the necessary technical expertise in designing and implementing PAM solutions involving but not limited to Microsoft Windows Server and SQL Server (including SQL Server Management Studio (SSMS)). The Supplier shall demonstrate proven methodologies, secure handling frameworks, effective project management tools, a qualified and experienced team, and a verifiable track record in similar projects.

3.2 The Awarded Supplier shall detail in the proposal their approach, methodology, framework, and tools that will be used to execute the Services. This includes risk mitigation strategies and cyber security protocols.

4. Experience of assigned personnel

4.1 The Awarded Supplier shall propose a team of personnel with relevant experience in designing and implementing PAM solution for Microsoft Windows Server and SQL Server (including SQL Server Management Studio (SSMS)), as part of their proposal.

4.2 The same proposed list of assigned personnel shall also perform the Services as required until completion of the required Services. Any change in the assigned personnel during the review period shall be highlighted to SCCL at least ONE week in advance and subject to SCCL's approval.

4.3 SCCL reserves the right to object to any personnel assigned by the Supplier. SCCL reserve the right not to notify the Supplier of the reasons for the objection.

4.4 If the assigned personnel are not performing to the expectation or the contractual clauses, SCCL reserve the right to request a change of personnel without any impact on the schedule and cost.

4.5 The Awarded Supplier shall assign a single point of contact (POC) and the POC shall report to SCCL on the project status.

5. Deliverables

5.1 The Supplier shall provide the following deliverables in soft copy (including editable formats), as part of the Services. This may include, but not limited to, the following:

i. Project plan with key project timelines, approach, methodology and tools involved in the delivery of the service.

6. Evaluation Criteria

6.1 The following are the criteria and assigned weightages:

S/No	Criteria	Weightage
1	Quality • Effectiveness of solution (30%) • Experience & skills of personnel (10%) • Implementation & timeline (10%) • Proven credentials & track records of similar projects (10%)	60%
2	Cost Competitiveness	40%
	Total	100%

7. Document Submissions

7.1 The closing date of submission is **18 Nov 2026 (Thursday), 5pm.**

7.2 Incomplete submission and submission received after the closing date and time may be liable for disqualification.

7.3 A complete Proposal shall include but not limited to:
- Annex A: Form of Declaration and Undertaking to Safeguard Confidential Information
- Annex B: Price Breakdown
- Annex C: Track Records
- Annex D: Technical Data Information

7.4 Failure to submit the above-mentioned documents may disqualify the proposal from further evaluation. Suppliers may submit additional supporting documents that may help SCCL in the evaluation of the quotations.

7.5 SCCL does not bind itself to accept the lowest or any offer. SCCL reserves the right to accept the offer as a whole, in part or not award it at all.

7.6 SCCL shall not be required to enter into any discussions, negotiations or correspondence of whatever nature with any contractor(s) regarding the reasons for non-acceptance of a quotation.

8 OTHER NOTES

8.1 The Awarded Supplier will be required to segregate SCCL's data from other clients.

8.2 The Awarded Supplier shall follow SCCL policies with regard to security incident management and escalation where applicable.

8.3 The Awarded Supplier shall follow the physical and logical access control set by SCCL on on-premises work (if any).

9 LIASION CONTACT

9.1 For all clarifications or enquiries, please email Mr Cillin Tio at it_support@sccl.sg or Mr Tay Yong Xiang at yongxiang.tay@sccl.sg

FORM OF DECLARATION AND UNDERTAKING TO SAFEGUARD CONFIDENTIAL INFORMATION

REFERENCE NO.: ITO-FY27-08-000022

To: Singapore Centre for Chinese Language Limited ("SCCL")

I, _____ HEREBY DECLARE that my attention has been drawn to the confidentiality obligations of _____ _____ [the Contractor's Company Name] under the Invitations to Quotations and Conditions of Contract.

I HEREBY UNDERSTAND that all information as defined in the Quotation is of a strictly confidential nature and in the event of being unsuccessful in the Quotation bid, I shall, upon the request of SCCL, return any specifications, plans, drawings, patterns, samples or instructions issued by SCCL.

In consideration of being provided with any Confidential Information, I HEREBY UNDERTAKE to observe all provisions relating to the Confidential Information in the said Quotation and Contract as though the same had been imposed on me directly and that I will not disclose, communicate or otherwise release to any person such information in any form whatsoever, in accordance with the said Quotation and Contract.

Signature : _____

Name : _____

Designation : _____

Company : _____

Date : _____

* *"Confidential Information" shall mean all information in any form or manner provided by SCCL to the Contractor or otherwise acquired by the Contractor in the course of or pursuant to this Contract relating to the Equipment, Works, the Requirement Specifications, SCCL and/or Affiliates, and/or their business, financial or other affairs.*

ANNEX B

Price Breakdown

S/N	Description of Services	One Time Cost ($)
1	PAM Solution Setup	
	Total Cost:	

S/N	Description of Services	Annual Cost ($)
1	PAM Solution Subscription (Year 1)	
2	PAM Solution Subscription (Year 2)	
3	PAM Solution Subscription (Year 3)	
	Total Cost:	

Note

(i) The unit cost shall be provided in Singapore dollars and exclude GST (Goods and Services Tax)

Annex C

CONTRACTOR'S PARTICULARS AND TRACK RECORDS

1) BizFile from ACRA or equivalent (for companies not registered with ACRA) **dated not more than 3 months from quotation closing date.**

2) Details of completed similar Projects in the past 2 years (since 2024)

S/No	Description of Project	Name of organisation Contact details: 1. Name of contact person 2. Email address (if any) 3. Contact No.	Period		Final Contract Sum (S$)	Any feedback / testimonial
			From	To		

Annex D

Privilege Access Management (PAM) Solution Professional Services Specifications		**Compliance Yes / No**	**Description, Details, Comments, etc.**
A. Configuration and Deployment			
A1.	The PAM solution must support deployment as a virtual appliance and/or hardware appliance where required.		
A2.	The PAM solution must provide a fully redundant architecture and capability to operate in High Availability (HA) and Disaster Recovery (DR) failover modes.		
A3.	The PAM solution must expose APIs to support integration with other third-party solutions.		
A4.	The PAM solution must ensure that all communications between PAM components are encrypted.		
A5.	The PAM solution shall support time synchronisation to ensure accurate session and audit timestamps.		
A6.	The vendor shall supply, install, configure, test, and commission the PAM solution, including all required licenses and software components, for operation in SCCL's environment.		
A7.	The PAM solution must support at least 3 IT administrators.		
A8.	The PAM solution must support at least 6 targets, including 4 Windows Servers and 2 Microsoft SQL Server databases.		
A9.	The vendor shall conduct system testing and User Acceptance Testing (UAT) prior to commissioning of the PAM solution.		

Technical Data Information

Annex D

B. Credential Vaulting and Password Management			
B1.	The PAM solution shall securely store privileged credentials in an encrypted vault, including Windows Server Administrator accounts and Microsoft SQL Server accounts.		
B2.	The PAM solution shall ensure that users do not need to know or view target credentials to launch privileged sessions.		
B3.	The PAM solution must support scheduled automatic password rotation for privileged accounts on target systems.		
B4.	The PAM solution shall enforce configurable password complexity rules that comply with the SCCL Password Construction Standard for passwords it generates and rotates on target systems.		
B5.	The PAM solution shall provide configurable password expiry settings and proactively notify designated responsible users of upcoming password expiration via email and audit logs.		
B6.	The PAM solution shall allow secrets and privileged credentials to be organised into folders with granular access permissions.		
B7.	The PAM solution's vault must support multiple target and credential types.		
C. Privileged Access Control			
C1.	The PAM solution must support Role-Based Access Control (RBAC).		
C2.	The PAM solution must support a configurable, multi-level approval workflow before granting privileged access.		
C3.	The PAM solution must support exclusive credential check-in/check-out mechanisms to prevent concurrent use of a privileged credential.		
C4.	The PAM solution must support emergency ("break-glass") privileged access with full auditing and traceability.		

Technical Data Information

Annex D

C5.	The PAM solution must support Multi-Factor Authentication (MFA) for privileged access, with support for integration with SCCL's existing Microsoft Active Directory accounts where possible.		
C6.	The PAM solution must support SSH command-level filtering.		
C7.	The PAM solution must support Just-in-Time (JIT) privileged access.		
D. Privileged Session Monitoring, Auditing and Compliance			
D1.	The PAM solution shall record full privileged sessions and retain session recordings for audit, review, and export.		
D2.	The PAM solution shall support live monitoring ("over-the-shoulder" monitoring) of active privileged sessions and provide authorised administrators with the ability to terminate active sessions when required.		
D3.	The PAM solution shall provide comprehensive audit logs of all privileged activity and support export/forwarding to external systems.		
D4.	The PAM solution shall capture keystrokes, commands, mouse activities/clicks, and other relevant privileged session activities where supported by the applicable access protocol.		
D5.	The PAM solution shall provide configurable email alerts for security-relevant events, including high-severity alerts and activation of emergency ("break-glass") access.		
D6.	The PAM solution shall provide audit reports suitable for security review and compliance purposes.		
E. Access Methods, Protocols and Integration			
E1.	The PAM solution shall support browser-based, agentless privileged access to target systems without requiring client software where applicable.		
E2.	The PAM solution shall support client-based privileged access using supported native and/or third-party client		

Technical Data Information

Annex D

	applications.		
E3.	The PAM solution shall integrate with enterprise identity providers for Single Sign-On (SSO) and automated user lifecycle management.		
E4.	The PAM solution shall support integration with SCCL's existing Microsoft Active Directory environment for authentication and privileged access management.		
F. Training, Documentation and Knowledge Transfer			
F1.	The vendor shall provide knowledge transfer and administrator training sessions for SCCL administrators and relevant personnel.		
F2.	The vendor shall provide comprehensive system documentation covering, at minimum, solution architecture, system configuration, administration procedures, operational procedures, backup and recovery procedures where applicable, and troubleshooting and maintenance procedures.		
F3.	The vendor shall provide relevant configuration records and operational documentation necessary for SCCL to administer and maintain the PAM solution after implementation.		
G. Post-Implementation Support, Maintenance and Warranty			
G1.	The vendor shall provide post-implementation technical support for the proposed PAM solution.		
G2.	The vendor shall provide maintenance and warranty services covering the proposed solution, including the supplied software/hardware, and associated components as applicable.		
G3.	The vendor shall provide support for troubleshooting, defect resolution, configuration issues, and other technical issues relating to the implemented PAM solution during the contracted support and maintenance period.		

Technical Data Information