AGENSI KAUNSELING DAN PENGURUSAN KREDIT

VULNERABILITY ASSESSMENT AND PENETRATION TESTING

(REF: AKPK/RFQ19/OCT01)

Request for Quotation

[RFQ]

[VENDOR'S NAME HERE]

Issuer

Agensi Kaunseling Dan Pengurusan Kredit (AKPK)
Level 14, TH Perdana Tower
1001 Jalan Sultan Ismail
50250 Kuala Lumpur

ISSUE DATE **: 4 OCTOBER 2019**
CLOSING DATE/TIME **: 16 OCTOBER 2019 / 3:00 PM**

1 INTRODUCTION

The purpose of this Request for Quotation (RFQ) is to seek proposals from qualified technology security consultants to provide Vulnerability Assessment and Penetration Testing Services to assist in strengthening AKPK's system and technology security posture. The services include vulnerability assessment, penetration testing, security review and related information security assessment services. This assessment exercise is expected to be completed within two (2) month from the project kick-off, to be followed by subsequent retests (where applicable) and report finalisation.

2 REQUIREMENTS

The following are the requirements for the Deliverables:

No.	Descriptions	Quantity
1	**Application Penetration Testing Services** The supplier shall provide application testing services for internal and external environment including but not limited to the following: i. Manual probing of application interfaces; ii. Authentication process testing (understanding how the **authentication process** works and using that information to circumvent the **authentication** mechanism); iii. Automated fuzzing (**automated software testing technique** that involves providing invalid, unexpected, or random data as inputs to a computer program. The program is then monitored for exceptions such as crashes, or failing built-in code assertions or for finding potential memory leaks); iv. Encryption usage testing (e.g. applications' use of encryption); v. Forming manual and automatic code review for sensitive information of vulnerabities in the code; vi. Testing of the application functionality including but not limited to: a. Input validation (e.g, bad or over-long characters, URLs); and b. Integration testing; vii. Check and validate applications URL if it contained sensitive data and to see if unauthorized access can be permitted including but not limited to: a. Input validation of login fields; b. URL validation;	Number of core application to be tested: 1. Internal apps: **1** 2. External apps: **6**

No.	Descriptions	Quantity
	c. Secret password saved by programmer/developer in the application; d. Cookie security; e. Lockout testing; f. Log-out security testing; g. Application/Web configuration files; viii. User session integrity testing. ix. To assess the web application and identify vulnerabilities based on latest OWASP Top ten (10) Web Application Vulnerabilities. x. To use the following testing methodologies: a. Black Box and; b. White Box. xi. To conduct a controlled penetration attempts or exploitation of identified vulnerability as discussed and agreed with AKPK's representatives.	
2.	**Host Security Configuration Review** *To perform configuration review of AKPK's operating systems and Internet services including but not limited to the following:* i. To obtain and perform configuration review towards AKPK's operating systems and Internet services using manual or automated tools. ii. To perform gap assessment to the host configurations against best practice benchmarks. iii. Host Security Configuration Review may include, but not limited to the following areas: a. Users and groups; b. File permissions and check for suspicious files; c. Password management settings; d. Start-up files; e. Network configurations and Trust relationships; f. OS and firmware and patch levels; g. Running processes; and h. Folder sharing	No. of hosts: **20**
3.	**Database Security Assessment** *To assess the database security and identify vulnerabilities based on Top 10 Database Threats:* i. Excessive privilege abuse; ii. Legitimate privilege abuse; iii. Privilege elevation;	a) No. of Microsoft SQL Database server: **6** b) No. of MySQL DB server: **2**

No.	Descriptions	Quantity
	iv. Exploitation of vulnerable, misconfigured databases; v. SQL injection; vi. Malware; vii. Denial of service; viii. Database communication protocol vulnerabilities; ix. Unauthorized copies of sensitive data; and x. Backup data exposures	
4.	**Network Devices Security Configuration Review** *To perform configuration review of AKPK's network devices.* i. To identify vulnerabilities and related threats that may arise from misconfiguration of network devices. ii. Network Devices Security Configuration Review may include, but not limited to the following areas: a. Patching / Firmware status; b. Password management. c. Authentication, Authorization and Accounting; d. Access rules, rules and signatures; e. Auditing and Logging;	No. of network devices: **12**
5.	**Network Assessment and Penetration Testing** *The Supplier shall provide network penetration testing Services including but not limited to the following:* i. Provide penetration testing from both internal and external of AKPK network; ii. Identify targets and map attack vectors (i.e., threat modelling); iii. Internet Protocol ("IP") address mapping of network devices; iv. Logical location mapping of network devices; v. Transmission Control Protocol ("TCP") scanning, connect scan, SYN scan, RST scan, User Datagram Protocol ("UDP") scan, Internet Control Message Protocol ("ICMP") scan, File Transfer Protocol ("FTP/sFTP") and Remote Procedure Call ("RPC") port scan; vi. Operating System ("OS") fingerprinting (OS fingerprinting is the combination of passive research and active scanning tools to generate an accurate network map); vii. Banner grabbing*;*	a) No. of external IP address: **10** b) No. of internal IP address: **32**

No.	Descriptions	Quantity
	viii. Brute force attacks; ix. Denial of Service ("DDoS") testing; x. Network sniffing; xi. Spoofing; xii. Trojan attacks; and xiii. War dialling.	
6.	**Wireless Assessment and Penetration Testing** *The Supplier shall provide wireless assessment and penetration testing services including but not limited to the following:* i. Wireless network testing (*is the act of locating and possibly exploiting connections to* **wireless** *local area networks while walking around HQ office or elsewhere via laptop or smartphone*) and; ii. Wireless, wired equivalent Privacy (WEP) / WiFi Protected Access (WPA) cracking.	
7.	**Physical Security Assessment** The supplier shall conduct Physical Security assessment involving interviews with key staff, documentation review, and on-site visit to assess appropriate physical and environmental controls for safeguarding computing resources.	
8.	**Compromise Assessement** *The supplier shall conduct Compromise assessment to identify on-going compromises and uncovers the malicious access and usage of the environment. The scope of investigation must include but not limited to the following:* i. File and Operating System Audit, ii. Network Logs Audit, iii. Host Memory Analysis, iv. Network Logs Audit, v. Host Memory Analysis, vi. Host Disk Forensics and vii. Network Forensics.	
9.	**Social Engineering** *The supplier shall provide human centric social engineering testing Services must include but not limited to the following:* 1. Baiting scenarios; 2. Phishing campaigns (e.g. email, phone); and 3. Physical test (e.g. tailgating, entry into controlled facility areas).	

No.	Descriptions	Quantity
10.	**Server Hardening Baseline Review** *The supplier shall conduct a review on AKPK server hardening baseline that include but not limited to the following:* 1. **Account Policies** (e.g.: Enforced password, max/min password age and length, Account lockout duration, password complexity, and etc); 2. **Audit Policies** (e.g.: Audit Logon Event, Audit Process Tracking, Audit System Event, etc); 3. **Detailed Security Auditing** (e.g.: Logon-Logoff, Privilage Use, System Integrity, etc); 4. **Event Log**; 5. **Windows Firewall**; 6. **Windows Update**; 7. **User Rights** (e.g.: accessibility over the network, Bypass traverse checking, Ability to change the system time, etc); 8. **Security Options** (e.g.: Network security, Network access, Account: Rename admin/guest account, Domain member, etc) 9. **Internet Communications** (e.g.: Downloading driver over HTTP, Printing over HTTP, etc) 10. **Additional Security Settings** (Registry policy processing, Remote assistance, Remote sharing, etc) *The supplier also shall create a checklist on server hardening baseline for AKPK that based on hardening standard.*	
11.	**IT Security Awareness** The vendor is required to conduct an IT Security Awareness talk to all AKPK staff based on Social Engineering conclusion and recommendation.	

3 DELIVERY TIMEFRAME

No.	Description	Expected Timeframe
1	First Assessment Reports	2 months
2	Post Patch Retests	2 times after first assessment report
3	Final Assessment Report	After final post past retests.

4 DELIVERABLES

Interested vendor wishing to participate in this RFQ exercise is required to:-

4.1 Provide the following information/documents as Solution Proposal (**Appendix A)**:-

4.1.1 Project Plan

4.1.2 Project Organization Chart

4.1.3 Project Timelines

4.1.4 Minutes of Meeting

4.1.5 Project Documentation

4.1.6 Project Management

4.1.6.1 A synopsis of the then current status of the project

4.1.6.2 Progress of the overall project

4.1.6.3 Address risks and the associated mitigation plans

4.1.6.4 A summary of key deliverables

4.1.6.5 A preview of the activities for the next period

4.1.6.6 Documented changes to the project plan(s)

4.1.7 System Assessment Study: assessment exercise to be completed within 2 months from project kickoff for this one-time engagement. All work must be done during standard business hours (**Monday – Friday, 8:00 am – 6:00 pm**).

4.1.8 Management Report and Technical Report on the AKPK's Security Posture Assessment and the recommendations

4.1.8.1 Management Summary with overall severity graph

4.1.8.2 Detailed results for vulnerabilities discovered, exploited vulnerabilities and proof of concepts/screenshots

4.1.8.3 Detailed explanations of the implications of findings, business impacts, and risks for each of the identified exposures

4.1.8.4 Vulnerabilities Report would be delivered in a password

Protected Adobe Acrobat (PDF) document format

4.1.9 Advisory for vulnerability remediation and recommendation

4.1.10 Post Patch Retests

4.1.11 Signed off for each deliverables

4.1.12 To fill up the checklist as follows:

i. Delivery timeline

ii. Attach relevant Suruhanjaya Syarikat Malaysia's (SSM) documents as follows:-

<u>For Enterprise Company</u>

- ✓ SSM Company Profile
- ✓ SSM Corporate Information
- ✓ Form D

<u>For Sendirian Berhad & Berhad Company</u>

- ✓ Company Profile
- ✓ Memorandum and Articles of Association
- ✓ SSM Corporate Information
- ✓ Form 49
- ✓ Form 9 (Sendirian Berhad) & Form 8 (Berhad)

iii. Latest Audited Financial Statements

iv. Certification of Penetration Testers

v. Technical Data Sheet for Penetration Tools

vi Declaration of any relationship with AKPK Board members or Staff i.e. parents, spouse, children, siblings (if any)

4.1.13 Fill up the Person In-Charge Form.

4.1.14 Fill up the Company Profile Form.

4.2 Provide the following information/documents as <u>Cost Proposal</u> (**Appendix B)**:-

4.2.1 Provide **Official Company Quotation** for the Deliverables. (Vendor **must** submit this and refer to **items #10 VALIDITY OF THE QUOTATION** for the validity period of the Quotation)

4.2.2 Fill up the Cost Summary.

4.2.3 Provide propose Payment Term.

4.2.4 Provide Bank Info.

5 METHOD OF SUBMISSION

By hand ONLY, proposals to this RFQ must be deposited in a sealed envelope into tender box at:

Level 14, TH Perdana Tower,
1001, Jalan Sultan Ismail,
50250 Kuala Lumpur.

(The remaining page is intentionally left blank)

The proposals to be submitted in a **separate cover**, **sealed envelope** and to be labelled clearly as follows:

i. Solution Proposal (Appendix A)

"NOTE: DO NOT OPEN. SOLUTION PROPOSAL ENCLOSED FOR AKPK VULNERABILITY ASSESSMENT AND PENETRATION TESTING, RFQ# AKPK/RFQ19/OCT01 SUBMITTED BY [VENDOR'S NAME HERE]"

(Note: Should submit 3 sets of copies – 1 original, 2 photocopies in one envelope)

ii. Cost Proposal (Appendix B)

"**NOTE: DO NOT OPEN. COST PROPOSAL ENCLOSED FOR AKPK VULNERABILITY ASSESSMENT AND PENETRATION TESTING, RFQ# AKPK/RFQ19/OCT01 SUBMITTED BY [VENDOR'S NAME HERE]"**

(Note: Should submit 3 sets of copies – 1 original, 2 photocopies in one envelope).

(Note: Any submission of RFQ Proposal to be registered in our "Schedule of Tender RFQ Submission" during submission i.e. Name of Company and Contact Details, Name, Designation, IC Number, H/P Number, Email Signature, etc.

6 DELIVERY LOCATION

The location for the Deliverables to AKPK's office is at:

No	Location	Address
1.	AKPK HQ Attention: IT Department	Level 8, Maju Junction Mall 1001 Jalan Sultan Ismail 50250 Kuala Lumpur

7 AKPK's OFFICER IN-CHARGE

a. AKPK's Procurement officer in-charge is:
Name : Nur Hayati Mat Salleh / Ezreen Ezairy Hussin
Contact No : 03-2610 5678 / 03-2610 5696

b. AKPK's Technical officer in-charge is:
Name : Mohd Azmi Bin Mohd Supian
Contact No. : 03-2616 7768
Email : azmi@akpk.org.my

Name : Tan Sze Chun
Contact No. : 03-2616 7761
Email : chun@akpk.org.my

Name : Halim Saleh
Contact No. : 03-2616 7770
Email : halim.s@akpk.org.my

8 DEADLINE OF SUBMISSION

a. All quotations must reach us by / before **3:00 pm** on **16 October 2019.**

b. Tender received after the deadline and/or not comply with method of submission as above mentioned will be rejected.

c. The vendor's proof of posting and/or submission by other means shall not be accepted as proof of receipt by AKPK.

d. Document that are rejected or disqualified will be disposed-off at our end.

e. Regardless of the method used for delivery, vendors shall be wholly responsible for the timely delivery of submitted proposal.

9 CLARIFICATION

Vendors are required to be present at AKPK office for a clarification session on a date to be confirmed by both parties between **23 to 24 October 2019**.

10 VALIDITY OF THE QUOTATION

a. The validity of the quotation submitted is 180 calendar days;

b. All costs and expenses incurred by vendor in any way associated with the development, preparation, and submission of responses, including but not limited to; the attendance at meetings, discussions, demonstrations, proof of concept, etc. and providing any additional information required by AKPK, will be borne entirely and exclusively by the vendor.

c. All cost are inclusive SST, delivery charges & installation cost and all other taxes incidental to the Deliverables.

11 AWARD OF THE CONTRACT

a. Before the expiry of the period of validity of the proposal, AKPK shall notify the selected vendor in writing by registered letter or by email that its Proposal has been accepted by AKPK and any intention to award a Contract.

b. The selected vendor will be issued with an official Letter of Award (LOA) or Purchase Order (PO).

c. Prior to such an issuance, price negotiation may be carried out with the selected vendor.

d. The parties to the contract shall have it signed within **ten (10) days** from the date of LOA issuance unless there is an administrative review request.

e. The selected vendor shall prepare the Project Agreement or Maintenance Agreement **within two (2) weeks** upon acceptance of the Letter of Award from AKPK.

f. Stamp duty to be borned by the selected vendor.

g. The project shall commence once the Project Agreement or Maintenance Agreement is signed by both parties AKPK and the selected vendor.

12 ANTI-BRIBERY AND ANTI-CORRUPTION

a. AKPK is committed to conducting business in an ethical and honest manner and has zero-tolerance for bribery and corrupt activities.

b. We are committed in all business dealings and relationships and will constantly uphold all laws relating anti-bribery and anti-corruption in Malaysia in particular the Malaysia Anti-Corruption Commission Act 2009.

13 WHISTLE BLOWING

Report on whistleblowing matters are as follows:

a. The Supplier is encouraged to report any concern by completing the Whistleblowing Incident Report Form (WIRF) as attached in **Appendix C.**

b. The Supplier shall as soon as possible, in writing or orally, inform the CEO of AKPK, upon having knowledge of any director, officer or employee of AKPK, directly or indirectly, asking for or receiving, any gratification whether for his own personal benefit or advantage or for the benefit or advantage of any other person, in relation to this Agreement, whether before, during or after the term of this Agreement at ceo@akpk.org.my

c. If the concern involves the CEO of AKPK, the whistleblower could address his concern either by post or email to the Chairman of AKPK's Audit Committee at acchairman@akpk.org.my

d. If the concern involves a director of the Board, you should share your concern either by post or email with the Chairman of the Board at chairman@akpk.org.my

'Gratification' includes corruption or bribery, any gift, money, property or thing of value, or any service, favour or other intangible benefit or consideration of any kind, or any other similar advantage.

(The remaining page is intentionally left blank)

APPENDIX A

A. SOLUTION PROPOSAL

1. CHECKLIST (TO HAVE THE FOLLOWING DOCUMENTS)

No	Description	Tick (✓)	Envelope
i	Company Profile form		
	Business Registration Certificate		
	Memorandum and Articles of Association		
	SSM Corporate Information		
ii	Form D (Enterprise), Form 9 (Sendirian Berhad) & Form 8 (Berhad)		
	Form 49 (Sendirian Berhad & Berhad)		
	Latest Audited Financial Statements		
iii	Certification of Penetration Testers		
iv	Technical Data Sheet for Penetration Tools		
v	Proposal		
vi	Declaration of any relationship with AKPK Board members or Staff i.e. parents, spouse, children, siblings (if any)		

2. PERSON IN-CHARGE

Name	
Designation	
Contact Number (Off) **Mobile Number (HP)**	
Email	
Signature	
Date	
Company Stamp	

3. DELIVERY TIMELINE

No	Description	Delivery Timeline
1	Application Penetration Testing Services	
2	Host Security Configuration Review	
3	Database Security Assessment	
4	Network Devices Security Configuration Review	
5	Network Assessment and Penetration Testing	
6	Wireless Assessment and Penetration Testing	
7	Physical Security Assessment	
8	Compromise Assessment	
9	Social Engineering	
10	Server Hardening Baseline Review	
11	IT Security Awareness	

(The remaining page is intentionally left blank)

COMPANY PROFILE FORM

This section covers generic company information that will provide a quick overview of the vendor/solution provider organization. Please fill in as much information as possible, and feel free to add additional information in the form of attachment.

i. Particulars of Company

No	Items	Explanation
1.	Company Name	
2.	Company Registration No. (for company registered in Malaysia)	
3.	Business Address	
4.	Correspondence Address (if different from the above business address)	
5.	Telephone No.	
6.	Fax No.	
7.	Contact Person(s)	
8.	Number of years in business operation	
9.	Latest Audited Financial Statements	
10.	SSM Certification (e.g. Form 49. Form 9, etc.)	

ii. Company's Directors (Please add more where required)

No.	Name of Directors	Position in Company	Period
1.			
2.			
3.			

iii. Company's Current and Past Work Experience (latest 3 projects)

Please attach the list of similar contracts/projects performed by your company. **The list should be confined only to similar or related supply/services/works described in this RFQ document** and presented in the format specified below (please add more rows if not sufficient).

No.	Client Name	Project Description	Completion Date
1.			
2.			
3.			

DECLARATION

We declare that all information on the company is true and correct; and there has been no deliberate suppression of facts, which are required in this form.

Signature _____

Name _____

Designation _____

Date _____

APPENDIX B

B. COST PROPOSAL

1. CHECKLIST

No	Description	Tick (✓)	Envelope
1.	i. Official Quotation (must submit this)		**Cost Proposal**
	ii. Cost Summary (as per item 2 below)		
2.	i. Propose Payment Term		
	ii. Bank Info		

2. COST SUMMARY

No	Description	QTY	Cost per unit (RM)	Total Cost (RM)
1	Application Penetration Testing Services	7		
2	Host Security Configuration Review	20		
3	Database Security Assessment	8		
4	Network Devices Security Configuration Review	12		
5	Network Assessment and Penetration Testing	42		
6	Wireless Assessment and Penetration Testing	1 lot		
7	Physical Security Assessment	1 lot		
8	Compromise Assessment	1 lot		
9	Social Engineering	1 lot		
10	Server Hardening Baseline Review	1 lot		
11	IT Security Awareness	1 lot		
			GRAND TOTAL	

PROPOSE PAYMENT TERM

No	Description
1.	Preferred Payment Term (min. 5% for each milestone) i. Upon Acceptance of LOA/PO : 10% ii. Upon Delivery of Initial Test Reports : 40% iii. Upon Delivery of Post Remediation Test Reports : 40% iv. Upon Final Check on the Remediation & Project Closure : 10% (Please state if the payment term is not as per the above preferred term)
2.	Manner of Payment i. Name of Bank : ii. Address of Bank : iii. Account number : iv. Account type : Current / Saving v. Account scheme : Conventional / Islamic

(The remaining page is intentionally left blank)

APPENDIX C

Whistleblower Incident Report Form (WIRF)

Instruction: All reports should be made using the WIRF

Reporting Misconduct

You should share your concerns of misconduct to the Chief Executive Officer (CEO) of AKPK. If it is inappropriate to make the report to the CEO, you can report your concerns to the Chairman of the Board of Directors or Chairman of the Board Audit Committee. Alternatively, you may mail the completed WIRF to the Chairman of the Board of Directors or to the Chairman of the Board Audit Committee.

Date of Report: _____

Person reporting the actual or suspected misconduct.

(Do not complete this section if you wish this to be an anonymous report)

Name : _____
Email address : _____
Telephone number : _____

Person against whom the report of actual or suspected misconduct is being made:

Name : _____
Email address : _____
Telephone number : _____

Use the back of this form or additional sheets of paper to describe the alleged misconduct. Include specific facts and documentation, if any, as well as the names of any individual at AKPK with whom you have discussed your concerns.

(The remaining page is intentionally left blank)

[END OF THE RFP]