# AGENSI KAUNSELING DAN PENGURUSAN KREDIT

# SUPPLY, DELIVERY AND COMMISSIONING OF NEXT-GENERATION SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) SOLUTION

## (REF: AKPK/RFP19/OCT01)

# Request for Proposal

# [RFP]

**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** **: 17 October 2019 / 03:00PM**

## 1 INTRODUCTION

The purpose of this Request for Proposal (RFP) is to solicit proposals from suppliers for the SUPPLY, DELIVERY AND COMMISSIONING OF NEXT GENERATION SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) SOLUTION for Agensi Kaunseling Dan Pengurusan Kredit (AKPK). Please note that this proposal should not include managed services and/or hosted solution

This RFP document describes the SIEM project with a detailed scope outlined in Section 2 and mandatory requirements in Appendix A item 3. All Vendors must respond to the mandatory and rated requirements as outlined in this RFP for their proposals to be deemed compliant. However, vendors are encouraged to provide alternative solution that meet would meet the project requirements where better value or increased operational effectiveness can be realized.

The NEXT GENERATION SIEM solution is to improve information security operations in AKPK where It shall help protect AKPK's business operations and intellectual properties, comply to regulations and enable better detection leading to faster response to security incidents.

## 2 DELIVERABLES

The SIEM Project should include all the equipment and implementation services necessary to provide a total SIEM Solution ( to connect to the various network elements and meet the capacity, functionality and feature requirements outlined in this RFP). The Deliverables of this RFP includes the following:-

| No | Descriptions | Quantity | Requirements |
|---|---|---|---|
| 1 | **The Solution at Datacenter (DC) (KL)**<br>To supply, deliver and commission the SIEM Solution at Data Center.<br>1) Identification and recommendation of an appropriate SIEM solution, which fits with AKPK's requirements and allows for future growth. | 1 Lot | Refer to Apendix A item 3 (Specifications and features) |

| | | | |
|---|---|---|---|
| | 2) Supply, configuration, installation and testing of the proposed solution, including any required interfaces and data conversions.<br>3) On-site hardware installation and setup, software configuration and user settings. | | |
| 2 | **Backup at Disaster Recovery Center (DRC) (Cyberjaya)**<br>To supply, deliver and commission the SIEM Solution at DRC as a cold backup. | 1 Lot | Refer to Apendix A item 3 (Specifications and features) |
| 3 | **Training**<br>1) Training to be conducted before the go live date - administrator with hands on (operational) training materials.<br><br>2) Training to be conducted after project go-live - a formal classroom training. | 4 Paxs | Refer to Apendix A item 3 (Specifications and features) |
| 3 | **Support & Maintenance**<br>The hardware, software and maintenance services is for **3 years:-**<br>1) Hardware/software warranty & Support.<br>2) 24 x 7 support, phone & online supports<br>3) Onsite Response – Next business day<br>4) Provide monthly report and facilitate continuous improvement.<br>5) Provide preventive maintenance twice a year. | 3 years | Refer to Apendix A item 3 (Specifications and features) |
| 4 | **Implementation services**<br>To provide professional services for the above implementations via<br>i. Project management approach. | 1 Lot | Refer to Apendix A item 3 (Specifications and features) |

| | | | |
|---|---|---|---|
| | ii. On-site hardware installation and setup, software configuration and user settings for DC and DRC.<br>iii. Implementation services to assist AKPK in setting up back-ups; using existing AKPK data backup solution.<br>iv. Provision of documentation in printed and electronic format, including administrative and end user manuals, troubleshooting guides and/or Q&A. | | |

## 3. IMPLEMENTATION REQUIREMENTS

The solution should be designed to accommodate current and future growth of AKPK infrastructure. Tenderes are advised to propose the right solution sizing based on the current AKPK IT environment as explained below, strictly follow the solution requirements as per appendix A item 3 . Vendors are also expected to work closely with AKPK IT department and its current vendors for the implementation.

**Current AKPK IT Environment**

It is very important for vendors to understand the AKPK infrastructure and configuration to come up with a comprehensive write up in proposing the **solution**.

All AKPK applications are located and managed centrally from AKPK DC and backup at AKPK DRC serving all AKPK branches nationwide (10 branches) and HQ through TM IPVPN line. All branches' internet connection requests are channelled through DC internet link and filtered by AKPK security devices such as Firewall and Internet Access Manager (IAM). The bandwidth access is as follows:-

a. HQ Office : 10 Mbps (120 clients).
b. Branches: 1 Mbps each ( 8 clients per branch).
c. DC : 20 Mbps IPVPN & 20 Mbps Internet line.
d. DRC : 10 Mbps IPVPN & 10 Mbps internet line.

All AKPK client desktops and laptops are running on Windows 7 (to be upgraded to windows 10 by end 2019) and Windows 10 respectively. All internal users authenticate to the network through Microsoft Active Directory (AD). All AKPK PCs/Laptops are using Bitdefender as anti-virus solution.

The server infrastructure consists of mostly Microsoft Windows Server 2012 R2 (Estimated 50 servers) and Linux Centos 6 & 7 (4 servers), virtualised at about 90% with VMware 6.7. AKPK has a disaster recovery site that host a subset of the DC environment (Estimated 20 servers) in case of a disaster. In addition to the servers, AKPK infrastructure consists of :-

**a. Web Services/Applications**: Web services, IIS, .Net Framework, PHP

**b. Security devices ( Firewall,WAF, IAM, IPS)**: ~ 6 devices

**c. Network Switches**:

a. Core switch: 2 at HQ, 2 at DC and 1 at DRC

b. L2 switch : 20 units located at HQ and branches.

**d. Routers**: ~ 15 units

**e. Anti-virus** : 300 clients of Bitdefender (Gravityzone Business Security)

**f. Databases**: MS SQLServer & MySQL Server

**g. Other components**: 25 units of Ruckus WiFi AP & 1 Console, 2 units of SAN storage.

## 4 DELIVERY TIMEFRAME

The project is expected to complete as per timeframe below:

| No | Description | Expected Timeframe |
|---|---|---|
| 1 | Delivery of the Deliverables | 20 weeks |

(The remaining page is intentionally left blank)

# 5 RFP SUBMISSION

## 5.1 Solution Proposal

The vendor's proposal MUST be organized using the content numbering scheme described below.

**Required Structure of Proposals and Content Numbering**

Solution Proposal

1.0 Project Management and Implementation
- 1.1 Project Orgasisation
- 1.2 Project Timeline
- 1.3 Implementation plan & strategy

2.0 Description of Product Being Proposed
- 2.1 Product Architecture
- 2.2 Product Features
- 2.3 Product Operations

3.0 Training

4.0 Post Implementation Support and Maintenance

5.0 Corporate information

6.0 Response to Requirements (Appendix A item 3)

7.0 References

Appendices

A Certifications

B Sample License and Maintenance/Support Agreements

C Product Information (Brochure)

D Attachment ( As per item 5.1.1)

In addition to the above , interested vendors are required to include the following as attachment:

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

For Enterprise Company; or

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

For Sendirian Berhad & Berhad Company

- ✓ Company Profile
- ✓ Memorandum and Articles of Association
- ✓ SSM Corporate Information
- ✓ Form 49
- ✓ Form 9 (Sendirian Berhad) & Form 8 (Berhad)
- ✓ Latest Audited Financial Statements 2017 and 2018
- ✓ Product Brochures
- ✓ Letters of Authorization from Principals and Distributors

5.1.2 Fill up the Person In-Charge Form.

5.1.3 Fill up the Company Profile Form.

5.2 Provide the following information/documents as Cost Proposal (**Appendix B)**:-

5.2.1 Provide **Official Company Quotation** for the Deliverables. (Vendor **must** submit this and refer to **items #9 VALIDITY OF THE QUOTATION** for the validity period of the Quotation)

5.2.2 Fill up the Cost Summary.

5.2.3 Provide propose Payment Term.

5.2.4 Provide Bank Info

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

## 6 METHOD OF SUBMISSION

**By Hand ONLY**, proposals to this **RFP** must be deposited in a sealed envelope into tender box located at:

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

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 SUPPLY, DELIVERY AND COMMISSIONING NEXT-GENERATION SIEM SOLUTION, RFP# AKPK/RFP19/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 SUPPLY, DELIVERY AND COMMISSIONING COMMISSIONING NEXT-GENERATION SIEM SOLUTION, RFP# AKPK/RFP19/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.

## 7 DELIVERY LOCATION

The locations for the **Deliverables** to AKPK's office will be at:

| No | Location | Address |
|---|---|---|
| **1.** | AIMS Data center<br>Attention: AKPK IT Department | 1st Floor, Menara AIMS,<br>Changkat Raja Chulan,<br>50200 Kuala Lumpur. |
| **2.** | Disaster Recovery Center,<br>Attention: AKPK IT Department | CJ1 Center, Jalan Cyberjaya<br>Point 4, Cyberjaya 8,<br>63000 Cyberjaya, Selangor |

(The remaining page is intentionally left blank)

## 8 AKPK's OFFICER IN-CHARGE

**a. AKPK's Procurement officer in-charge is**:

Name : Ezreen Ezairy Hussin / Nur Hayati Mat Salleh

Contact No : 03-2610 5696 / 5678

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

Name :Raja Mohd Hisham Bin Raja Muzaffar
Contact No. : 03-2616 7766 (ext 684)
Email : Hisham@akpk.org.my

(The remaining page is intentionally left blank)

## 9 DEADLINE OF SUBMISSION

a. All quotations/RFP must reach us by / before **03:00 pm** on **17 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. Documents 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.

## 10 PROOF OF CONCEPT (POC)

a. Shortlisted vendors will be notified via email and required to perform Proof Of Concept on a date to be confirmed by both parties between **22 October to 25 October 2019** where failing to perform the POC will disqualify the vendor from the further process of evaluation.

b. The following are the scope of the POC (but not limited to) :-

1. **Log source configurations** : To demonstrate the process of adding and configuring various log data source system.
2. **Event correlation, alerting, log analysis, and incident management:** To demonstrate the solution capabilities for event correlation, alerting, associated log data analysis, and event/incident workflow management.
3. **Reporting features: :** To demonstrate the solution capabilities for report creation and report review tracking.
4. **Dashboard and access control features**: **:** To demonstrate Solution capabilities for customized access and display.

## 11 VALIDITY OF THE QUOTATION

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

b. To provide additional service with the same specification and price within twelve (12) months (if require) after first purchase done; and

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

## 12 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).

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 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 borne 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.

## 13. 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

## 14. 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, favor 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. | Solution Proposal write up (item no 5.1) | | Solution Proposal |
| II. | Product Brochures (if applicable) | | |
| III. | Letters of Authorization from Principals and Distributors, if any | | |
| IV. | Company Profile form | | |
| | Business Registration Certificate | | |
| | Memorandum and Articles of Association | | |
| | SSM Corporate Information | | |
| V. | Form D (Enterprise), Form 9 (Sendirian Berhad) & Form 8 (Berhad) | | |
| | Form 49 ( Sendirian Berhad & Berhad) | | |
| | Latest Audited Financial Statements 2017 & 2018 | | |
| VI. | Certification of Project Manager and System Engineer | | |
| VII. | 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** | |



[**VENDOR'S COMPANY STAMP HERE**]

## 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.<br>(for company registered in Malaysia) | |
| 3. | Business Address | |
| 4. | Correspondence Address<br>(if different from the above business address) | |
| 5. | Telephone No. | |
| 6. | Fax No. | |
| 7. | Operation hours and support contact numbers<br>( Helpdesk) | |
| | 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.) | |
| 11. | Company Nature of Business | |
| 12. | Company Paid up Capital | |
| 13. | Company Share Holder Fund | |
| 14. | Total Staff – Company | |
| 15. | Total Staff – For This Project | |



[**VENDOR'S COMPANY STAMP HERE**]

**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 RFP 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. | | | |
| 4. | | | |
| 5. | | | |

Failure to provide suitable references may result in the Vendor's proposal being rejected without further consideration.

**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 _____



[**VENDOR'S COMPANY STAMP HERE**]

## 3. Specifications and Features

The offered solution by the vendor should fulfill the following requirements where vendors are to response int the Tender Response column indicating the location (page#) where the informations/requirments stated or shown in the proposal document.

### A. Product Architecture

| Description | Requirements | Vendor Response (Proposal Page #) |
|---|---|---|
| 1. Deployment | a. Vendors are to describe how they will implement the proposed SIEM Solution.<br>b. Fully centralized (central collection, central analysis & alerting.<br>c. Virtual machine-based (virtual appliances for collection and analysis & alerting).<br>d. Have its own data store that supports for active archival for short-term reference data, for up to one year.<br>e. Have its own, role based user management module with capabilities to assign and manage privileges, and shall support integration with Microsoft and/or industry standard identity & access management solution. | |
| 2. Infrastructure | a. Please indicate how many collectors/ aggregators/ analyzers.<br>b. What type (if the proposed Solution is based on point capability solutions) will be required for optimal levels of network protection.<br>c. Please provide justification for that number of devices/licenses. | |

| | | |
|---|---|---|
| 3. Licenses | Please indicate all of the licensing details for the proposed Solution:-<br>a. Perpetual<br>b. Licensed by:<br>i. Seat ;or<br>ii. IP address;or<br>iii. named-user;or<br>iv. Events per second. | |
| 4. Supporting Devices | The proposed Solution does not require a separate reporting device / license. | |
| 5. Scability | Individual collector/aggregator/analyzer can be scaled and managed via the management interface. | |
| 6. System Integration | Integrate without customisation ( Out of the box):-<br>a. Perimeter anti-malware solutions<br>b. Firewall/UTM solutions<br>c. Intrusion detection/prevention solutions<br>d. Managed network switches<br>e. Enterprise WIFI<br>f. Managed routers<br>g. Application servers (application logs)<br>h. Database servers (database logs)<br>i. Web servers<br>j. Communications servers (Icewarp / exchange email)<br>k. Workstation security solutions (anti-virus, anti-malware, desktop management, )<br>l. Identity and Access Management systems<br>m. Configuration Management Database<br>n. Workstation and server operating systems | |



[**VENDOR'S COMPANY STAMP HERE**]

**B. Product Features**

| Description | Requirements | Vendor Response (Proposal Page #) |
|---|---|---|
| 1. Discover and collect event data from all infrastructure devices and servers. | a. Support automated discovery of information processing equipment/devices, through an agent-less deployment.<br>b. Capable of discovering new information processing equipment/devices, added to the existing scope.<br>c. Capable of collecting, understanding or provide standardized support in identifying all types of event/log data formats, generated by operating-systems, virtual-machines, networking equipments, security devices, applications (custom-made & out-of-shelf), web-servers, databases, any other IT infrastructure devices and industry recognized formats (like SNMP Trap, SYSLOG, etc.).<br>d. Store event/log data in a compressed manner.<br>e. Collecting event data over a secure channel<br>f. Support automated timestamp synchronization through standard Network Time Protocol (NTP).<br>g. Capable of detecting inconsistencies/ variations in the source time stamp and provide meaningful / right information for correlation. | |



[**VENDOR'S COMPANY STAMP HERE**]

| | | |
|---|---|---|
| 2. Correlation<br>Correlate event data and effective detection of complex cyber-attacks & security incidents. | a. Real-time cross-correlation of events across AKPK information processing environment to identify security incidents and identify key performance issues of information processing equipments / devices, under the scope of solution's coverage.<br>b. Correlation mechanism used to correlate and identify anomalies. The details shall at least include:-<br>• Behavioral patterns considered;<br>• Time frame during which events/logs are considered;<br>• Predefined criteria;<br>• Useful information from other integrated security infrastructure.<br>c. Correlation algorithm;during correlation, the solution shall consider the following:-<br>1) Distinguish between authorized privileged operations and anomalies<br>2) Failed authentication request<br>3) Failed resource access (authorization)<br>4) Successful logons, after consecutive failed access attempts.<br>5) Network failures and floods<br>6) Start-up / start & shut-down / stop of system(s) and service(s).<br>7) Changes in the operating environment:<br>• System state<br>• Operationg systems<br>• Application<br>• Database<br>• Configuration files<br>• Network infrastructure<br>• Security infrastructure | |

| | | |
|---|---|---|
| | • Privileges<br>• Access methods<br>d. Classifying /identifying anomalies and performance issues.<br>e. Results of correlations should provide meaningful information.<br>f. The solution shall be capable of integrating with other security infrastructures of AKPK (like vulnerability management solution, data leakage prevention solution, firewall, intrusion preventions system, end-point security solutions, etc.) to correlate and provide a central dash-board to manage all security related anomalies. | |
| 4. Ability to analyse | a. The solution shall provide for deep data analysis, so as to generate meaningful information to satisfy requirements of;<br>▪ Management reporting<br>▪ Addressing security and operational anomalies<br>▪ Protocol analysis<br>▪ Compliance and audit reporting<br>▪ Forensic analysis<br>▪ Trend analysis & predictions<br>▪ Bench marking<br>▪ Anomaly identification with respect to most affected system, mostly present incident type, etc.<br>▪ Detailed reporting<br>b. Based on defined criteria's, the solution shall provide automated analysis report on a daily/weekly/monthly/yearly basis, and shall | |

| | | |
|---|---|---|
| | be forwarded to identified resources through AKPK's e-mail infrastructure.<br>c. The solution shall provide options to save generated analysis reports, with-in and/or out-of the solution.<br>d. Ability to conduct analysis and generate report shall be controlled through appropriate privilege assignment. | |
| 5. Data Management- Preserve native logs and maintain central repository of log data | a. Preserve all native logs, generated by various system/ equipments/ application/ service.<br>b. Maintain a central repository of log data, in its native and normalized forms, for a period not less than one year.<br>c. Purging of data, from the central log repository shall be allowed only after successful archival of log data.<br>d. Access to the log repository shall be controlled by the solution, and shall be granted only to administrators.<br>e. Integrity of log data shall be maintained by the solution, and attempts to modify log data shall be logged and alerted.<br>f. Native logs at no point-in-time shall be modified and shall support, as evidence/records, for legal proceedings and forensic analysis.<br>g. The solution shall support AKPK's requirements on log retention.<br>h. Support data archival and shall have capabilities in making reference to archive logs, during analysis and report generation. | |
| 6. Alerting and reporting | a. Built-in and customizable reporting format to generate comprehensive and brief reports, | |



[**VENDOR'S COMPANY STAMP HERE**]

| | | |
|---|---|---|
| | with respect to the event data under consideration.<br>b. Generating incident report, with all relevant supporting data / information /evidence to provide detailed and brief insight into the incident, and shall support in the incident management process of AKPK.<br>c. Capabilities to provide executive reports, of events/incidents, in a pictorial representation.<br>d. Generating reports on changes to information processing equipments or devices.<br>e. Securing the following reporting requirements, as a minimum ;<br>▪ Reports based on individual system.<br>▪ Reports based on specific service.<br>▪ Reports based on specific events/incidents.<br>▪ Reports based on application(s) in use.<br>▪ Reports based on location.<br>▪ Reports based on source & target.<br>▪ Reports based on specific timing / duration.<br>▪ Reports based on priority / criticality of the events/incidents.<br>▪ Reports based on impact (system / service / application / infrastructure unavailability).<br>▪ Reports based on ownership of system / equipments / application / service.<br>▪ Reports based on changes to system / equipments / application / service.<br>▪ Reports on exploited . | |

| | | |
|---|---|---|
| | ▪ Reporting formats – at least two of the following formats “PDF, MS Excel, HTML & plain text”.<br>▪ Reports based on native format of the system / equipments / application / service under consideration.<br>f.Produce a pictorial representation of the anomaly detected, highlighting all involved components and affected systems / equipments / applications / services.<br>g. Provide for the export of log / event data (selective or complete).<br>h. Support audit and forensic requirements of the authority or regulatory / law enforcement authorities, by means of providing required event data information and the relevant native log information (native-format) of the event.<br>i. Meaningful use of off-line storage, archived log-data for compliance requirements.<br>j. On real-time basis, the system shall have the capability for early alerting of identified/nominated individual or group of individuals, by means of e-mail & SMS, at-least for the following situation/criteria;<br>▪ During detection of attack patterns & incidents affecting critical assets.<br>▪ During detection of incidents, targeted towards critical system/ equipments/ application/ service.<br>▪ During successful exploitation.<br>▪ During the health degradation or before failure of assets under scope.<br>▪ During high resource utilization. | |

| | | |
|---|---|---|
| | k. Detect and alert on any interruption caused in getting logs / event data or stoppage of event data logging, from the source, and the possible cause for the same.<br>l. Alerting mechanism shall be capable of the following as a minimum:-<br>▪ sending repeated alerts, till such time the incident is addressed or has been turned-off by authorized resources.<br>▪ Provide means for escalations, when the alerts are not addressed with-in stipulated time window, for various identified category of alerts.<br>▪ Manual alerting mechanism shall be provided by the solution, used by administrators to manually raise alerts during discovery of anomalies, using custom alerts.<br>▪ On a real-time basis, the solution shall alert the administrator(s) or nominated person, on identification/discovery of new information processing equipments or devices.<br>m. The solution shall provide for generating trend analysis reports.<br>n. Capabilities to provide remedial recommendations, to effectively mitigate reported incidents. | |



[**VENDOR'S COMPANY STAMP HERE**]

## C. Product Operations

| Description | Requirements | Vendor Response (Proposal Page #) |
|---|---|---|
| 1. Implementation and configuration | Please describe how to implement a fully functional SIEM with the following specifications: -<br>a. Capacity for 70 servers<br>b. Capacity for 25 network devices<br>c. Near real-time management<br>d. Real-time events analysis<br>e. Real-time correlation<br>f. Normalisation of data<br>g. Log/data retention for minimum 365 days.<br>h. Ablity to utilise SAN technology<br>i. SIEM data is encrypted .<br>j. Correlation rules and alerts are user-configurable via a GUI.<br>k. Data connectors available for common OS and Network elements.<br>l. 6 Security devices.<br>m. Bitdefender AV console and 300 AV clients.<br>n. Data Loss Protection system log. | |
| 2. Managing daily operations | a. Solution that is easy to maintain<br>b. Not require analyst to log in continuosly<br>c. Generate daily, weekly and monthly reports.<br>d. Not require extensive report customisation.<br>e. Easily configurable based on rules. | |



[**VENDOR'S COMPANY STAMP HERE**]

| | | |
|---|---|---|
| | f. Provide Automated Security Operation Center (SOC).<br>g. Simple interface that requires a minimal navigation to access information, modify configuration and define security,policy and rules. | |
| 3. Backup and recovery | a. Both backup and recovery should allow for full and incremental notions of backup.<br>b. Support off-site storage of backup. | |

**D. Post implementation support and maintenance**

| Description | Requirements | Vendor response |
|---|---|---|
| 1. **Warranty** | a. Warranty period should be in 3 months after system go-live.<br>b. All maintenenance during warranty period will be performed by a successful vendor.<br>c. All maintenance during warranty period will be at no additional cost to AKPK. | |
| 2. **Maintenance and support** | Successful vendor should provide standard service level agreement based on the following requirements:-<br>a. 24x7 support.<br>b. Phone support.<br>c. Online support.<br>d. Onsite support.<br>e. Problem log and escalation.<br>f. 4 hours response time.<br>g. 1-1 Hardware replacement (if any).<br>h. Consultancy and advice.<br>i. Continouse system improvement. | |

| | | |
|---|---|---|
| | **Preventive maintenance**<br>Successfull vendor will carry out **twice** a year a preventive maintenance.<br>• SIEM health check (monthly report).<br>• Version upgrade and Patch updates as and when required.<br>• Quaterly logs/alert review. | |

**E. Project Management**.

| Description | Requirements | Vendor response |
|---|---|---|
| 1. Project Management | a. The method and approach used to manage the overall project. Also, briefly describe the execution plan of the project, covering the complete life cycle of the project.<br>b. Please provide proposed Project Team Structure.<br>c. Provide a description of the proposed project team structure to be used during the course of the project, including any subcontractors. | |
| 2. **Staff Qualifications/ Experience** | a. Identify staff, including subcontractors, who will be assigned to the project.<br>b. Provide cv' for the Project Manager and Team lead, which include information on the individual's particular skills related to this project, education, experience, significant accomplishments (certifications) and any other pertinent information.<br>c. Please specify the relevant certification of the team for this project to support the proposal. | |



[**VENDOR'S COMPANY STAMP HERE**]

| | | |
|---|---|---|
| 3. **High Level Project Plan & Timeline** | a. Please provide a project plan, showing the high level activities, key dates, time frames, resources and dependencies for procuring and implementing the SIEM solution.<br>b. A detailed effort estimation chart, detailing efforts required for each of the activity identified as part of the project life cycle. | |
| 4. **Testing Process** | a. Please provide standard test methodology documented process for testing purposed SIEM solutions.<br>b. Provide high-level test plan including types of test and measurements that will be performed to validate the proposed solution and outcome of the tests. | |
| 5. **Training program** | a. Training is part of the project's requirements and the vendor shall provide details on the level of training recommended and to be presented included as a minimum the following:-<br>1. Transfer of technology (TOT)<br>2. Formal Class room training.<br>b. Describe training courses that are provided as part of the solution. | |
| 6. **Project experience** | List of 5 past related/similar project experiences and reference sites (year 2015, 2016, 2017, 2018 & 2019)<br>1. Project name & description.<br>2. Company name.<br>3. Year of award.<br>4. Project duration.<br>5. Total resources involved.<br>6. Size of deployment.<br>7. Number of partners involved. | |



[**VENDOR'S COMPANY STAMP HERE**]

**APPENDIX B**

## B. COST PROPOSAL

### 1. CHECKLIST

| No | Description | Tick | Envelope |
|---|---|---|---|
| 1. | Official Quotation ( Must provide details Bill of Materials) | | **Cost Proposal** |
| 2. | Cost Summary (as per item 2 below) | | |
| 3. | Propose Payment Term | | |
| 4. | Bank Info | | |

### 2. COST SUMMARY (One time Cost)

| No | Description | QTY | Cost per unit (RM) | Tax (RM) | Total Cost (RM) |
|---|---|---|---|---|---|
| 1 | SIEM and miscellaneous equipment (e.g., software, hardware) | | | | |
| 2 | Licensing | | | | |
| 3 | Training (system and user) | 4 Paxs | | | |
| 4 | Professional services for the above implementations. | 1 Lot | | | |
| 5 | Warranty and maintenance support (hardware and software) for year 1 | 1 Lot | | | |
| 6 | Documentation | | | | |
| 7 | Other costs (if any, please describe) | | | | |
| | Subtotal (One time Cost for year 1) | | | | |
| **Recurring Cost** | | | | | |
| 8 | Warranty and maintenance support (hardware and software) for year 2 Other costs (if any, please describe) | 1 Lot | | | |
| 9 | Warranty and maintenance support (hardware and software) for year 3 Other costs (if any, please describe) | 1 Lot | | | |
| | Subtotal ( recurring cost year 2 & 3) | | | | |
| | **GRAND TOTAL** | | | | |



[**VENDOR'S COMPANY STAMP HERE**]

## 3. PROPOSE PAYMENT TERM

| No | Description |
|---|---|
| 1. | Preferred Payment Term (min. 5% for each milestone)<br>i. Upon Project kick-off : 5%<br>ii. Upon Completion of Installation and Configuration : 30%<br>iii. Upon Completion of User Acceptance Testing : 30%<br>iv. Upon Completion of go-live : 20%<br>v. Upon Completion of user training : 10%<br>vi. Upon Project Closure and Handover to AKPK IT : 5%<br><br>(Please state if the payment term is not as per the above preferred term) |
| | Manner of Payment<br>i. Name of Bank :<br>ii. Address of Bank :<br>iii. Account number :<br>iv. Account type : Current / Saving<br>v. Account scheme : Conventional / Islamic |

(The remaining page is intentionally left blank)



[**VENDOR'S COMPANY STAMP HERE**]

## 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]