INVITATION TO QUOTE
ITQ REF NO: NKF/PL/2020/004
DATE: 9 MARCH 2020

TITLE: THE SUPPLY, DELIVERY, AND COMMISSIONING OF CYBERARK PRIVILEGED ACCESS SECURITY SOLUTION.

1. Introduction

1.1. The National Kidney Foundation ("NKF") wishes to invite vendor (the "Vendor") to quote for the supply, delivery, and commissioning of CyberArk privileged access security and application access management solution.

1.2. The Vendor shall provide a seamless transition for all users without any disruption to NKF operations.

2. Requirement Specification

2.1. Please refer to Annex A for details.

3. Submission of ITQ

3.1. The quotation submitted by the Vendor shall be as in "**Price Schedule**" - **Annex F**. Full set of quotation must be submitted with Vendor's stamp on all pages stipulated in the ITQ. The quotation may be submitted by hand or post in a sealed envelope and endorsed with the words "**ITQ Ref No: NKF/PL/2020/004 ITQ for the Supply, Delivery and Commissioning of Cyberark Priviledged Access Security Solution"**. All submission should be no later than **13 March 2020, Friday, 3pm** (the "**Closing Date**") and delivered by:

If sent by hand

To deposit to : ITQ Box A
Security Counter
National Kidney Foundation
81 Kim Keat Road
Singapore 328836
Attn: Ms Pauline Leong

If sent by post : National Kidney Foundation
81 Kim Keat Road
Singapore 328836
Attn: Ms Pauline Leong

3.2. The submitted quotation shall be irrevocable and open for acceptance by NKF for **90 days** from the Closing Date.

3.3. The Vendor, at the point of submission of its bids, is required to provide the following information and/or documents to NKF:

3.3.1. Annex A to H;

3.3.2. Comprehensive Credit Report

3.3.3. Extract of company/ business registration from the Accounting & Corporate Regulatory Authority (ACRA), showing a full list of directors/partners of the Vendor. The date of the extract of company/business registration from ACRA shall not be earlier than 26 October 2015; and

3.3.4. Any other documents relevant to the ITQ.

3.4. If you have any inquiries relating to this invitation to quote, please contact Ms Pauline Leong at telephone no 6506-2104 or email to pauline.leong@nkfs.org.

4. Terms and Conditions

4.1. The terms and conditions set out in **Annex G** shall form part of the binding contract between the successful Vendor and the NKF.

5. Price Quotations

5.1. All prices quoted by the Vendor shall be in the lawful currency of the Republic of Singapore and exclusive of GST.

5.2. All prices quoted by the Vendor shall represent the total cost to NKF.

6. Payment Schedule

6.1. The payment shall be paid according to the following schedule

6.1.1. 100% Payment for Hardware and Software upon delivery.

6.1.2. 100% Payment for Services Upon Services Completion.

ANNEX A

SPECIFICATIONS

NKF will be calling an ITQ for the supply, delivery, and commissioning of CyberArk privileged access security and application access management solution.

We are opening this ITQ to interested vendors for submission of quotations.

Refer to the following Annexes for more information.

Annex A: Specification – Project Scope of Work
Annex B: Technical Specifications
Annex C: High Level Project Plan
Annex D: Vendor's Experience in Similar Projects
Annex E: Project Requirement
Annex F: Price Schedule
Annex G: Terms and Conditions
Annex H: Information About Vendor

1. Project Scope of Work

1.1. To supply, delivery, commissioning, test, maintain of the CyberArk Privileged Access Security (PAS) solution.

1.2. The vendor shall ensure interoperability of the CyberArk PAS solution with the existing infrastructure, network, systems and applications including their future upgrades.

1.3. The vendor shall include the following scope of work in their proposal.

1.3.1. Supply, delivery, setup implementation and commissioning of PAS including:

(I) Latest version of software with media kit;
(II) 20 user licenses;
(III) Management of 400 managed IP target systems;
(IV) User behaviour analytic solution up till 400 IP target systems;
(V) Detection of Privileged Threat Account Analytics;
(VI) Unlimited number of password objects for management up till 400 managed IP target systems;
(VII) Unlimited installation of web portal for management access;
(VIII) Unlimited installation of privileged session management module;
(IX) All required hardware/virtualization for primary site and disaster recovery site.

1.3.2. Professional Services including

(I) Project plan and implementation approach upon award;
(II) Delivery, setup, configuration and implementation of PAS;
(III) User Acceptance Test (UAT) and documentation;
(IV) Vendor certified administrator training (06 pax).

1.4. To provide maintenance of the PAS solution including the following:

1.4.1. 24x7x4 on-site support on trouble-shooting of PAS and related software.

1.4.2. Implementation of software upgrades, patches and verification of PAS related software.

1.4.3. Assurance of setup by local product principal.

1.4.4. Provide half-yearly health check on the solution during the Contract Period.

1.4.5. All the supplied software and hardware.

1.5. The contract period for PAS is 3 years.

ANNEX B

TECHNICAL SPECIFICATIONS

1. General Requirements

1.1. The proposed solution shall secure and manage privileged password and session of systems and applications effectively.

1.2. The proposed solution shall provision 2 sets of test licenses for UAT/Development in the future.

1.3. Unlimited support of password object based on the proposed number of managed devices for password management, session recording and privileged threat analytic.

1.4. The proposed solution shall have System Health Monitoring capabilities Out Of Box. This shall be presented in a dashboard providing drill down functionality on overall system health and individual components.

1.5. For ease of self-help, the proposed solution shall provide Out Of Box documentation in the form of a searchable web portal.

2. Platform / Target System Support / OS

2.1. The proposed solution shall support the ability to manage passwords and perform session recording for the privileged accounts on the following platforms:

2.1.1. Windows (local and domain)
2.1.2. Linux
2.1.3. Solaris
2.1.4. Databases
2.1.5. Network Devices via SSH and Telnet
2.1.6. AS/400 (iSeries), via default port and support SSL
2.1.7. zSeries (OS/390), via default port and support SSL
2.1.8. Mainframe (Access Control Software)
2.1.9. Virtual Servers (e.g. VMware, Oracle VM, etc)
2.1.10. Client Server Based Applications i.e. SAP, Checkpoint Smart Dashboard etc.
2.1.11. Support any SSH devices
2.1.12. Support any ODBC devices
2.1.13. Support AWS console access keys credentials for its AWS IAM accounts
2.1.14. Support loosely connected devices (roaming Windows machines)

2.2. The proposed solution shall support target accounts organized by both policies and password safes**.**

2.3. The proposed solution shall automatically detect new Windows Desktops & Laptops devices, Windows services, scheduled tasks; IIS service accounts etc., provision them to the product and automatically enforce the right password policy on these new managed devices.

2.4. The proposed solution shall also automatically discover privileged accounts in an Active Directory, Linux/Unix environment and SSH Keys using a simple and intuitive web based wizard, and following a review of the results, to allow automatic provisioning of these accounts for password management.

2.5. The proposed solution shall facilitate creation and management of pre-defined account on boarding rules to automatically on board newly discovered accounts directly.

2.6. The proposed solution shall be able to automatically detect new hypervisors, guest machines in a dynamic virtualised environment, provision them to the product and automatically enforce the right password policy on these new managed devices.

3. SYSTEM ARCHITECTURE

3.1. The proposed solution shall provide multi-tier architecture where the database and application level is separated.

3.2. The proposed solution shall provide scalability where it is not limited by the hardware. Also the solution shall provide modular design for capacity planning and scalability metrics.

3.3. The proposed solution shall support for high redundancy or DR architecture even when deployed on different network segments or locations.

3.4. Data replication between different network segments shall be perform natively without the need for external solution or infrastructure.

3.5. **Distributed Setup**

3.6. The proposed solution shall supports Distributed Vault in a Master and Satellite Vault concept.

3.7. Distributed Vault shall have the ability to provide read only access to Vault data for front end services.

3.8. Satellite Vault shall consolidates audit records into the primary Master Vault to provide a complete view of all deployment activities in one place.

3.9. **Disaster Recovery**

3.10. The proposed solution shall have the ability to support multiple mirrored systems at offsite Disaster Recovery Facilities across different data centre locations

3.11. The proposed solution shall have ease of recovery should any fault occur, DR activation shall be as seamless as possible with minimum disruption to the day to day operations

3.12. **Backup and Restoration**

3.13. The proposed solution shall have built-in options for backup or integration with existing backup solutions

3.14. The proposed solution backup shall be encrypted with strong security controls.

3.15. Restoration of the backup data to the proposed solution shall be protected with strong authentication.

3.16. **Network Architecture**

3.17. The proposed solution shall handle loss of connectivity to the centralized password management solution automatically.

3.18. The proposed solution shall not require any network topology changes in order to ensure all privileged sessions are controlled by the solution.

3.19. Supports distributed network architecture where different segments need to be supported from a central location.

4. APPLICATION SECURITY

4.1. The proposed solution should use built-in FIPS 140-2 validated cryptography for all data encryption.

4.2. The proposed solution should have minimum Common Criteria Evaluation Assurance Level EAL 2+.

4.3. Communication between system components, including components residing on the same server should be encrypted.

4.4. The proposed solution shall provide full encrypted backups where back up keys are self-managed and securely stored by the system.

4.5. Secured platform - main password storage repository should be highly secured (built-in firewall, hardened machine, limited and controlled remote access etc.) where the super administrator user should not be accessible via web interface/remote client.

4.6. Secure and tamper-proof storage for audit records, policies, entitlements, privileged credentials, recordings etc.

4.7. Each password containers and password object stored in the password safes in the solution shall be encrypted by unique encryption keys.

4.8. Access to super administrator account (for recovery and full access) of the system should be allowed only locally from the application server where the database and secured passwords and recordings are stored. 2FA authentication if possible should be enforce to ensure integrity of the super administrator logon.

4.9. Administrative configurations (e.g. configuration of user matrix) shall be accessible via a separate client where client access is controlled by IP address.

4.10. Segregation of Duties - The Administrator user cannot view the data (passwords) that are controlled by other teams/working groups (UNIX, Oracle etc.).

4.11. If external identity stores are used, the proposed solution should perform reconciliation to ensure synchronization. E.g. when a user is added/removed from the directory, it is automatically provisioned/de-provisioned in the solution.

4.12. The proposed solution supports integration with the Hardware Security Module (HSM) devices to store the encryption keys.

4.13. The proposed solution provides several authentication options for logging on to the system such as local database, Windows, PKI, RADIUS, RSA SecurID, Oracle SSO, LDAP, SAML and Google Authentication.

4.14. Ability to provide detailed auditing information regarding any privileged access related activities.

4.15. Ability to automate tasks which are usually performed using Web UI using API. The API must be able to be used immediately without any additional configuration.

5. PRIVILEGED ACCOUNT MANAGEMENT

5.1. The proposed solution shall preferably provide a tool to discover where the privileged accounts exist, verify privileged accounts risks, identify all privileged passwords/SSH Keys/password hashes, embedded credentials in IIS , WebLogic, WebSphere, Ansible, Microsoft SQL Database, and Cloud users/instance keys in AWS.

5.2. The proposed solution shall provide ease of policy *management including:*

5.2.1. Allow single baseline security policy across all systems, applications and devices (e.g. one single update to enforce baseline policy)

5.2.2. Ability to create exception policies for selected systems, applications and devices

5.3. The proposed solution shall perform password change options which is parameter driven.

- 5.3.1. Ability to set password options every 1 days, months, years and compliance options *via the use of a single, master policy*
- 5.3.2. Ability to change passwords at one time for single, group and all systems based on specific criteria
- 5.3.3. The product should support changing a password or group of passwords *via a single master policy*:
  - (I) According to a policy (every 1 days or 'on-demand')
  - (II) Manually by a user
  - (III) Automatically, when a password is not synchronized (verification failure)

5.4. The proposed solution should change target accounts passwords be set to a random value

- 5.4.1. Ability to change target accounts passwords manually by an administrator at any time
- 5.4.2. Ability to automatically “check-out” after a specific time and “check-in” within a specified time

5.5. The proposed solution shall support password verification

- 5.5.1. Automatically verify password value against its target system
- 5.5.2. Auto notify on 'out of sync' passwords
- 5.5.3. Report on all 'out of sync' passwords

5.6. The proposed solution shall support password reconciliation

- 5.6.1. Automatically reconcile passwords that are detected 'out of sync' or lost without using external restore utilities
- 5.6.2. Ability to reconcile the passwords on selected, multiple or all systems.
- 5.6.3. Ability to reconcile passwords manually, upon demand

5.7. The proposed solution shall have support password policies

- 5.7.1. Ability to set a minimum password length and complexity for super-user accounts across all systems in a single master policy
- 5.7.2. Ability to maintain password history, e.g., last three passwords or by timeframe and provide easy access to them through the product web interface.
- 5.7.3. Ability to manage super-user accounts that have been renamed from the default name
- 5.7.4. Ability to enforce the password policy when manually changing accounts as well as when the systems randomly changes the password
- 5.7.5. Ability to enforce 8 last unique passwords (i.e. do not repeat last 8 passwords)
- 5.7.6. Ability to provide unique passwords per device.
- 5.7.7. Ability to enforce different policies per line of business when the device type is the same

5.7.8. Ability to enforce unified policies for privileged account management and session monitoring

5.8. The proposed solution shall have the following password checkout process
- 5.8.1. Supports multiple LDAP realms for authentication, e.g. Sun One, MS AD.
- 5.8.2. Ability to generate 'one-time' passwords as an optional workflow
- 5.8.3. Ability to send notifications via email or other delivery methods triggered by any type of activity
- 5.8.4. Ability to checkout a password for a specified time period, e.g., hour and/or days.
- 5.8.5. Ability to send notification via email to the user requesting the password that checkout is completed
- 5.8.6. Ability to send notification via email to the user notifying them of password expiration where a new password has not been assigned (e.g. password needs to be changed manually)
- 5.8.7. Flexibility that allows exclusivity for password retrieval or multiple users checking out the same password for the same device in the same time period

5.9. The proposed solution shall be able to connect to the target systems
- 5.9.1. Supports transparent connection to the target device, without seeing the password or typing it as part of the connection
- 5.9.2. Provides the ability to support direct connection to the Windows Managed Devices
- 5.9.3. Provides the ability to support direct connection to the Unix/Linux Managed Devices (SSH)
- 5.9.4. Dynamic support for additional target systems that are not supported out-of box
- 5.9.5. The system shall have the ability to send emails for the following:
- 5.9.6. System Access
- 5.9.7. System Changes
- 5.9.8. Password Usage
- 5.9.9. Password Requests and Approvals

5.10. The support for AD Bridge capability must be agent-less.

5.11. The AD Bridge must be able to integrate with centralized management and auditing capabilities.

5.12. The proposed solution must be able to limit Domain Account access to specific remote machines

5.13. The proposed solution must be able to provide flexibility to configure web plugins to allow connection to web related application via chrome browser

6. PRIVILEGED ACTIVITY MONITOR & RECORDING

6.1. The proposed solution should be able to record privileged sessions out of the box under 4.0 PLATFORM/TARGET SYSTEM SUPPORT/OS indicated above.

6.2. The proposed solution shall be expandable to support any application or device connection including web applications for monitoring and enabling privileged single sign on.

6.3. The proposed solution shall not require any forms of agent to be deployed on target systems to allow for recording search capability across all platforms.

6.4. The proposed solution shall have keystroke recording across all platforms.

6.5. The proposed solution shall have the capability to search across both text and windows based recording by keywords, time, users and target address

6.6. The proposed solution shall allow reviewing of recording from point in time of the searched keyword for both text and windows based recording instead of playing from beginning of the recording

6.7. The proposed solution shall cater for live monitoring of sessions and manual termination of sessions when necessary

6.8. The proposed solution shall allow a blacklist of SQL commands that will be excluded from audit records during the session recording. All other commands will be included.

6.9. The proposed solution shall allow the creation of SSH command white-listing and black-listing in SSH sessions without the need of an agent installed on the target system.

6.10. The proposed solution shall enable users to connect securely to remote machines through the session recording tool from their own workstations using all types of accounts, including accounts that are not managed by the privileged account management solution.

6.11. The proposed solution shall allow configuration at platform level to allow selective recording of specific users and groups. In addition, certain users and groups can be excluded from that this list.

6.12. The proposed solution shall allow specific commands to be executed for RDP connections (e.g. Start the connection by launching a dedicated program on the target machine without exposing the desktop or any other executables).

6.13. The proposed solution shall support correlated and unified auditing for shared and privileged account management and activity.

6.14. The proposed solution shall support adding custom code in session pre-connection or post-connection phases to perform specific logic before the session starts or ends in order to trigger certain activities and workflows with external systems.

6.15. The proposed system shall support full colour and resolution video recording.

6.16. The proposed system shall support video session compression with no impact on video quality.

6.17. All activities performed by requestors shall be recorded including mouse-trail movement for RDP session.

6.18. Established session shall have the function to be remotely viewed on a live feed / live monitored situation.

6.19. Auditors / session reviewers shall have capabilities to remote terminal an established session.

6.20. If Microsoft Remote Desktop Host / Terminal server is needed as part of implementation, to include CAL licensing required

6.21. The proposed solution shall provide the ability to provide classification of recording safes based on user-defined dynamic parameters.

6.22. The proposed solution shall provide alternative ways to provide the user the native experience to logon to the Target Unix and Windows servers through the gateway using their own native SSH and RDP Client.

6.23. The proposed solution shall provide alternate connectivity methods such as HTML 5 based proxy to prevent limitation which might occur due to user OS platform or browser.

6.24. The proposed solution must be able to do risk-based prioritization of privileged sessions review by Auditors and Security teams.

6.25. The proposed solution must provide Searchable and detailed audit trail for applications – Software-as-a-Service (SaaS), Cloud Consoles, Client Applications.

7. SYSTEM ADMINISTRATION

7.1. Central administration within unified suite (single user interface, central repository).

7.2. The proposed solution shall support both client based (in the case where browser is not available) as well as browser based administration.

7.3. If a back-end database is used, the solution needs to be fully self-managed and should not require a database administrator (DBA) for production deployment, backup/recovery or database hardening.

7.4. The proposed solution should restrict the solution administrators from accessing or viewing passwords or approve password requests.

7.5. Ability to track usage for up to 01 year and report changes of the solution for up to 01 year.

7.6. Ability to provision users via AD or LDAP Directory including ongoing, transparent and automatic provisioning of accounts to reflect changes in the directory.

7.7. Transparent group/role management using AD Groups or via LDAP Directory for Role Based access control.

7.8. The proposed solution should support bulk operations performed on accounts.

7.9. The proposed solution should be able to assess privileged account security risks and highlight potential pass-the-hash risks.

7.10. The proposed solution should be 100% agentless that includes password storage, password management and session recording features.

7.11. The proposed solution shall have a system health monitoring page to have an overview of all the running components.

8. ENTERPRISE INTEGRATION

8.1. Ability to integrate with enterprise authentication methods e.g. multiple 3rd party authentication methods including LDAP, Windows SSO, PKI, RADIUS, SAML and a built-in authentication mechanism.

8.2. Ability to integrate with LDAP/AD Directories.

8.3. Ability to support querying and controlling access to passwords for nested global groups, including multiple forests, geographical locations, sophisticated LDAP searches and high performance queries.

8.4. Ability to integrate with (Arcsight) SIEM systems.

9. WORKFLOW SUPPORT

9.1. Ability to support dual control - The system should support different configurations of approvals e.g. “4-eyes principle” when trying to retrieve a password including automatic email notification support.

9.2. The proposed solution shall support user requesting the use of a target account for a future date/time.

9.3. Supports a workflow approval process that is flexible to assign multiple level of approvers based on product or model (i.e. require 2 or more approvals before access is allowed).

9.4. Supports a workflow approval process that requires approvers to be in sequence before final approval is granted.

9.5. Supports a workflow approval process that only allows the direct manager of a requester to approve a request based on information from the LDAP server.

9.6. Ability to support split password process where each half of a password can only be checked out by an authorized requester while storage of password is in full to ensure password is changed automatically.

9.7. Ability to log workflow processes and/or have the ability to be reported or audited.

9.8. The proposed Solution shall support the ability to secure access to target Windows systems from the user’s endpoint using their preferred RDP Client Applications.

9.9. Supports an Ad-Hoc access with Just-in-Time access to Windows Server with a customizable timeframe.

10. REPORTING/AUDIT/ASSESSMENT

10.1. Map privileged and personal accounts in the organization with a standalone tool

10.2. Ability to easily discover and flag accounts that do not adhere to the corporate password policy without having to implement a PAS solution.

10.3. Ability to list accounts used to login to workstations/servers in the last 90 days (last quarter for example) without having to implement a PAS solution.

10.4. Ability to quickly identify all non-built-in local administrator accounts in your environment (flag possible 'backdoor' accounts) without having to implement a privileged account management system.

10.5. Dashboard - for at a glance management of devices, events and password policies. Describe your dashboard capabilities

10.6. The solution shall have the ability to run all reports by frequency, on-demand and schedule them

10.7. The solution should provide detailed and scheduled reporting with the following basic reports:
- 10.7.1. Entitlement
- 10.7.2. User's activities
- 10.7.3. Privileged Accounts inventory
- 10.7.4. Applications inventory
- 10.7.5. Compliance

10.8. The solution shall support the following report outputs:
- 10.8.1. Formatted Microsoft Excel
- 10.8.2. CSV
- 10.8.3. Output to an external database (MS SQL)

10.9. Ability to report on All System Administrative Changes

10.10. Ability to report on System Access

10.11. Ability to report password checkouts on systems and users requesting passwords

10.12. Ability to report password lockouts (failure logon attempts)

10.13. Ability to report on verification of password value

10.14. Ability to report on password change following verification process

10.15. Ability to report on reconciliations on single & multiple systems. Reconciliation is the automatic recovery by the system when a password has been (mistakenly) changed on the target device but not synchronised with the solution

10.16. Ability to report on passwords that mismatch their policy

10.17. Ability to report by system id or device type within a policy

10.18. Ability to report on password status

10.19. Reports should be customizable

10.20. Reports shall be automatically distributed by email

10.21. Access to audit reports (and report configuration) shall be restricted to "auditor" end-users

10.22. Ability to replay actual session recordings for forensic analysis

11. Privileged Accounts Threat Analytics

11.1. To be able to provides intelligence-driven analytics to identify suspicious and malicious privileged user behaviour.

11.2. To be able to detect malicious activity caused by privileged accounts and proactively responds to in-progress attacks.

11.3. The proposed additional solution must have the following capabilities:

11.3.1. Detection of security incidents on authorized users and managed accounts - To be able to detect security incidents on abnormal privileged user activities / managed privileged accounts.

11.3.2. Response to security incidents flagged -To be able to generate actionable insights to support rapid incident mitigation.

11.3.3. Determines overall risk score based on overall security events flagged - Calculates an overall threat index of the system to indicate an ongoing threat or attack.

11.3.4. Ability to response immediately to security incidents when unauthorized commands are executed during an on-going privileged session.

11.3.5. Assist auditors to prioritize on reviewing of privileged session video recordings based on the risk score rating.

11.4. The Proposed Solution shall be able to detect the following Profiles such as :

11.4.1. Privileged access during irregular hours – Detected when a user retrieves a privileged account password at an irregular hour for that user.

11.4.2. Excessive access to privileged accounts – Detected when a user accesses privileged accounts more than the number of times that characterize that user.

11.4.3. Privileged access from irregular IP – Detected when a user accesses privileged accounts from an unusual IP address or subnet.

11.4.4. Machine accessed from irregular IP – Detected when a machine is accessed from an unusual IP address or subnet.

11.4.5. Machine accessed during irregular hours – Detected when a machine is accessed at an irregular hour.

11.4.6. Machine accessed excessively – Detected when a machine is accessed more frequently than normal for that machine.

11.4.7. Irregular source machine – Detected when a user logs onto a target machine from an unusual source machine.

11.4.8. Irregular user logged on from a source machine – Detected when access from a source address is performed by an unusual user at this source address.

11.4.9. Irregular target machine – Detected when a user accesses an unusual target machine for this user.

11.4.10. Suspected credentials theft – Detected when a user connects to a machine without first retrieving the required credentials from the Vault.

11.4.11. Unmanaged privileged access – Detected when a connection to a machine is made with a privileged account that is not managed in the Vault.
Or a connection to a machine or a cloud service is made with a privileged account that is not stored in the Vault
Or detected when an account is added in to the Windows Local Administrator group of a Windows Machine

11.5. Active Dormant - User - Detected when a relatively inactive PAM User accounts is activated and used to login to the PAM solution.

11.6. Unconstrained Delegation - Detected when service accounts that are granted with permissive delegation privileges.

11.7. Exposed Credentials - Detected when exposed credentials transmitted in plain text over the network. The exposed credentials risk is caused by a service that allows authentication with LDAP in a non-secured manner.

11.8. Unauthorized Commands - Detected when a list of user-defined unauthorized commands are executed during an on-going privileged session.

11.9. Interactive Logon of Service Account- Detected when a service account is used for interactive logon on the Windows Server Operating Systems.

11.10. Detection of Risky service accounts – Detect Privileged Accounts with SPN(service principal name) configurations that are vulnerable to offline- brute-force and dictionary attacks, allowing a malicious insider to recover the account’s clear-text password.

11.11. Irregular day anomaly – Detect abnormal work day activity of privileged users.

11.12. Suspicious password change - Detected an activity to change or reset a password on the target Windows Server Operating Systems.

11.13. PAC attack - Detected an indication of a PAC (Privilege Account Certificate) attack in the network.

11.14. OverPass the Hash attack – Detected an indication of an Overpass the Hash attack in the network.

11.15. Golden Ticket attack - Detected an indication of a Golden Ticket attack in the network.

11.16. These alerts shall be made available and all system activity, analysis to be displayed in a dashboard with the information constantly updated on the overall system score according to the number of incidents (bubbles) and their risk index.

11.17. These alerts shall be made available and all system activity, analysis to be displayed in a dashboard with the information constantly updated on the overall system score according to the number of incidents (bubbles) and their risk index.

11.18. The proposed solution should also correlates multiple security events that occur during a certain period involving the same authorized user and/or attacked asset into one or more incidents.

11.19. The proposed solution shall be able to provide an overview of general system status for a selected period of time, as well as details about current and past incidents and a summary of system activity. Information displayed should be in multiple graphic analyses of system activity and security incidents to be able to see and understand system activity at a glance.

11.20. The proposed solution shall be able to integrate with organization infrastructure which include:

11.20.1. LDAP integration
11.20.2. Email notification
11.20.3. HP Arcsight / SEPM EDR / SEPM

11.21. The proposed solution shall be able to generate high-level report of all anomalies for a particular authorized user during a specified period.

11.22. The proposed Solution shall automatically add unmanaged Privileged Accounts detected to the list of accounts to be on-boarded into the system.

11.23. The proposed Solution shall be able to define a response to highly risky activities. Activities that shall be configured are:

11.23.1. Automatically remediate by rotating the credential used immediately for credential theft incident.
11.23.2. Automatically remediate by terminating the risky privileged session.
11.23.3. Automatically remediate by suspending the risky privileged session.
11.23.4. Allow detailed assignment of high risk commands based on specific define scope.

ANNEX C

HIGH LEVEL PROJECT PLAN

Proponents should provide a project plan, showing the high level activities, key dates, time frames, resources and dependencies for procuring and implementing the PAM solution. The plan should have defined steps with specific milestones covering all critical elements of the commissioning process. Included in the commissioning plan should be the expected outcome of the activities to be performed.

ANNEX D

VENDOR'S EXPERIENCE IN SIMILAR PROJECTS

**** All requirement mentioned herewith are mandatory, sufficient details must be provided to demonstrate relevance to this project***

S/N	Item	Numbers / Description
1	Total number of successful PAM solution implementations projects (> $100k SGD) in last 2 years	
2	Provide list of local client references of successful implementation of similar projects (at least 3 local client references)	
3	Past infrastructure projects experiences with NKF Information Technology Department.	
4	Provide client and project information of successful implementations of similar projects (at least 3 local client references) Client Information 1.1 Customer Name 1.2 Company Address 1.3 Company Description 1.4 Contact Person 1.5 Contact Person Telephone Number 1.6 Contact Person Email Address Project Information 1.7 2.1 Estimated Project Value (S$) 1.8 2.2 Project / Scope Description 1.9 2.3 Duration of Project	

ANNEX E

PROJECT REQUIREMENT

All requirement mentioned herewith are mandatory

S/N	Requirement	Comply (Yes / No)	Remarks
1	**Specifications** As specified in **ANNEX A.**		
2	**Technical Specifications** As specified in **ANNEX B.**		
3	**High Level Project Plan** Please provide details listed in **ANNEX C.**		
4	**Track Record** Please provide details listed in **ANNEX D**.		

ITQ REF NO: NKF/PL/2020/004
DATE: 9 MARCH 2020

ANNEX F

INVITATION TO QUOTE
FOR THE SUPPLY, DELIVERY, AND COMMISSIONING OF CYBERARK PRIVILEGED ACCESS SECURITY SOLUTION.

PRICE SCHEDULE

No.	Item	Quantity Required	Unit Price (exclusive of GST)	Total Price (exclusive of GST)
	Upfront 3 Years Subscription			
1	PAS-User-T1 (Protects IT personnel and isolates datacenter resources. Including credential and access management, session isolation and recording, threat analytics) - 36 Months	20	**$**	**$**
2	CyberArk APAC Maintenance - 24x7 - 36 Months	1	**$**	**$**
	Professional Service			
3	Installation for CyberArk	1	**$**	**$**
	Training			
4	Privileged Account Security Administration - Per attendee (4 days training) The Privileged Account Security (PAS) Administration course	4	**$**	**$**
5	CPM Plugin & PSM Connector Development Per attendee, (4 days training)	2	**$**	**$**
	Post-Project Support			
6	Onsite technical support 3 year 7 x 24 support with 4 hours response	1	**$**	**$**

Accepted By:

Authorized Signature: _____ Date: _____

Signatory Name: _____ Signatory Title: _____

Telephone Number: _____ Vendor's Name: _____

Email Address: _____ Vendor's Stamp: _____

ANNEX G

TERMS AND CONDITIONS

1. Confidentiality

1.1 The Vendor agree to treat as confidential all information received from NKF where NKF has indicated in writing or labelled to be "Confidential", "Proprietary Information" or with any other comparable legend to similar effect, at the time of disclosure (or if disclosed orally, confirmed in writing by NKF as such within fifteen (15) days after its disclosure), which it may acquire in relation to NKF, including but without any limitation whatsoever, all business information, strategic and development plans, any matter concerning NKF, its affairs, business, shareholders, directors, officers, business associates, clients, patients or any other person or entity having dealings with NKF; information relating to the financial condition of NKF, its accounts, audited or otherwise, notes, memoranda, documents and/or records in any form whatsoever whether electronic or otherwise, and all records indicative of the financial health and status of NKF; technical information in any form whatsoever whether electronic or otherwise; information in any form whether electronic or otherwise, relating to methods, processes, formulae, compositions, systems, techniques, inventions, machines, computer programs, software, development codes and research projects; business plans, co-developer/collaborator identities, data, business records of every nature, customer lists and client or patient database, pricing data, project records, market reports, sources of supply, employee lists, business manuals, policies and procedures, information relating to technologies or theory and all other information which may be disclosed by NKF to the Vendor which the Vendor may be provided access by NKF whether stored electronically or otherwise; all information which is deemed by NKF to be confidential or which is generated as a result of or in connection with the business of NKF and which is not generally available to the public; and all copies, reproductions and extracts thereof, in any format or manner of storage, whether in whole or in part, together with any other property of NKF made or acquired by the Vendor or coming into their possession or control in any manner whatsoever (the "**Confidential Information**"), which shall be and remain the sole property of NKF and shall be returned to NKF forthwith on demand at any time.

1.2 The Vendor shall use all reasonable steps to ensure that any information marked as confidential or proprietary to NKF shall not be disclosed to third (3rd) parties.

1.3 The Vendor shall not, without the prior written consent of NKF, disclose any Confidential Information relating to this Contract or any of the contents hereof whether directly or indirectly to any third (3rd) party, which consent shall not be unreasonably withheld, except:-

(a) for the purpose contemplated in this Contract;

(b) with the consent of the other Party and then only to the extent specified in such consent;

(c) in accordance with the order of a court of competent jurisdiction; or

(d) to the extent as may be required by law, regulation, effective government policy or by any regulatory authority arising out of this Contract or relating to or in connection with the Vendor provided that the Vendor so required must give NKF prompt written notice and make a reasonable effort to obtain a protective order.

1.4 The restrictions on disclosure of Confidential Information described in this Clause 1 do not extend to any information that (i) already exists in the public domain at the time of its disclosure; (ii) is already in the Vendor's possession without restriction on disclosure, as evidenced by

written records; (iii) is independently developed by the Vendor outside the scope of this Contract; or (iv) is rightfully obtained from third (3rd) parties.

1.5 The Vendor hereby agrees that it shall:

(a) take all reasonably necessary steps to limit access to Confidential Information of the other Party to those principals, directors, officers, agents, employees, representatives, consultants, independent contractors and professional advisors who are directly concerned with the purposes contemplated by this Contract and are made aware of its confidential status, to the extent reasonably required for the performance of this Contract, and ensure that they do not disclose or make public or authorise any disclosure or publication of any Confidential Information in violation of this Contract; and

(b) not to use any Confidential Information for any purpose other than the purposes for which it is intended, pursuant to and in accordance with the terms of this Contract.

1.6 The Vendor must promptly inform NKF about any unauthorised disclosure of NKF's Confidential Information.

2. Payment

2.1 Unless otherwise specifically provided in this Contract or otherwise agreed between the parties, NKF's obligation to pay is conditional upon its receiving an invoice from the Vendor for the amount payable, giving NKF no less than thirty (30) days from receipt of such invoice to make payment.

2.2 If any invoice is not submitted to NKF within six (6) months upon completion of the Services, NKF shall be released and discharged from any liability to make any payment of the debt in relation to such invoice.

2.3 Payment by NKF of any invoices shall not affect NKF's right to reject any of the Services or Deliverables or the Vendor's responsibility to re-perform any Services or re-deliver any Deliverables that do not conform to this Contract. NKF shall have no obligation to pay for any such Services or Deliverables which have not been re-performed or re-delivered by the Vendor in accordance with Requirement Specification in Annex A. Such non-payment shall not constitute a default or breach of this Contract by NKF. In the event of any dispute between NKF and the Vendor with respect to the invoiced Services and/or other related matters, NKF shall pay the undisputed amount and NKF and the Vendor shall promptly seek to resolve the disputed matters with the Vendor.

2.4 The Vendor shall submit such invoices or other documents as NKF may require for the purpose of making payment.

2.5 NKF shall not pay for expenses or cost of whatever nature other than those expressly set forth in this Contract.

2.6 There will be no late payment service charge of any kind.

3. Termination

3.1 NKF shall be entitled to terminate this Contract, giving the other not less than two (2) months' notice in writing and thereupon this Contract shall come to end but without prejudice to any right of action of either party against the other in respect of any antecedent breach of the terms and conditions of this Contract by the other. For the avoidance of doubt, no reason needs to be given for the said notice.

4. Personal Data

4.1 Without prejudice to Clause 1 herein, the Vendor shall take all reasonable measures to ensure:

(a) that any personal data (as defined in the Personal Data Protection Act 2012 ("Act") as may be amended from time to time) belonging to NKF which is held by the Vendor pursuant to this Contract is protected against loss, unauthorised access, use, modification, disclosure or other misuse in accordance with the provisions of the Act and/or its regulations etc, and that only authorised personnel have access to that personal data;

(b) that, to the extent that the personal data is no longer required by the Vendor for legal or business purposes, that personal data is destroyed or re-delivered to NKF in accordance with this Contract;

(c) that NKF is immediately alerted in writing (with full particulars) of any unauthorised access, disclosure or other breach of this Clause 4 and the Vendor shall take, as soon as reasonably practicable, all steps to prevent further unauthorised access, disclosure or other breach of this Clause 4 (including providing NKF with such reports or information concerning such steps as and when requested by NKF); and

(d) it keeps itself appraised of any and all notices and circulars which NKF may from time to time notify to the Vendor, including without limitation any policies, guidelines, circulars or notices relating to personal data ("**Documentation**"), and to perform its duties or discharge its liabilities pursuant to this Contract in a manner which is consistent with Documentation, and will not cause NKF to be in breach of the same.

4.2 For the purposes of (c) above, the Vendor hereby expressly acknowledges and agrees that it has read the Documentation and is aware of and will compensate NKF for any and all potential loss and damage caused to NKF arising from or in connection with any breach of the above. The Vendor will indemnify and hold NKF harmless from claims or proceedings by third parties and any proceedings, investigations, orders, directions, judgments issued by a court, statutory body or regulatory authority, in connection with any breach of this obligation.

4.3 Notwithstanding and further to anything stated elsewhere in this Contract, NKF reserves the right and the Vendor agrees that NKF may conduct (or appoint a qualified, independent third party to conduct) an audit and/or assessment of the standard of compliance or non-compliance by the Vendor with the obligations under this Clause 4.

4.4 To the extent that the Vendor sub-contracts its obligations under this Contract to a sub-contractor, such sub-contracting shall be subject to NKF's prior written approval and the Vendor agrees and acknowledges that it shall ensure that this Clause 4 is incorporated into the sub-contractor's contract.

4.5 Subject to the foregoing, the Vendor's confidentiality obligations under this Clause 4 shall survive the expiry or termination of this Contract

Accepted By:

Authorized Signature: _____ Date: _____

Signatory Name: _____ Signatory Title: _____

Telephone Number: _____ Vendor's Name: _____

Email Address: _____ Vendor's Stamp: _____

ITQ REF NO: NKF/PL/2020/004
DATE: 9 MARCH 2020

ANNEX H

INFORMATION ABOUT VENDOR

ITQ REF NO. _____

ITQ FOR _____

1. Vendor's name: _____
2. Company/Business registration no.: _____
3. Registered address: _____

   _____
4. GST registration no. (if applicable): _____
5. Type of business (please select)

   ( ) Sole proprietorship ( ) Private company (limited by shares)

   ( ) Partnership ( ) Public company (limited by shares)

   ( ) Others (please specify): _____

   _____
6. Contact person

   Name: _____

   Title: _____

   Tel No.: _____

   Fax No.: _____

   Email: _____

7. **I declare that I/the Vendor is not related[1] to any person in NKF who is involved in this ITQ howsoever and whatsoever.**
8. The above named Vendor certifies and declares that all information, documents and materials provided in connection with its quotation bid are true and accurate to the best of its knowledge.

Authorised Signature: _____

Signatory's name: _____ Signatory's title: _____

Vendor's name: _____ Vendor's stamp:_____

[1]Related refers to the following: Spouse, domestic partner, child, mother, father, brother or sister or close associates; any corporation, business or non-profit organization of which you are serving as staff, officer, board member, partner, participate in management or are employed by; any trust or other estate in which you have a substantial interest or as to which you serve as a trustee or in a similar capacity.