Procedures in Submission and Opening of Electronic Bid

1. Upon submission of a duly filled-up LBP Secure File Transfer Facility (LBP SFTF) User Registration Form together with copies of LANDBANK Official Receipt and Payment Acceptance Order for non-refundable bidding fee to the HOBAC Secretariat, the prospective bidder shall receive an email with log-in credentials to access the LBP SFTF.

2. The electronic bid shall be submitted by uploading the same in the LBP SFTF (please refer to the Guide in Accessing LBP Secure File Transfer Facility below). *Electronic bids received after the set deadline basing on the date and time on the electronic folders of bidders shall not be accepted by the HOBAC*. Thus, bidders are requested to upload their electronic bids at least two (2) hours before the set deadline.

3. The electronic bid consisting of two copies/files shall be labelled with bidder's *assigned* short name, last seven (7) digits of the bidding reference number including the parenthesis if there are any, and bid copy number, each separated with a dash sign. Thus, for a project with bidding reference number LBPHOBAC-ITB-GS-20200819-01(2) that XYZ Company wants to bid on, the archived files shall be labelled as XYZ-081901(2)-C1 and XYZ-081901(2)-C2. The archived files shall be generated using either WinZip, 7-zip or WinRAR and password-protected.

   Each of the above mentioned archived files shall contain the Technical Component and Financial Component files. The PDF files shall be labelled as above plus the word "Tech" or "Fin" in the case of the Technical Component and Financial Component, respectively. Thus, using the above example, XYZ-081901(2)-C1 shall contain the PDF files labelled XYZ-081901(2)-C1-Tech and XYZ-081901(2)-C1-Fin while XYZ-081901(2)-C2 shall contain the PDF files labelled XYZ-081901(2)-C2-Tech and XYZ-081901(2)-C2-Fin.

   In case of modification of bid, the qualifier "Mod" and a numeric counter indicating the number of times that the bid had been modified shall be added at the end of the filenames of both the archived and PDF files [e.g. First Modification: XYZ-081901(2)-C1-Mod containing XYZ-081901(2)-C1-Tech-Mod and XYZ-081901(2)-C1-Fin-Mod and Second Modification: XYZ-081901(2)-C2-Mod1, containing XYZ-081901(2)-C2-Tech-Mod1 and XYZ-081901(2)-C2-Fin-Mod1].

   All the required documents for each component of the bid shall be in one (1) PDF file and sequentially arranged as indicated in the Checklist of Bidding Documents. The documents must be signed by the authorized signatory/ies when required in the form.

<u>Each of the archived files and the PDF files shall be assigned with a different password</u> and these passwords shall be disclosed by the bidder only upon the instruction of HOBAC during the actual bid opening.

Electronic bids that are not assembled, labelled and password-protected in accordance with these procedures shall not be rejected/disqualified but the Bidder or its duly authorized representative shall acknowledge such condition of the bid as submitted. The HOBAC/LANDBANK shall assume no responsibility for the non-opening or premature opening of the contents of the improperly assembled, labelled and password-protected electronic bid.

4. The prospective bidder shall receive an acknowledgement receipt via email *<u>after</u>* successful uploading of its/his electronic bid. If no email is received within one (1) hour after successful uploading, the bidder shall call the HOBAC Secretariat at (02) 8522- 0000 local 2609 to confirm whether the submission has been received, and if so, request for the acknowledgment of receipt of the electronic bid.

5. On the bid opening date, the bidder shall confirm its/his participation in the online meeting with the HOBAC Secretariat at least one (1) hour before the scheduled meeting. The bidder shall be able to log in into MS Teams and join the Waiting Room of the HOBAC meeting. Only one account/connection per participating bidder shall be allowed to join the meeting. If the bidder has more than one (1) representatives, the said representatives may take turns in using the allowed account/connection.

6. Projects with participating bidders in attendance shall be given priority in the queuing.

7. Upon the instruction of the HOBAC Chairperson to start the bid opening activity, the HOBAC Secretariat connects the participating bidder/s to the videoconferencing/group calling session. The HOBAC Secretariat shall record the session and act as Moderator of the meeting all throughout.

8. Once the connections are in place, the HOBAC, with the assistance of the HOBAC Secretariat, retrieves the archived file from the LBP SFTF and opens the same. The Technical Proposal shall be opened first. Upon instruction from the HOBAC, the bidder concerned shall disclose the passwords for the archived file and the PDF file of the Technical Component.

In case an archived/PDF file fails to open due to a wrong password, the specific bidder shall be allowed to provide the HOBAC with passwords up to five (5) times only. The same number of attempts shall apply to Copy 2 of the bid, in case there is a need to open it. If the archived/PDF file still could not be opened after the maximum allowable attempts, the bidder concerned shall be disqualified from further participating in the bidding process.

9. The HOBAC then determines the eligibility and compliance with the technical requirements of the specific bidder using a nondiscretionary "pass/fail" criterion. Only bidders that have been rated "Passed" shall be allowed to participate in the succeeding stages of the bidding process.

10. The HOBAC, with the assistance of the HOBAC Secretariat, shall then open the Financial Components of those bidders that have been rated "Passed". Upon instruction from the HOBAC, the bidder concerned shall disclose the password for its/his Financial Component.

11. The HOBAC, with the assistance of the HOBAC Secretariat, conducts bid evaluation and ranking of the bids. The results of bid evaluation and ranking shall be recorded in the Abstract of Bids, which shall be signed by the HOBAC Members and Observers. The result of evaluation and ranking shall also be announced to the participants.

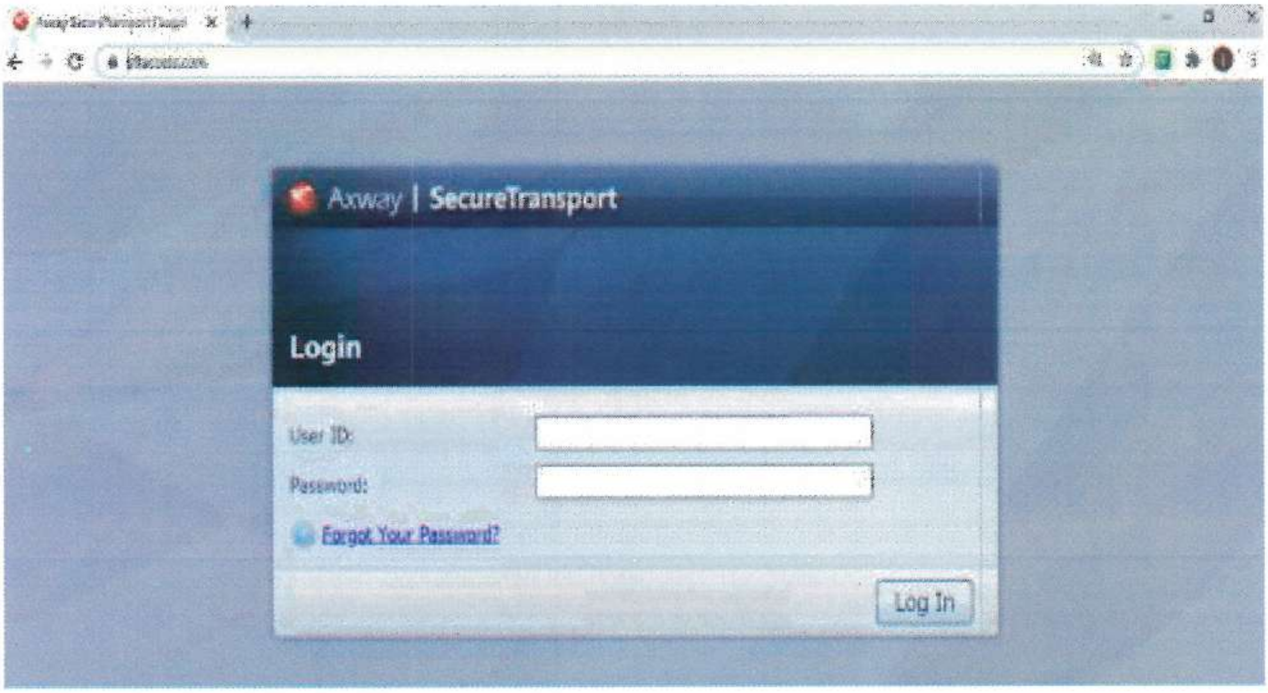
12. The retrieval and opening of the electronic bids, page-by-page review of documents and the results of the bid evaluation and ranking shall be shown to the participants through the screen sharing feature of MS Teams.

13. The access of the bidders to the videoconferencing/calling session shall be terminated once the Chairperson has declared that the bid opening activity for a specific project has been finished.

14. MS Teams Application shall be used in the conduct of online bidding. In the event that it is not available, other videoconferencing/group calling applications may be used as an alternative in conducting the meeting.

Guide in Accessing LBP Secure File Transfer Facility

1. Open browser and type the url: **https://www.sftaccess.com**



2. Log-in with the credentials provided via email. (Note: Log-in credentials will be received upon submission of a duly filled-up LBP SFTF User Registration Form together with copies of LANDBANK Official Receipt and Payment Acceptance Order for non-refundable bidding fee)

   Username: **[E-mail Address] e.g. bidder1@bidder.com**

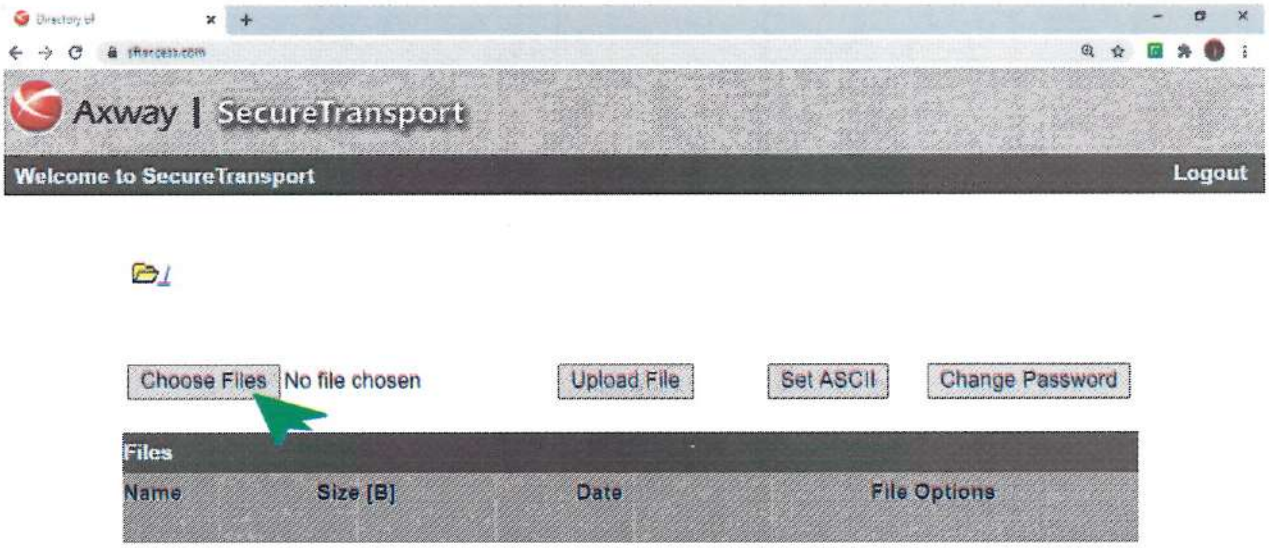
   Password: **[Landbank-provided password]**

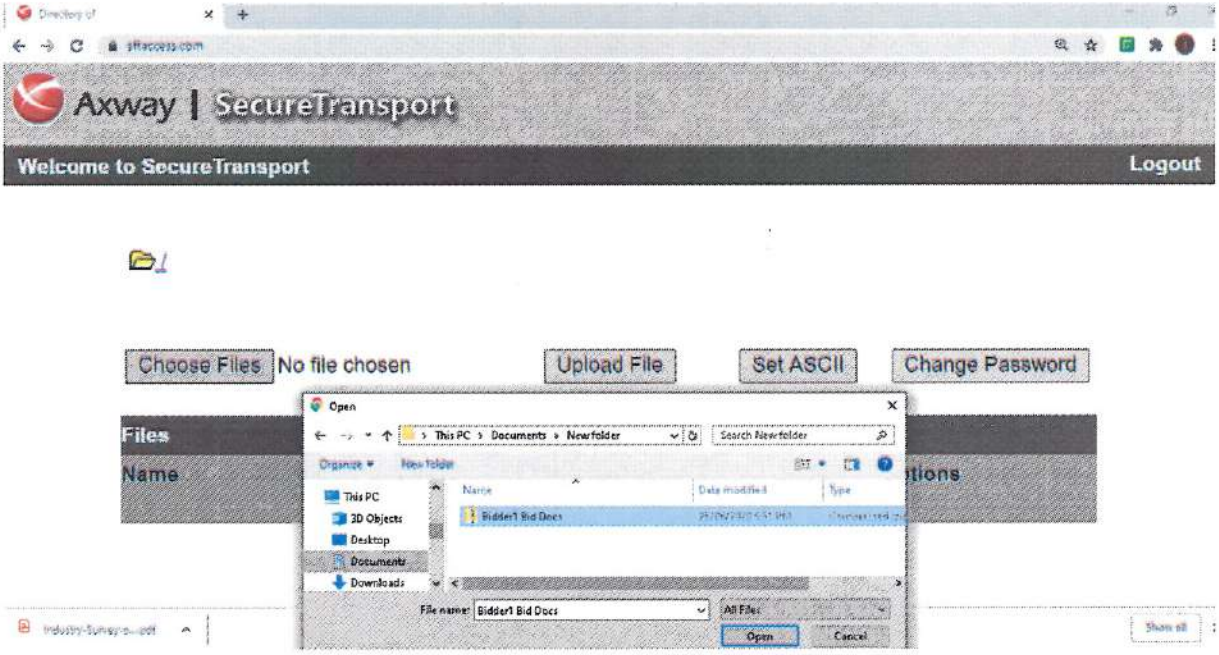
3. Upon successful login, click '**Choose Files**' to upload file/s.

Notes:

1. Files should be encrypted/password-protected.

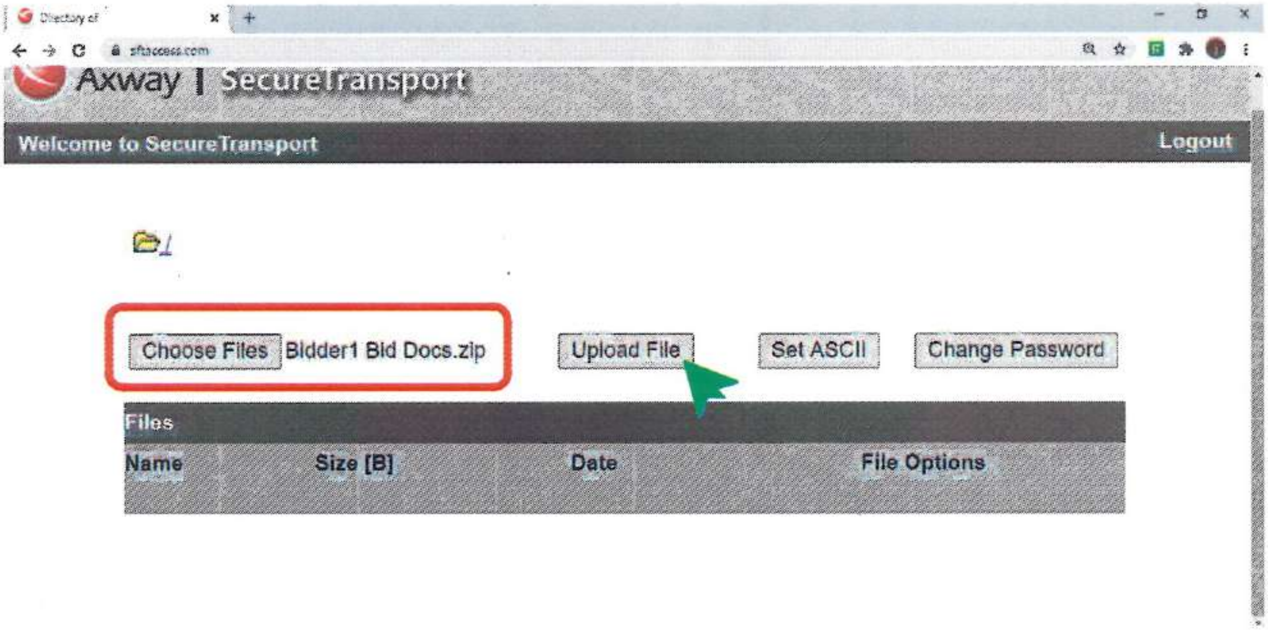
2. Please follow the instructions in Item 2 of the above Procedures in Submission and Opening of Electronic Bids.





Annex D -5

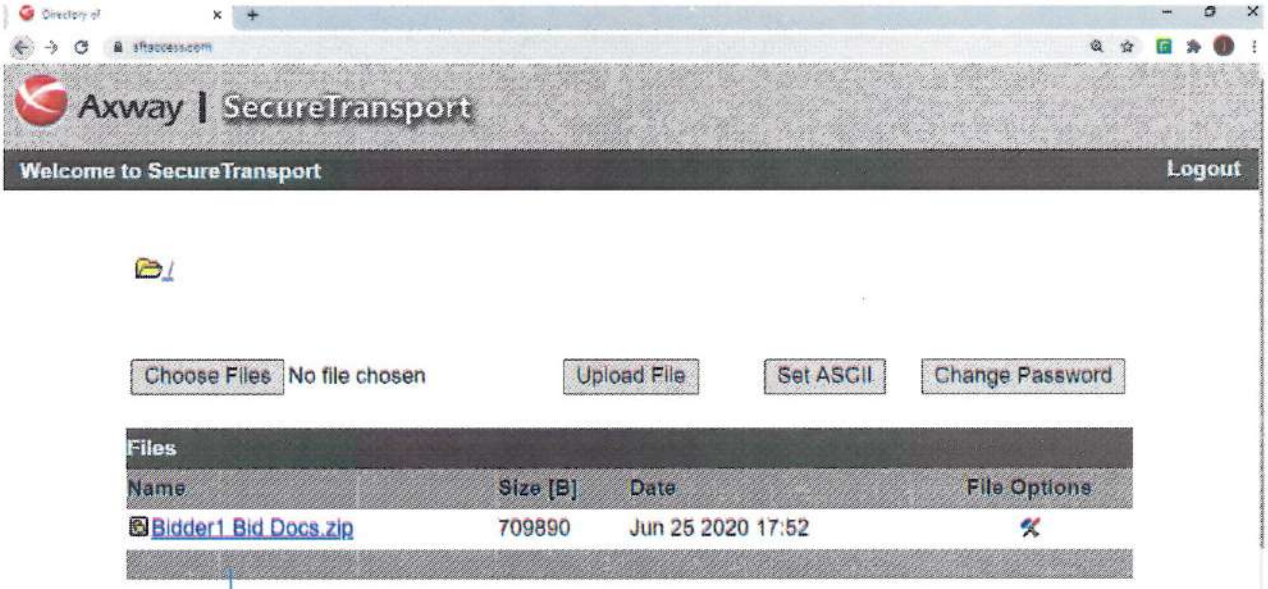
4. Click '**Upload File**' to upload the selected file/s.



Choose Files: Bidder1 Bid Docs.zip

Files			
Name	Size [B]	Date	File Options

5. Once a successful upload is completed, the files cannot be deleted anymore. The bidder will also receive a system-generated acknowledgement receipt in its registered e-mail address. A screenshot of the uploaded Bid/s should be taken by the bidder for record purposes.



Choose Files: No file chosen

Files			
Name	Size [B]	Date	File Options
Bidder1 Bid Docs.zip	709890	Jun 25 2020 17:52	

Successful upload

Annex D -6

File Repository of Bid Documents

All uploaded bid documents will be stored in the dedicated SFTF directory of a particular bidder and will be accessible by the assigned ProcD personnel.

No revisions as of September 08, 2020

LBP SECURE FILE TRANSFER FACILITY
REGISTRATION FORM

Name of Participating Bidder/"Company"		
Complete Address of the Company:		**Contact Number/s:**
AUTHORIZED LBP SECURE FILE TRANSFER USER/S:		
Name of Authorized Representative:	**Official Email Address:**	**Contact Number/s:**

TERMS AND CONDITIONS:

The Company, through its Authorized User/s, shall:

1. Use LBP's Secure File Transfer Facility to securely transmit files to LBP Procurement Department only for the purpose of online submission of bidding documents.

2. Be responsible for the confidentiality of its assigned log-in credentials. (i.e. assigned user ID)

3. Only upload agreed upon file formats and shall not upload any file/s containing inappropriate content, material that violates or infringes in any manner on the intellectual or proprietary rights of others, and any malwares, software virus, "Trojan Horse" program, "worm" or other harmful or damaging software or software component.

4. Agree and ensure that the computing devices to be used for LBP's Secure File Transfer Facility have the updated anti-virus software and operating system security patches, as minimum requirements in order to establish connectivity, to maintain and ensure the security, integrity and availability of the LBP Secure File Transfer Facility.

5. Agree not to use a public wi-fi/hotspot such as but not limited to those offered in coffee shops, malls, restaurant or hotels to access into the LBP Secure File Transfer Facility.

6. Agree that LANDBANK may revoke, block, or permanently disallow the use of this facility without prior notice due to reasons that may compromise the Bank's security.

AGREEMENT:

As an Authorized User, I hereby agree:

To the above terms and conditions
Not to disclose any confidential information regarding the LBP Secure File Transfer Facility.
To avoid using unauthorized users/computers to input credentials; and
That unauthorized dissemination of information about the LBP Secure File transfer Facility shall be considered a security breach and is ground for the immediate termination of the account.

____
Authorized User
(Signature over Printed Name)

Please print N/A in blank spaces

Annex F

Supply, Delivery, Installation and Configuration of Privileged Access Management (PAM) Solution with Hardware Appliance *Term of Reference*

Item	Description	Trends Inquiries/Remarks	LBP Response
Hardware Infrastructure Requirements			
1	**3 units (2 in HO and 1 in DR) Gateway Servers with minimum specs of the following:** - Single CPU with atleast 8Core, 3Ghz/11M Cache -16Gb Memory -5 x 600Gb SAS Hard Drives, RAID 1 + RAID 5 -Management Controller -Dual 1GbE Network Interface Card -Red Hat Operating System, 3Yrs Premium Subscription -Dual Power Supply -Rack Railing Kit -3Yrs Hardware and Software Warranty	Instead of proposping a 3rd party servers for PAM solution, can we propose a hardend and purpose built appliance of our solution? With our solution, we can only provide 4 x Server (2 x PAM Sever, 2 x Gateway Server) which will help LBP on the footprint for rack space, powe consumption and appliance management.	Scalability and flexibility will be the advantage of using HCI.
2	**2 units (1 in HO and 1 in DR) Application Servers with minimum specs of the following:** -Single CPU with atleast 12Core, 2.7Ghz/19.25M Cache -32Gb Memory -5 x 600Gb SAS Hard Drives, RAID 1 + RAID 5 -Management Controller -Dual 1GbE Network Interface Card -Windows Server Operating System -Management Controller -Dual 1GbE Network Interface Card -Windows Server Operating System -Dual Power Supply -Rack Railing Kit -3Yrs Hardware and Software Warranty		
3	**2 units (1 in HO and 1 in DR) Database Servers with minimum specs of the following:** -Single CPU with atleast 8Core, 3Ghz/11M Cache -32Gb Memory -2x 600Gb SAS Hard Drives, RAID 1 for OS -8 x 1.8Tb SAS Hard Drives, RAID 5 fot Data -Management Controller -Dual 1GbE Network Interface Card -Windows Server Operating System -Windows SQL Server Database License -Dual Power Supply -Rack Railing Kit -3Yrs Hardware and Software Warranty		
Single - Sign On and Authentication Models			
4	**The solution should be able to create seamless single sign-on for** a. Microsoft Windows 2003/2008/2013/2012/2016 b. AIX		

	c. Redhat Linux d. Unix Systems e. Solaris Systems f. Oracle g. MS SQL Server / DB2 / MYSQL h. Network Devices (e.g. Router, Switches, etc)) i. Security Devices (e.g. Firewalls, IPS, etc) i. Generic Target System Connectors		
5	The solution should be agentless in nature		
6	The solution should support transparent connection to the target device, without seeing the password or typing it in as part of the connection		
7	The solution should support direct connections to windows, ssh, databases and other managed devices without having to use a jump server		
8	The solution shall also include an option of biometric based authentication and/or hardware-less strong authentication (eg Mobile OTP). Further the solution should be able to integrate out of the box with leading dual factor authentication products.		
9	The solution should have an inbuilt dual factor authentication for soft token, mobile OTP etc. Also it should have an inbuilt authentication for Bio-Metrics without having to acquire another biometric authentication server.	Since LBP is using RSA MFA, can we just use your existing MFA solution to integrate with our PAM Solution	No. Since it is part of the appliance/license, LBP can use this inbuilt OTP even without the RSA 2FA.
10	The solution shall also include an option of hardware-based tokens. Further the solution should be able to integrate out of the box with leading dual factor authentication products.	Since LBP is using RSA MFA, can we just use your existing MFA solution to integrate with our PAM Solution	Yes. Can use the existing RSA for integration
11	The solution should be able to integrate with enterprise authentication methods e.g. multiple 3rd party authentication methods including LDAP, RADIUS and a built-in authentication mechanism		
12	The solution should also provide local authentication and all the security features as per best standards		
13	The solution should provide flexibility user/device wise for local authentication or enterprise authentication		
14	The solution should support an application integration framework for web based as well as .exe based applications. There should be strong out of the box support including ease of integration with any third party connectors.		
15	The solution should provide multi-tenancy feature whereby the entire operations can be carried out within a tenant or line of business.	Instead of having a multi-tenancy requirement which is applicable for service provider, can we provide workspaces that allow logical separation based on	This is for a creation of business unit for segregation of duties per group delegated admin

		department, group or organization?	
16	The solution should provide multi-domain feature whereby the entire operations can operate in an distributed environment		
17	The solution can restrict end-user entitlements to target accounts by location; that is, allow access only from a specified PC or range or class of PCs.		
18	The solution should provide an inbuilt PCI-DSS compliant MFA tool/solution	Since LBP is using RSA MFA, can we just use your existing MFA solution to integrate with our PAM Solution	Yes. Since RSA is PCI-DSS compliant
19	Ability to allow self-registration of MFA solution for authenticating user	Since LBP is using RSA MFA, can we just use your existing MFA solution to integrate with BeyondTrust?	Yes.
20	The solution should be able to handle multi-location architecture or distributed architecture with seamless integration at the User Level. For example: Multiple datacenter can be handled with just one installation.		
Shared Account Password Management			
21	The solution shall perform password change options which is parameter driven		
22	The solution should set password options every x days, months, years and compliance options via the use of a policy		
23	Ability to create exception policies for selected systems, applications and devices		
24	The solution should enable an administrator to define different password formation rules for target accounts on different target systems and supports the full character set that can be used for passwords on each target system.		
25	The solution enables an administrator to change a target-account password to a random value based on a manual trigger or automatic schedule.		
26	Allow single baseline policy across all systems, applications and devices (eg one single update to enforce baseline policy		
27	The solution should support changing a password or group of passwords according to a policy (time based or 'on-demand')		
28	Ability to generate 'One-time' passwords as an optional workflow	Since LBP is using RSA MFA, can we just use your existing MFA solution to integrate with our PAM Solution	No. Since it is an inbuilt OTP.
29	Ability to send notifications via email or other delivery methods triggered by any type of activity		

30	Ability to send notification via email to the user requesting the password that checkout is complete		
31	Flexibility that allows exclusivity for password retrieval or multiple users checking out the same password for the same device in the same time period.		
32	The solution generates an alert if the password change fails after an administrator-specified number of retries.		
33	The solution should identify pending password changes to any target system that was unavailable at the time the change was initiated		
34	All locally stored target-account passwords should encrypted using AES or similar encryption with at least 256 bit keys.		
35	The solution should automatically reconcile passwords that are detected 'out of sync' or lost without using external restore utilities		
36	The solution should have the ability to reconcile passwords manually, upon demand		
37	The solution should automatically verify , notify and report all passwords which are not in sync with PIM		
38	The solution should have the ability to automatically "check-out" after a specific time and "check-in" within a specified time.		
39	The solution should set unique random value anytime a password is changed. The password generated should be strong and should not generate a similar value for a long iteration.		
40	The tool allows secure printing of passwords in Pin Mailers. Lifecycle of printing and labelling of envelopes should be part of the module.	This will add a large overhead on PAM Administrator to manage frequent password rotation, printing and secure storage. Can we just do the password rotation in the system automatically which don't need printing of password?	No. This is for a breakglass scenario, if PAM goes down this will be the alternative way to obtain credentials of target systems. For password vaulting.
41	The solution should be able to control re-prints with adequate authorization	This will add a large overhead on PAM Administrator to manage frequent password rotation, printing and secure storage. Can we just do the password rotation in the system automatically which don't need printing of password?	Same as above
42	Secured platform - main password storage repository should be highly secured (built-in firewall, hardened machine, limited and controlled remote access etc.)		
43	The proposed solution should restrict the solution administrators from accessing or viewing passwords or approve password		

	requests		
44	The solution should have the capability to seamlessly change the passwords for the large number of desktops.		
45	Ability to manage privileged passwords for multi-lingual servers		
46	Provision to prompt for a password change immediately after onboarding/vaulting a privileged account		
47	Provision to configure/define custom commands for password change without OEM's intervention.		
Access Control			
48	The solution should be able to restrict usage of critical commands over a SSH based console based on any combination of target account, group or target system and end-user.		
49	The solution should restrict privileged activities on a windows server (e.g. host to host jumps, cmd/telnet access, application access, tab restrictions) from session initiated with PIM		
50	The solution should be able to restrict usage of critical commands on command line through SSH clients on any combination of target account, group or target system and end-user.		
51	The solution should be able to restrict usage of critical commands on tables for database access through SSH, SQL+(client/), front-end database utilities on any combination of target account, group or target system and end-user.	Instead of block listing for the critical commands. Can we approach to have DB accounts with least privilege/need to know basis/whitelisting? The administrator should have access and privilege only to accounts that allows him/her to perform her task.	No. Restriction of critical command even to an administrator access is to prevent unnecessary execution, deletion and alteration of critical command in the target system.
52	The solution enables an administrator to restrict a group of commands using a library and define custom commands for any combination of target account, group or target system and end user.		
53	The solution should provide secure mechanism for blacklisting/whitelisting of commands for any combination of target account, group or target system and end user.		
54	The solution can restrict user-specific entitlements of administrators individually or by group or role.		
55	The solution should have worklfow control built-in for critical administrative functions over SSH including databases (example user creation, password change etc) and should be able to request for approval on the fly for those commands which are critical.	Instead of block listing for the critical commands. Can we approach to have DB accounts with least privilege/need to know basis/whitelisting? The administrator should have	No. Since Execution of critical command is restricted. An administrator or a user must have to go to an approval process before executing.

		access and privilege only to accounts that allows him/her to perform her task.	
56	The solution can restrict target-account-specific entitlements of end users individually or by group or role.		
57	The solution can restrict end-user entitlements to target accounts through a workflow by days and times of day including critical command that can be fired.		
58	System should be able to define critical commands for alerting & monitoring purpose and also ensure user confirmation (YES or NO) for critical commands over SSH.	This is an end point functionality. Can we approach that account should have least privilege setup for the required job function to limit their command to use?	No. This feature will notify and alert SOC team if someone is running unauthorized execution or process of the target system.
Privileged Session Management and Log Management			
59	The solution should be able to support any session recording on any session initiated via PIM solution including servers, network devices, databases and virtualized environments.		
60	The solution should be able to **log commands** for all commands fired over SSH Session and for database access through ssh, sql+		
61	The solution should be able to log/search text commands for all sessions of database even through the third party utilities		
62	The solution should be able to log/search text commands for all sessions on RDP		
63	The solutions should support selective option for enabling session based recording on any combination of target account, group or target system and end-user.		
64	All logs created by the solution should be tamper proof and should have legal hold		
65	The solution logs all administrator and end-user activity, including successful and failed access attempts and associated session data (date, time, IP address. Machine address, BIOS No and so on). The tool can generate — on-demand or according to an administrator-defined schedule — reports showing user activity filtered by an administrator, end user or user group.		
66	The tool can restrict access to different reports by administrator, group or role.		
67	The tool generates reports in at least the following formats: HTML, CSV and PDF		
68	System should be able to define critical commands for alerting & monitoring purpose through SMS or Email alerts		
69	The solution should provide separate logs for commands and session recordings. Session recordings should be available in image/ video based formats		
70	The session recording should be SMART to		

	help jump to the right session through the text logs		
71	Secure and tamper-proof storage for audit records, policies, entitlements, privileged credentials, recordings etc.		
72	The proposed solution shall cater for live monitoring of sessions and manual termination of sessions when necessary		
73	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.	Instead of excluding SQL commands to log, can we consider logging ALL commands which will align on audit compliance	This will prevent execution of prohibited commands that might cause unnecessary activities on the target systems.
74	The proposed solution shall enable users to connect securely to remote machines through the tool from their own workstations using all types of accounts, including accounts that are not managed by the privileged account management solution.		
75	The proposed solution shall allow configuration at platform level to allow selective recording of specific device.		
76	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).		
77	The proposed solution shall support correlated and unified auditing for shared and privileged account management and activity.		
78	The proposed system shall support full colour and resolution video recording.		
79	The proposed system shall support video session compression with no impact on video quality.		
80	Ability to capture text logs for all privileged sessions		
81	Ability to perform text based search on video logs		
82	Ability to identify direct access to managed devices (bypass PAM) and alert/block access	Instead of the PAM solution, can we use your SIEM and FW to Alert/block direct access to managed devices? Implementation will require all access to managed devices will be through our PAM Solution	This will monitor if someone is trying to bypass the PAM
PIM Security			
83	The solutions should use minimum FIPS 140-2 validated cryptography for all data encryption.		
84	All communication between system components, including components residing on the same server should be encrypted.		
85	All communication between the client PC and the target server should be completely		

AMMF F-7

	encrypted using secured gateway. (Example: a telnet session is encrypted from the client PC through the secured gateway)		
86	The Administrator user cannot see the data (passwords) that are controlled by the solution.		
87	Secured platform - main password storage repository/Vault should be highly secured (hardened machine, limited and controlled remote access etc.).		
88	The solution should secure master data, records, entitlement, policy data and other credentials in tamper proof storage container.		
PIM Administration			
89	The solution should have central administration web based console for unified administration.		
90	The tool uses Active Directory/LDAP as an identity store for administrators and end users.		
91	The tool enables an administrator to define groups (or similar container objects) of administrators and end users.		
92	The tool enables an administrator to add an administrator or end user to more than one group or to add a group to more than one supergroup.		
93	The tool enables an administrator to define a hierarchy of roles without limit.	Since you have an IAM solution, can we just use your existing IAM since this can be done through IAM?	As long as the proposed solution has an integration with the bank IAM
94	Administrative configurations (e.g. configuration of user matrix) shall be accessible via a separate client where client access is controlled by IP address.		
95	Important configuration changes in the solutions (example changes to masters) should be based on at least 5 level workflow approval process and logged accordingly	Can we support parallel approval as an other of option for multiple level of approvers / hierarchy?	
96	Segregation of Duties - The Administrator user cannot view the data (passwords) that are controlled by other teams/working groups (UNIX, Oracle etc.).		
97	All administrative task should be done LOB wise i.e. Line of Business Wise		
98	Provision for User Creation approval/rejection via E-mail	Since you have an IAM solution, can we just integrate our PAM solution with your IAM to have a singel point of truth for user creation and approval?	As long as the proposed solution has an integration with the bank IAM
99	Provision for User self-registration in PAM	Since you have an IAM solution, can we just integrate our PAM solution with your IAM since the user can self-register in IAM and can be provisioned to	As long as the proposed solution has an integration with the bank IAM

		BeyondTrust.	
100	Provision for bulk operation for management of devices inside PAM		
101	Provision for scheduling user access review inside PAM		
System Architecture			
102	The solution architecture should be highly scalable.		
103	The proposed solution shall provide multi-tier architecture where the database and application level is separated.	Can we proposed or recommend a hardened and purpose build PAM Appliance for ease of use & security.	
104	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.		
105	The proposed solution shall have the ability to support multiple mirrored systems at offsite Disaster Recovery Facilities across different data centre locations.		
106	The proposed solution shall have built-in options for backup or integration with existing backup solutions		
107	The proposed solution shall handle loss of connectivity to the centralized password management solution automatically.		
108	The proposed solution shall not require any network topology changes in order to ensure all privileged sessions are controlled by the solution.		
109	The proposed solution shall support distributed network architecture where different segments need to be supported from a central location.		
110	The proposed solution shall support both client based (in the case where browser is not available) as well as browser based administration	Instead of the solution to support client-base AND browser-base, can we just require supporting any of the two (client-base OR browser-base)	
111	The proposed solution should be 100% agentless that includes password storage, password management and session recording features.		
112	The solution must support parallel execution of password resets for multiple concurrent requests.		
113	The solution should provide fully automatic failover from a single active instance to a backup/standby instance with a fully replicated repository		
114	The solution should support multiple active instances with load balancing and fully automatic failover to another active instance	BeyondTrust supports multi-site Active-active deployments. For the load balancing, can we use	No. unless there is a separate load balancer for this.

		your load balancer solution (F5)?	
115	The solution provides automatic detection of failure of the single/multiple active instance(s), and fully automatic failover to a backup/standby instance on a DR site.	BeyondTrust supports to failure detection in Active-Passive set-up. The passive instance detects failure of the active instance and promotes itself to active .Or can we use your load balance solution for this?	Capability to monitor if primary site is down and automatic failover to DR
116	The solution if required should be available to install on a virtual sever		
117	The system should be highly available (24x7x365) and redundant from a hardware failure, application failure, data failure, and or catastrophic failure. Please elaborate		
118	The solution should have an ability to have direct connection to target device as well as using secured gateway channel		
119	Provision to deploy the solution on-premise, cloud or hybrid environment.		
120	Ability to run multiple PAM instances locally in case of connectivity failure (for multi-site setup)		
121	Zero downtime for performing upgrades/planned activities	May require scheduled downtime for certain upgrades.	Since it is HA with Active Passive mode
Out of box Integration			
122	Ability to integrate with enterprise authentication methods e.g. multiple 3rd party authentication methods including AD, LDAP, Windows SSO, PKI, RADIUS and a built-in authentication mechanism.		
123	Ability to integrate with Bio-Metric Solutions	Can we use your RADIUS Server? This can be achieve through BeyondTrust integration with your RADIUS Server	
124	Ability to integrate with Hard and Soft token solutions		
125	Ability to integrate with ticketing systems.		
126	Ability to integrate with Automation softwares for enhancing productivity in the data center		
127	The proposed solution supports integration with the Hardware Security Module (HSM) devices to store the encryption keys.		
Ticketing System integration			
128	The solution can force the requestor of password / session to provide a reason, including a service desk incident ticket number, for the request.		
129	The solution can communicate with a workflow engine to verify an incident ticket number cited in the end user's request.		
130	The solution provides the capability to		

	enable end users to retrieve (or reset) a target-system password only after approval by a designated approver (to allow dual control). Approval criteria can be based on any combination of target account, group or target system and end-user identity, group or role, as well as contextual information such as day of the week or time of day.		
131	Ability to enforce ticketing integration as well as approval workflow for specific ticket types (e.g. change/incident ticket)		
132	Inbuilt ticketing system with 5 level workflow approval with ticket level validation, risk and impact assessments as per LOB wise, Service type and user type. This ticketing system to help in creating a work order on an executer, who will then request for the access through the request workflow with this valid ticket	Since LBP is using CA for the Ticketing system, can we levereage your existing Ticketing system solution to integrate with our PAM solution so LBP will be having a single/centralized ticket system to used?	
SIEM Integration			
133	The solution should be able to integrate with the bank SIEM and other leading SIEM Solutions.		
134	The solution should be able to integrated with applications like VA Systems, performance monitoring applications to eliminate hard coded passwords		
Application Password Management (Hard-Coded Password Management)			
135	The solution should have an ability to eliminate, manage and protect privileged credentials in applications, scripts, configuration files etc.		
136	The solution should be able to authenticate and trust the application requesting the privileged password based on various authentication methods		
137	Application Servers Support - The product should support removing static hard coded passwords from Data Sources in Application Servers. Please elaborate.		
Auto Discovery of Privileged Accounts			
138	The solution should be able to perform auto discovery of privileged accounts on target systems and perform two way reconciliation.		
139	The solution should provide feature for user governance on the target devices i.e autodetect users and schedule a governance workflow and user certification process with adequate review process.		
140	Ability to easily discover and flag accounts that do not adhere to the corporate password policy without having to implement a PAS solution		
141	Map privileged and personal accounts on various target systems		
142	Ability to quickly identify all non-built-in local administrator accounts in your environment (flag possible 'backdoor' accounts)		

143	Ability to quickly identify private and public SSH keys, including orphaned SSH keys, on Unix/Linux machines, extracts key related data and ascertain the status of each key.	Instead of extracting the SSH keys which can easily be copied. Can we just identify the accounts/user/admin using SSH key authentication and let the PAM solution manage these keys.	
Notification Engine			
144	The solution should have capability to provide alerts and notification for critical PIM events over SMS & Email		
145	The solution should have capability to provide alerts and notification for all administration/configuration activities over SMS & Email		
146	Customizable notification for command executed on SSH and Telnet based devices		
147	Customizable notification for command/Process executed on Windows	This is an end point functionality.Instead of the notification, we can have least privilege setup for the required job function and to limit any command/process execution.	This is for the command restriction alerts and notification if someone is trying to execute a command on a target system without authorization.
148	Notification on target being access on criteria like Line of Business or Groups		
Solution Workflow			
149	The solution should have inbuilt workflow to manage a. Electronic Approval based Password Retrieval b. Onetime access / Time Based / Permanent Access c. 5 level approval workflow with E-mail and SMS notification with delegation rules	Instead of workflow approval like:(1) Electronic approval-based Password Retrieval(2) Onetime access/ Time Based / Permanent Access(3) 5 level approval workflow with E-mail and SMS notification with delegation rules can we also consider(1) Onetime access/ Time Based / Permanent Access(2) Location Base(3) Parallel approval	
150	Ability to provide for delegation at all levels in the workflow	Instead of delegation, can we support parallel approval, where a single or two approval suffice	
151	Mobile device support - ability to send a request to access a password, approve the request and retrieve the password, all from a hand-held mobile device e.g. smart phones		
152	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).	Instead of multiple level of approvers / hierarchy approval can we also support parallel approval?	
153	Supports a workflow approval process that requires approvers to be in sequence before final approval is granted.	Instead of multiple level of approvers / hierarchy approval can we also support parallel approval?	

154	Ability to log workflow processes and/or have the ability to be reported or audited.		
Dashboard & Reporting			
155	Dashboard Capabilities should included real-time view of activities performed by the administrators		
156	The system shall have the ability to run all reports by frequency, on-demand and schedule.		
157	The solution should provide detailed and scheduled reporting with the following basic report sets Entitlements Reports, User's activities, Privileged Accounts inventory and Activities log		
158	The solution should have ability to report on all system administrative changes performed by PIM Administrators with relevant auditable records		
159	The solution should be able to report password lockouts (failure logon attempts)		
160	Ability to report password checkouts on systems and users requesting passwords		
161	Ability to report password lockouts (failure logon attempts)		
162	Ability to report on password change following verification process		
163	Ability to report on password status		
164	Reports should be customizable		
165	Audit data can be exported for use for any BI Tool		
166	Reports shall be automatically distributed by email		
167	Access to audit reports (and report configuration) shall be restricted to "auditor" end-users		
168	Ability to replay actual session recordings for forensic analysis		
169	Dashboard - for at a glance critical events and password policies.		
Risk & Threat Assessment			
170	Ability to analyze user behavior and predict unusual activity inside PAM		
End-Point Privilege Management			
171	Ability to manage passwords of privileged accounts on user workstations		
172	Ability to facilitate remote access of workstations with administrative rights to system administrators locally (over LAN) as well as over the internet		
Additional Features			
173	PAM Users to have a personal vault for secure storage of confidential files	Our PAM solution can just integrate with LBP's existing file vault or similar solution.	This will serves as users vault where users can hide their sensitive files or confidential information instead of storing to file folder of workstation.
174	Provision to select file types that a PAM user		

	can secure using the personal vault		
175	Configurable automatic deletion of files inside personal vaults after a specified period		
176	Ability to share files uploaded in personal vault with other PAM users		
177	Ability to authenticate Linux/Unix servers against Windows Active Directory (AD Bridging)		
178	The solution should provide multi-browser support		
179	The solution should bundle utilties for easy access to target devices incase of absence of native clients	Instead of using bundle utilities that might have an issue with vulnerability and compatibility on your managed devices, it's recommended to us the native client that LBP is currently using since it has patches and compatibility to access their managed device	This is in case of the absence of thick client sysytem such as putty, it is an alternative way to access the system/devices. So the users don't need to download such client.
180	The solution must support integration with target devices for Single Sign On (SSO) using native client (e.g. NMS, IAM)		
Supplier's Eligibility Requirements			
181	The supplier must be at least five (5) Years of existence in the IT Industry. Information should be based from SEC (Security and Exchange Commission) incorporation information, that the vendor is at least five (5) years. The bidder must submit a notarize certification from them with reference to SEC documents.		
182	The supplier must be an authorized reseller or distributor of the brand being offered. Must submit certification from distributor or principal.		
183	The principall represented by the supplier must have a local Technical manager or Information Technology (IT) support engineers to support the installations, configurations and 24x7 uptime services within the warranty period. Must submit Certificate of employment and Resume/Curriculum Vitae (that the local IT support engineers has at-least 5 years work experience in handling of the product being offered or other related security devices, include list of trainings and seminars attended)		
184	Three (3) years warranty on hardware and software. Warranty shall also cover any reconfiguration/integration after successful implementation. (The warranty certificate will be submitted by the winning bidder)		
185	The supplier must have a local helpdesk to provide 24x7 technical assistance. Must provide detailed escalation procedure and support including contact numbers and email		

	addresses.		
186	The supplier must have a dedicated Project Manager (PM) to oversee the project. Must submit Certificate of Employment and Resume/Curriculum Vitae (that the PM has at-least 5 years work experience and handled at least One (1) Commercial or Universal bank and one (1) non-bank clients as proof of his/her experience on how to handle projects.)		
187	The supplier must have at-least three (3) installed base of same solution or complex technology like Application Programming Interface (API) Management, Security Information and Event Management (SIEM) wherein one (1) is a Universal or Commercial Philippine Bank. Must submit list of installed base with client name, contact person, address, telephone number and email address.		
Delivery Terms and Condition			
188	Delivery after receipt of NTP: 60 calendar days		
189	Installation will start 7 calendar days after delivery and will end 90 calendar days after.		

One Commerce Clarification		**LBP Response**
It was mentioned not to use a jump server. Can we explain what is the purpose of Gateway server?	*Terms of Reference PAMS TOR A-2, Item no. 7, A-7 Item no. 144, 145, A-8 Item no. 144, 149*	*We want to eliminate the direct port connection from user workstation to the managed assets (as much as possible) and therefore we are looking for a gateway-based solution. In addition, this will also eliminate additional sources (Server and license) when there is a need to increase number of users.*
Except for built-in MFA, can we propose 3rd party MFA to compy?	*Terms of Reference PAMS TOR, A-2, Item no. 8, 9, 10, 1*	*The solution must be able to integrate to the bank's existing 2FA. However, due to a limited license, inbuilt OTP of the PAM solution will be utilize in compliance with PCIDSS without additional cost.*
Is there other tenants residing in Landbank premise?	*Terms of Reference PAMS TOR, A-2, Item no. 15.*	*We wish to implement a solution that supports multi-tenancy for future requirements. Should there be companies that will be bought by the bank, this will enable us to manage their devices by integrate them in the PAM solution.*
Our understanding here is that once the MFA tool is up, PAM will automatically detect it (without integration) and the PAM user can use it on the fly. Kindly verify if our mentioned use case is correct, or explain your use case here	*Terms of Reference PAMS TOR, A-2, Item no. 19.*	*This is for PAM's in-built MFA tool. PAM Admin should be able to enable it for a user and the user should be able to complete MFA registration by themselves. Kindly elaborate how does the enabling process for in-built MFA for a user works in the proposed solution.*
Kindly further explain the use case or a scenario for this item.	*Terms of Reference PAMS TOR, A-3, Item no. 38.*	*This requirement is for automatic 'check-out' and 'check-in' of privileged passwords managed by PAM. For e.g. if a user is requesting password*

		checkout for a specific time for a specific duration.
CyberArk uses digital vault to securely keep accounts passwords and keys. Could you explain the use case for printing the password to Pin Mail?	*Terms of Reference PAMS TOR, A-3, Item no. 40.*	*This is for generating hard/printed copies of managed privileged passwords in form of pin mailers for secure (encrypted) forms for a break glass scenario and access backup, if all the PAM goes down this will be the alternative way to obtain credentials of target systems.*
Would like to verify if we can comply for just supporting English server or you have multi-language servers?	*Terms of Reference PAMS TOR, A-3, Item no. 45.*	*Bank wishes to implement a solution that supports multi-lingual servers for future requirements.*
Kindly further explain the use case or a scenario for this item.	*Terms of Reference PAMS TOR, A-3, Item no. 47.*	*This is to understand whether the password change operation/process bundled in the proposed solution has the provision to be modified by the Bank without requiring the proposed solution's OEM's intervention.*
Can we comply by just using an email notification?	*Terms of Reference PAMS TOR, A-4, Item no. 68.*	*The SMS is to immediately notify security administrators or SOC team that if someone might try to run a command that might be critical to the system or if someone is trying to run unauthorized access or execution to the target systems.*
CyberArk captures all the commands executed by the users during its session for security reason. Kindy further explain our use case for this item.	*Terms of Reference PAMS TOR, A-4, Item no. 73.*	*This will prevent execution of prohibited commands that might cause unnecessary activities on the target systems. Also, On certain medium or low critical Database assets, Bank may wish to log only critical SQL commands or exclude non-critical*

		commands from being logged. The Bank is looking for a solution that offers this flexibility in logging policies.
It can be done by the legacy system of CyberArk. However, we do not practice it anymore. Bypassing a PAM or its jump server will avoid the user session monitoring which pose a security risk. Else,kindly help explain our use case for this item.	*Terms of Reference PAMS TOR, A-5, Item no. 74.*	*This is to allow Bank to implement either Single Sign On and Session Recording both for a given asset or only implement Session Recording and let the user enter their own credentials. PAM solution should NOT be bypassed in any scenario*
In CyberArk, user creation who will use the PAM can only be done by CyberArk Administrator.This is to limit the access the PAM with authorized users. We can do integration with Identity Access Management (IAM) to automate the user enrollment toCyberArk. Kindly help to explain our use case for this item.	*Terms of Reference PAMS TOR, A-5, Item no. 99.*	*The Bank is looking for a solution that has the provision to allow a privileged user to self-register into PAM to reduce the administrative overhead of user onboarding. A self-registration request has to go through an approval before successful onboarding. IAM integration will not be helpful for 3rd party administrators requiring temporary access.*
Our understanding here is that the PAM solution can switch with redundant centralized password management. Kindly help if our understanding is correct or explain your use case for this item.	*Terms of Reference PAMS TOR, A-6, Item no. 107.*	*The capabilities should include auto-reconnect and ability to switch to redundant centralized password management in case of auto-reconnect failure without affecting the operations or requiring human intervention.*
It can be done by the legacy system of CyberArk. However, we do not practice it anymore. Bypassing a PAM or its jump server will avoid the user session monitoring which pose a security risk. Else,kindly help explain our use case for this item.	*Terms of Reference PAMS TOR, A-6 Item no. 118.*	*This is to have privileged connections established either using an intermediary gateway or directly to the target asset. PAM solution should NOT be bypassed in any scenario.*
Kindly define the Automation	*Terms of Reference PAMS TOR,*	*The bank are in the process*

software mentioned here.	*A-6 Item no. 126.*	*of acquiring automated backup and recovery solution that also does task automation. The solution should be able to integrate to such solution as we continue to automate most of our data center processes.*
Kindly further explain the use case or a scenario for this item.	*Terms of Reference PAMS TOR, A-7 Item no. 139.*	*This is for user governance on a managed asset (user discovery). A newly identified account should undergo a review process automatically triggered by PAM.*