#	Specifications	Compliance (Yes / No)
A	**Single - Sign On and Authentication Models**	
1	The solution should be able to create seamless single sign-on for various technologies such as Operating Systems, Databases, Network and Security Devices.	
2	The solution should have a Generic Target System Connectors to enable one to uses this connector for non-standard devices etc	
3	The solution should be agentless i.e. does not require to install any agent on target devices	
4	The solution should support transparent connection to the target device, without seeing the password or typing it in as part of the connection	
5	The solution should support direct connections to windows, ssh, databases and other managed devices without having to use a jump server.	
6	The solution should have an inbuilt dual factor authentication for soft token, mobile OTP etc. Also it should have an inbuilt authenticiton for Bio-Metrics without having to acquire another biometric authentication server.	
7	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	
8	The solution should also provide local authentication and all the security features as per best standards.	
9	The solution should provide flexibility user/device wise for local authentication or enterprise authentication	
10	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 thrid party connectors.	
11	The solution should provide a method for creating new connectors with minimal intervention required from OEM.	
12	The solution should provide multi-tenancy feature whereby the entire operations can be carried out within a tenant or line of business.	
13	The solution should provide multi-domain feature whereby the entire operations can operate in an distriuted enviornment	
14	The solution should be able to handle multi-location architecture or distributed architecture with seamless integration at the User Level. For example: Multiple datacenter may have multiple secondary installations but the primary installation will also simultaneously work for all users and all locations	
B	**Shared Account Password Management**	
1	The solution shall perform password change options which is parameter driven	
2	The proposed solution should be able to manage the passwords of privilege accounts for below target devices:- - OS accounts (all flavors) - Windows local and domain account - Unix admin accounts and SSH keys - Databases (with clients like Toad, SQL Plus, SQL Server Management Studio and more) - Network and Security devices - Admin web console for applications - Cloud resources - Cloud console and access keys - VM infrastructure and ESXi	
3	The solution should set password options every x days, months, years and compliance options via the use of a policy	
4	The solution should be able to manage SSH Keys	
5	For Linux/Unix servers, the solution should have an option to generate the SSH key pair directly from the tool.	
6	Ability to create exception policies for selected systems, applications and devices	

7	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.	
8	The solution enables an administrator to change a target-account password to a random value based on a manual trigger or automatic schedule.	
9	Allow single baseline policy across all systems, applications and devcices (eg one single update to enforce baseline policy	
10	The solution should support changing a password or group of passwords according to a policy (time based or 'on-demand')	
11	Ability to generate 'One-time' passwords as an optional workflow	
12	Ability to send notifications via email or other delievery methods triggered by any type of activity	
13	Ability to send notification via email to the user requesting the password that checkout is complete	
14	All locally stored target-account passwords should encrypted using AES or similar encryption with at least 256 bit keys.	
15	The solution should automatically reconcile passwords that are detected 'out of sync' or lost without using external restore utilities	
16	The solution should have the ability to reconcile passwords manually, upon demand	
17	The solution should automatically verify , notify and report all passwords which are not in sync with PIM	
18	The solution should have the ability to automatically "check-out" after a specific time and "check-in" within a specified time.	
19	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.	
20	The tool allows secure printing of passwords in Pin Mailers. Lifecycle of printing and labelling of envelopes should be part of the module.	
21	The solution should also provide out-of-band vault capabilities (one or many)	
22	Secured Vault platform - main password storage repository should be highly secured (built-in firewall, hardened machine, limited and controlled remote access etc.)	
23	The proposed solution should restrict the solution administrators from accessing or viewing passwords or approve password requests	
24	The solution should have the capability to seamlessly change the passwords for the large number of desktops. It should be able to handle floating IPs	
25	The solution should have provision for secure offline access of managed credentials in case of vault failure (break glass scenario)	
26	The solution should have provision to allow authorized users to upload their sensitive/confidential files in the Vault for secured and encrypted storage.	
27	Files uploaded in Vault for secured and encrypted storage should be allowed to be shared between PAM users with an option to expire the share after defined period of time (in days).	

C	Access Control	
1	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.	
2	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	
3	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.	
4	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.	
5	The solution should provide for inbuilt database management utility to enable granular control on database access for Sql, my Sql, DB2, Oracle etc.	
6	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.	
7	The solution should provide secure mechanism for blacklisting/whitelisting of commands for any combination of target account, group or target system and end user.	
8	The solution can restrict user-specific entitlements of administrators individually or by group or role.	
9	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.	
10	The solution can restrict target-account-specific entitlements of end users individually or by group or role.	
11	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.	
12	The solution should provide for a script manager to help in access controlling scripts and allow to run the scripts on multiple devices at the same time.	
13	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.	
14	It should be possible to grant access to a managed asset using a specific method of access. For e.g. access to a SQL database ONLY through SQL Management Studio.	
15	Ability to Secure file transfers from Server to Server without the password	
D	Privileged Session Management and Log Management	
1	The solution should be able to support a session recording on any session initiated via PIM solution including servers, network devices, databases and virtualized environments.	
2	The solution should be able to log commands for all commands fired over SSH Session and for database access through ssh, sql+	
3	The solution shoud be able to log/search text commands for all sessions of database even through the third party utilities	
4	The solution should be able to log/search text commands for all sessions on RDP	
5	The solutions should support selective option for enabling session based recording on any combination of target account, group or target system and end-user.	
6	All logs created by the solution should be tamper proof and should have legal hold	
7	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.	
8	The tool can restrict access to different reports by administrator, group or role.	
9	The tool generates reports in at least the following formats: HTML, CSV and PDF	
10	System should be able to define critical commands for alerting & monitoring purpose through SMS or Email alerts	
11	The solution should provide separate logs for commands and session recordings. Session recordings should be available in image/ video based formats	
12	The session recording should be SMART to help jump to the right session through the text logs	
13	Secure and tamper-proof storage for audit records, policies, entitlements, privileged credentials, recordings etc.	
14	The proposed solution shall cater for live monitoring of sessions and manual termination of sessions when necessary	
15	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.	
16	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.	
17	The proposed solution shall allow configuration at platform level to allow selective recording of specific device.	
18	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).	
19	The proposed solution shall support correlated and unified auditing for shared and privileged account management and activity.	
21	The proposed system shall support full colour and resolution video recording.	
22	The proposed system shall support video session compression with no impact on video quality.	
25	The solution should provide an option to supervise privileged user activity with real time session shadowing capability.	

E	PIM Security	
1	The solutions should use minimum FIPS 140-2 validated cryptography for all data encryption.	
2	The Solution should be TLS 1.2 and SHA-2 compliant for PCI-DSS compliance	
3	All communication between system components, including components residing on the same server should be encrypted.	
4	All communicaiton between the client PC and the target server should be completely encrypted using secured gateway. (Example: a telnet session is encryted from the client PC through the secured gateway)	
5	The Administrator user cannot see the data (passwords) that are controlled by the solution.	
6	Secured platform - main password storage repository/Vault should be highly secured (hardened machine, limited and controlled remote access etc.).	
7	The solution should secure master data, records, entitlement, policy data and other credentials in tamper proof storage container.	
8	The solution should store Password and SSH keys safekeeping in the certified vault (minimum AES 256-bit encryption)	
9	The solution should not require direct third party access to PAM Database	
10	The solution should support common protocols to connect to PAM servers to ensure the best interoperability with environments.	
F	**PIM Administration**	
1	The solution should have central administration web based console for unified administration.	
2	The tool uses Active Directory/LDAP as an identity store for administrators and end users.	
3	The tool enables an administrator to define groups (or similar container objects) of administrators and end users.	
4	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.	
5	The tool enables an administrator to define a hierarchy of roles without limit.	
6	Administrative configurations (e.g. configuration of user matrix) shall be accessible via a separate client where client access is controlled by IP address.	
7	Important configuration changes in the solutions (example changes to masters) should be based on at least 5 level workflow approval process and logged accordingly	
8	The tool should have a provision to enable maker-checker configuration for critical administrative actions. For e.g. new user creation, on-demand password change etc.	
9	Segregation of Duties - The Administrator user cannot view the data (passwords) that are controlled by other teams/working groups (UNIX, Oracle etc.).	
10	The solution should provide for self service portal for users and devices for ease of on boarding both users and devices.	
11	All administrative task should be done LOB wise i.e. Line of Business Wise	
12	All administrative tasks/actions should be logged along with change in configuation value i.e. value before change made and after the change made.	
13	The solution should have Auto-Onboarding Feature for both User and Devices without having to do any manual activity.	

G	System Architecture	
1	The solution architecture should be highly scalable both vertically as well as horizontally.	
2	The proposed solution shall provide multi-tier architecture where the database and application level is separated.	
3	The solution should work at the network layer instead through a jump server.	
4	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.	
5	The proposed solution shall have the ability to support multiple mirrored systems at offsite Disaster Recovery Facilities across different data centre locations.	
6	The proposed solution shall have built-in options for backup or integration with existing backup solutions	
7	The proposed solution shall handle loss of connectivity to the centralized password management solution automatically.	
8	The proposed solution shall not require any network topology changes in order to ensure all privileged sessions are controlled by the solution.	
9	The proposed solution shall support distributed network architecture where different segments need to be supported from a central location.	
10	The proposed solution shall support both client based (in the case where browser is not available) as well as browser based administration	
11	The proposed solution should be 100% agentless that includes password storage, password management and session recording features.	
12	The solution must support parallel execution of password resets for multiple concurrent requests.	
13	The solution should provide fully failover from a single active instance to a backup/standby instance with a fully replicated repository	
14	The solution should support multiple active instances with load balancing and fully automatic failover to another active instance	
15	The solution if required should be available to install on a virtual sever	
16	The PAM Solution should have a option/capability to be configured in High Availability	
17	The solution should have an ability to have direct connection to target device as well as using secured gateway channel.	
18	Should include an enterprise version which will be highly scalable to support the High Availability at both site DC & DR	
19	Solution should support hybrid architecture	
20	There should be no latency or performance degradation in using an average of 40 concurrent users and 50 systems.	
H	Out of box Integration	
1	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.	
2	Ability to integrate with Bio-Metric Solutions	
3	Ability to integrate with Hard and Soft token solutions	
4	Ability to integrate with ticketing systems.	
5	Ability to integrate with Automation softwares for enhancing productivity in the data center	
6	Support for integration with the Hardware Security Module (HSM) devices to store the encryption keys.	
I	Ticketing System integration	
1	The solution can force the requestor of password / session to provide a reason, including a service desk incident ticket number, for the request.	
2	The solution can communicate with a workflow engine to verify an incident ticket number cited in the end user's request.	
3	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.	
4	Ability to enforce ticketing integration as well as approval workflow for specific ticket types (e.g. change/incident ticket)	
5	Inbulit ticketing system with 5 level workflow approval with ticket level validation, risk and impact assetments 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 throug the request worklfow with this valid ticket	

J	**SIEM Integration**	
1	The solution should be able to integrate with leading SIEM Solutions.	
2	The solution should be able to integrated with applications like VA Systems, performance monitoring applications to eliminate hard coded passwords	
K	**Application Password Management (Hard-Coded Password Management)**	
1	The solution should have an ability to eliminate, manage and protect privileged credentials in applications, scripts, configuration files etc.	
2	The solution should be able to authenticate and trust the application requesting the privileged password based on various authentication methods	
3	Application Servers Support - The product should support removing static hard coded passwords from Data Sources in Application Servers. Please elaborate.	
L	**Auto Discovery of Privileged Accounts**	
1	The solution should be able to perform auto discovery of privileged accounts on target systems and perform two way reconciliation.	
2	The solution should provide feature for user governance on the target devices i.e autodetect users and schdule a governance workflow and user certification process with adequate review process.	
3	Map privileged and personal accounts on various target systems	
4	Ability to quickly identify all non-built-in local administrator accounts in the environment (flag possible 'backdoor' accounts)	
5	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	

M	Notification Engine	
1	The solution should have capability to provide alerts and notification for critical PIM events over SMS & Email	
2	The solution should have capability to provide alerts and notification for all administration/configuration activities over SMS & Email	
3	Customizable notification for command executed on SSH and Telnet based devices	
4	Customizable notification for command/Process executed on Windows	
5	Notification on target being access on criteria like Line of Business or Groups	
6	Solution should have threat analytics and customised reporting capabilities	
N	**Solution Workflow**	
1	The solution should have inbuilt workflow to manage	
2	Electronic Approval based Password Retrieval	
3	Onetime access / Time Based / Permanent Access	
4	5 level approval workflow with E-mail and SMS notification with delegation rules	
5	Ability to provide for delegation at all levels in the workflow	
6	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	
7	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).	
8	Supports a workflow approval process that requires approvers to be in sequence before final approval is granted.	
9	Supports a workflow approval process that requires approvers to be in sequence before final approval is granted.	
O	**Dashboard & Reporting**	
1	Dashboard Capabilities should included real-time view of activities performed by the administrators	
2	The system shall have the ability to run all reports by frequency, on-demand and schedule.	
3	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	
4	The solution should have ability to report on all system administrative changes performed by PIM Administrators with relevant auditable records	
5	The solution should be able to report password lockouts (failure logon attempts)	
6	Ability to report password checkouts on systems and users requesting passwords	
7	Ability to report password lockouts (failure logon attempts)	
8	Ability to report on password change following verification process	
9	Ability to report on password status	
10	Reports should be customizable	
11	Audit data can be exported for use for any BI Tool	
12	Reports shall be automatically distributed by email	
13	Access to audit reports (and report configuration) shall be restricted to "auditor" end-users	
14	Ability to replay actual session recordings for forensic analysis	
15	The recorded session should be compressed and not take much space on storage and only active session has to be monitored	
16	Dashboard - for at a glance critical events and password policies.	
P	**Industry Certifications and Evaluations**	
1	The offered PIM/PAM OEM Solution must be certified for Common Criteria Certificate EAL 2+ and supporting certificate document should be submitted during bid submission	
Q	**Brand and Technology**	
1	OEM Should have 24*7 support center in India (Please share Support center details & address)	
2	The solution should be covered by the Gartner Magic Quadrant for last three consecutive years (2023, 2024 and 2025) & should be in Leaders/Challengers (MQ Gartner report to be submitted)	
3	The Solution must be a leading, mature, internationally recognised and widely used brand that has been in existence for at least 15 years India (Please provide certificate of incorporation)	
4	The Solution should have presence and support Centre in India for atleast 15 years with 400+ employee strength (Relevant declaration & proof must be submitted)	
5	The solution should be successfully implemented in at least 5 Government Customer's in India with relevent scope of implementation. (PO/Work order copies to be submitted for the same)	