## Scope of Work and Project Milestone

**General terms of the scope of work**

Scope of this RFP is to select a bidder for the purpose of Supply, Designing, Sizing, Implementing, Integrating with all the available and upcoming applications and infrastructure and maintaining the Identity & Access Management (IDAM) Solution for the period of contract with NPCI as per the terms of this RFP. NPCI intends to procure an Enterprise wide, integrated Identity & access management solution, which is comprised of the systems and processes that allow Infosec Team to assign a single digital identity to each entity, authenticate them when they log in, authorize them to access specified resources, and monitor and manage those identities throughout their lifecycle.

Based on the contents of the RFP, the Bidder shall be required to propose a solution, which is suitable for NPCI, after taking into consideration the effort estimated for implementation of the same and the resource and the equipment requirements. NPCI expressly stipulates that Bidder’s selection under this RFP is on the express understanding that this RFP contains only the broad provisions for the entire assignment and that the deliverables and the services in connection therewith are only a part of the assignment. The Bidder shall be required to undertake to perform all such tasks, render requisite services and make available all such resources as may be required for the successful completion of the entire assignment at no additional cost to the NPCI notwithstanding what is stated here and what is not stated.

The bidder shall coordinate with on-site management teams for integration with existing applications / solutions. IDAM solution should also facilitate access to underlying infrastructure components such as application servers, databases, big data stores, middleware & messaging components, web servers, web services, ERP packages, virtual systems and cloud resources. The IDAM solution should facilitate one digital identity per individual or item. Once that digital identity has been established, it must be maintained, modified and monitored throughout each user’s or device’s access lifecycle.

The broad scope of work includes (but is not limited to) the following:

**Scope Of Work**

1. The solution provider should supply, install, commission, integrate with all the existing application (60) and new applications (20).
2. The bidder shall propose, implement & support an Identity & Access Management (IDAM) Solution that complies with specifications mentioned in the Annexure - Technical Specifications.
3. The Bidder has to provide solution, perform implementation and testing for all the proposed modules after installation and take approval from internal stakeholders on satisfactory functioning of the solution as per RFP.
4. Bidders should provide application support from the OEM as per RFP terms and maintain the solution from the date of Acceptance till the term of contract.
5. Solution should be deployed in the NPCI’s DC & DR Site each in High Availability (Active-Active or Active-Passive) with no manual intervention required for site switch over.
6. Solution proposed should be completely On-premises deployment. The public Cloud based solutions should not be proposed under this RFP and if proposed, will not be considered.
7. All components of the solution offered should run on NPCI’s servers, at NPCI’s premises. In future, the solution/applications may be shifted to cloud infrastructure. The solution offered by the bidder should be able to handle this scenario. Bidder should support such migration activity during contract term.
8. The solution should include deployment of Directory Service, User Life Cycle Management functionality, Single Sign On (SSO), Identity governance module, Access certification and request with different back-end systems and should be integrated with our MFA solution.
9. The solution provider should provide a detailed Plan of Action (PoA) for implementing the solution. It should include the approach, risk, benefits. Post approval of PoA, solution provider should work with NPCI’s internal Information security team, application team and the other stakeholders to complete the integration with other tools and devices.
10. The bidder should provide updates, upgrades version of software, new vulnerability updates as and when released within the term of contract.
11. All critical/major vulnerabilities known till the time of implementation of the IDAM tool should be remediated for the deployed solution.
12. The solution should have the capability to on-board & integrate the users of NPCI & it’s subsidiaries.
13. The bidder shall assign project manager and associated support personnel to be positioned at NPCI site for complete project deployment in order to ensure smooth completion of this project within the agreed timelines.
14. Post implementation of the solution, the bidder shall perform the following activities, but not limited to, from time to time, in relation to maintenance and upgrades/updates/patches:

(a) Firmware Upgrades

(b) Software System monitoring,

(c) Troubleshooting & Performance Tuning,

(d) Operating System Upgrades,

(e) Upgrades of supplied software,

(f) Advisories on software upgrades & vulnerabilities,

(g) Support during DR Drills,

(h) OS Administration & patching as per OEM guidelines (In case of Software image supplied by OEM/Bidder.

(i) Any support required to make systems & software up and running.

Note – The list mentioned above is the indicative list, however the successful bidder shall provide end-to-end support, repair and upkeep related any activities and resolution of any issues related to solution deployment without any extra cost to the NPCI.

1. The updates/ patches (critical / non-critical) and security bug fixes/ patches as and when released by OEM or required upon any advisories from statutory/ regulatory bodies or required for any bug fixes in the solution, for the proposed solution/ servers/OS, to be tested first in non-production (UAT) environment, and thereafter deployed, installed and configured by bidder’s team at NPCI’s site, as per NPCI's requirement during the contract period without any additional cost to NPCI.
2. The services / solution offered should not have any significant adverse impact on the existing infrastructure/ business of the NPCI neither during installation nor during operations. There should be no service disruption as part of implementation or any upgrades. Any such incident may attract penalties as per SLA.
3. Bidder / OEM should perform an annual health check-up of the deployment to ensure effective usage and basis on the observation, should take necessary corrective action.

## Non-Functional Requirements

**Backup and Archiving**

1. There shall be a provision for taking backups and archive the replica of the systems’ database and the application as well. There should be a provision of adequate Business Continuity Management (BCM).
2. The methodology for the backing up of data and its archival may be indicated and provided by the bidder.
3. The methodology or strategy used should be in alignment with NPCI’s Backup and Archival strategy. NPCI will share the Backup, archival and restoration policy with the successful bidder. It is standard process which aims for zero data loss during failure.
4. The Application should have a capability for easy retrieval and restore of the backed-up data (both application and the database) with least amount of manual intervention with no data Loss events.
5. Backup and restoration should be on premise. Backup procedure for Application and Database server of the proposed solution is required and to be demonstrated.
6. Data retention period will be shared with the successful bidder only.
7. Backup & restore process should be smooth in case of both site failure & bidder should able to support for complete restoration, configuration & Integration with different application.

**Security Requirements**

1. Solution should provide security in compliance with NPCI security requirements to protect the confidentiality, integrity, and availability of the information systems.
2. The Bidder shall abide by the access level agreement to ensure safeguards of the confidentiality, integrity, and availability of the information systems.
3. Bidder shall not copy any data obtained while performing services under this RFP to any media, including hard drives, flash drives, or other electronic device, other than as expressly approved by NPCI.

**Guidelines for Maintenance and Support**

1. Bidder should follow NPCI policy on Change, Patch & Incident management process.
2. NPCI will conduct security assessment which will consist of VAPT and Risk Assessment of IDAM tool before production implementation. All the vulnerabilites idenfied in VAPT and risk / observations identified in risk asessment will be fixed by bidder/OEM prior to go-live without any additional cost to NPCI.
3. All exceptions to be documented and signed off by appropriate NPCI authority.
4. Configuration items such as computers and other devices, software contracts and licenses, third party tools and business services which are related to the application should be disclosed.
5. Additional guidelines would be provided based on the support scenario that’s decided between bidder and NPCI.
6. The cost of each of the line items (for each of the solution) as mentioned in the RFP has to be mentioned at appropriate place in the respective formats. The detail specification/datasheet of each line item/solution should be submitted as part of Bill of Materials (BOM) and will be construed as an integral part of a solution suite. NPCI shall not make any additional payment other than line items mentioned in the price bid format. ( non-functional requirements )
7. Bidder shall provide requirement explicitly for VM and Storage infrastructure for implementation of each solution as part of its bill of material(BOM). The change in requirement at later stage may affect the project and its timelines. The bidder shall own the responsibility for any such delay.
8. The bidder shall submit price bid as per given price schedule only. Any extra components (hardware or software) / item if required should be included in the cost of given line items only. The same should be clearly mentioned in the Bill of Materials submitted along with the bid. If any item, components (hardware or software) required for implementation and not mentioned in BOM, such items should be provided by the bidder without any extra cost to the NPCI.

**Onsite Manpower Required (In total for all solutions):**

|  |  |
| --- | --- |
| **Type** | **Quantity** |
| (10 am to 7 pm) 5 working days onsite for duration of Implementation and subsequently for 1 year of support. | 1 resource per shift |
| Remote support should be provided 24\*7 365 | Bidder / OEM |
| In Addition of above,  TAM from OEM should be available to support deployed resource at NPCI | 1 resource |

In case of exigency, support arrangement should be available during off-hours as a part of the crisis / incident management process and other planned activities.

**Deployment**

1. The Bidder’s resources shall be required onsite during the deployment phase as described in section **Onsite Manpower Requirement table.**
2. The bidder shall do the Configuration of IDAM Tool (Software/virtual/ appliance) and integrate the solution with all the available application and test IDAM functions for all the integrated applications.
3. The test case are to be submitted by the bidder and sign off needs to be obtained on the submitted test cases before initiating UAT.
4. Taking signoff from NPCI internal stakeholders post completion of UAT installation of IDAM solution.
5. Taking signoff from NPCI internal stakeholders post completion of Live installation of IDAM solution.

**Preparation of System Requirement Specification Document**

1. The Bidder is expected to create System Requirement Specification (SRS) Document under the scope of the Identity & Access Management Solution implementation including all proposed interfaces and customisations involved. The system specification document shall be signed off by the NPCI on acceptance of the same.
2. The Bidder is expected to prepare the System Requirement Specification Document containing the following details but not limited to:

a) Overview of the Process with System/Application FAQs.

b) Security features.

c) User manual & Run Book.

d) Version description document

e) Application upgradation and patches management document

f) Architecture & design document including Traffic flow document between the devices.

g) Project Plan with milestones, resourcing and deliverables

h) Testing cases and test results documented before and after implementation.

l) Standard Operating Procedures

n) Bidder support details and escalation matrix

o) OEM support details and escalation matrix

q) IT Security and Backup Architecture and parameterization with relevant details

s) User Manual and online tutorial

t) Performance Measurement Matrix.

u) User onboarding and offboarding process.

v) Automatic user recertification process( for audit purpose).

w) List of report which can be extracted from the solution (Customized Reports).

## Training

1. The bidder is expected to define the approach that will be taken to train the resources on the technical aspects of the solution. The quality of the Bidder’s approach to training shall form an integral part of the final evaluation and selection of the Bidder.
2. The Bidders shall provide professional training by OEM or its Certified Training partner to the identified team (minimum 5 in number) on the solution(s) (for minimum 3 days) for features / service architecture, and functionality during and after implementation. The related certification should also be awarded to the trainees.
3. The bidder should include all kind of trainings and other documentations preparation efforts in the given line items of the RFP only.
4. Training completion documents should be submitted along with signoff report of the document.
5. The Bidder should prepare the end-user manuals, FAQs and admin manuals.

## Implementation

The implementation phase shall be deemed as completed in all respects only after:

* All applications (including upcoming) and services should be integrated as per the intent of this RFP.
* All functionalities mentioned in this RFP should be implemented.
* All the related trainings should be completed.
* VAPT and Risk assestment exercise shall be conducted by the NPCI, it shall be the bidder’s responsibility to rectify the risk /observations unearthed during the VAPT and risk assestment at no additional cost to the NPCI during the contract period.

## Go Live

1. Before the final Go-Live the Bidder has to complete the development/ customization of the application as per the Technical Specifications agreed with the NPCI.
2. The Go-Live is an end‐to‐end responsibility of the Bidder who will manage total planning, hand holding support as per the scope of work.
3. Bidder should provide 180 Days of hand holding support post Go-Live.
4. On satisfactory performance of application post 180 days from Go-Live, NPCI will issue Completion Certificate.
5. All documents submitted by the Bidder must be in the format specified by NPCI. NPCI reserves the right to ask for re-work on the submitted document(s) in the delivery of Project, the Bidder is required to do the said re-work without any added cost to NPCI.
6. All deliverable milestones will be considered as completed only when they are explicitly accepted by NPCI.
7. In case of the Go-Live delays by the Bidder penalty will be imposed as specified in section.

**Acceptance:** A one-month test period will be used by NPCI to evaluate the selected Identity & Access Management (IDAM) Solution. After the selected solution has been successfully tested and implemented, NPCI and the bidder shall agree on the start date of the Go-LIVE.

## Technical Specification

|  |  |  |  |
| --- | --- | --- | --- |
| **Sr No** | **IDAM Specification** | **Requirements** | **Weightage** |
| **1** | **General Features** |  |  |
| 1.1 | The bidder should have back-to-back arrangement with the OEM so that NPCI will be able to log a call with the OEM directly. | Must Have |  |
| 1.2 | The vendor/bidder must be Gold/Tier-1 or Silver/Tier-2 or Authorized partner of the OEM for the proposed product. | Must Have |  |
| 1.3 | The bidder should have support offices in Mumbai, Hyderabad and Chennai in case of supply of Hardware module. | Must Have |  |
| 1.4 | The bidder should have minimum 2 skilled OEM certified staff deployed for NPCI for the proposed product. | Must Have |  |
| 1.5 | The Solution quoted by the bidder should be in Gartner Leader or Challenger Magic Quadrant for Identity and access management solution, or Forrester wave leader or strong performers in consecutively for last Two years (Two of last 3 years). | Must Have |  |
| 1.6 | Solution should also support Single sign on feature. In case of future requirement, NPCI can enable SSO on same console with license upgrade. | Good to have |  |
| 1.7 | The proposed solution should have single consoles for all features offerings: User life cycle management, Access request & Access Certification, Integration with Applications, Audit & Compliance Policy management & separation of duties. | Must Have |  |
| 1.8 | Solution should provide a facility to back up all the configuration and export in a file. | Must Have |  |
| 1.10 | The suite should support integration with all leading database servers including Oracle RDBMS, IBM DB2, Microsoft SQL Server, SAP Sybase ASE, Teradata, ADABAS, MySQL, FileMaker, Microsoft Access, Informix, SQLite, PostgresSQL, AmazonRDS, MongoDB, Redis, CouchDB, Neo4j, OrientDB, Couchbase, Toad, phpMyAdmin, SQL Developer, Seqel PRO, Robomongo, Hadoop HDFS, Cloudera, MariaDB, Informix Dynamic Server, Altibase, DbVisualizer. | Must Have |  |
| 1.11 | All the Software supplied under this contract should be IPv4/IPv6 & TLS 1.2, 1.3 or higher ready. | Must Have |  |
| 1.12 | The proposed solution(s) should provide dashboard view for various level of users / department heads as per NPCI’s requirement.  Creation of dashboard with the following features-   * Top Management View (Board) – Having Summarized view of various department (Can be explored to show the detailed information pertaining to the particular / all departments (individually). * Department Heads (Various IT Business Department Heads) – Having detailed information pertaining to a particular department. The department head can have access to information pertaining to their department only. However, being common department head, the head may have access to the information pertaining to more than one department. * Executive committee (complete and detailed dashboard of the organization). * System Administrator (for the systems associated with this administrator). | Good to Have |  |
| 1.13 | There shall be provision for complete audit trail of all operations by the users. There shall be provision / functionality to track down all backend modifications as per assigned users’ roles and responsibilities, if any by any user which can be retrieved and analysed to get the complete history of the issue. The bidder may take it as an input for redressal of the issue, if the same is application related. | Must Have |  |
| 1.14 | The bidder should schedule backup of full database & configuration of all components of Identity and Access Management Solution along with all its configurations on defined frequency. It should be possible to restore the backup of full database & configuration. The bidder shall perform the archival and purging of database as per laid down guidelines and policies of NPCI. | Must Have |  |
| 1.15 | High Availability- The solution must be configured in HA mode for all the components included as part of offering. | Must Have |  |
| 1.16 | DR - The solution offered should be replicated at Disaster Recovery (DR) sites of NPCI in active or passive mode. | Must Have |  |
| 1.17 | The solution should support configuring scheduled automatic backup of application with no dependency on operating system scheduled tasks.- Backup. | Must Have |  |
| 1.18 | The solution should be able to ingest data from an existing IDAM solution to determine existing access. | Must Have |  |
|  | solution should support the creation of an application risk model to determine the relative risk of each managed application based on pre-defined risk factors. | Good to Have |  |
| 1.19 | Solution should have centralized architecture with web or GUI based dashboard console to monitor, report, notification, maintaining and policy push for the registered users centrally for multiple sites. | Must Have |  |
| 1.20 | The solution must be able to highlight violations in real time or based on schedule in case of application access is provided from backend or by passing IDAM solution. | Must Have |  |
|  | solution should dynamically calculate a user’s risk score based on changes to access within the environment. | Good to Have |  |
| 1.21 | Proposed solution should support identity and access management console session time out and idle time out facility to forcefully logout the users. | Must Have |  |
| 1.22 | The solution should block users when multiple (configurable) numbers of policy violations are triggered simultaneously. | Must Have |  |
| **2** | **User Lifecycle Management** |  |  |
| 2.1 | User ID Creation/ Modification/ Deletion - creation and modification of users’ data manually or automatically based on event and / or workflow or script. | Must Have |  |
| 2.2 | User ID Lock/Unlock - locking and unlocking of users manually or automatically based on event or workflow and mass lock & unlock. | Must Have |  |
| 2.3 | Service / Support ID - Should be created automatically or manually based on event or workflow. | Must Have |  |
| 2.4 | De-Duplication of user ids - Duplicate user-ids should not be allowed. | Must Have |  |
| 2.5 | User ID Merging - Ability to merge user ID / identities in cases where multiple identities are created for a single person. | Must Have |  |
| 2.6 | Delegated User Administration - Allows user management to be distributed to users other than administrators, including providing multiple granular levels of identity administration permissions. | Good to Have |  |
| 2.7 | Delegation of Authority - Allows users to assign a delegate while away from the office for example, while on vacation. | Must Have |  |
| 2.8 | Single User ID repository - Identity repository for users to know all type of access user having and eliminate the application-level user ID management. | Must Have |  |
| 2.9 | Group Management in Active Directory - Allows creation/deletion of groups and addition/deletion of group members. | Must Have |  |
| 2.10 | Delegated Group Management - Allows group creation, deletion, and management to be performed by identified users based on authority delegation by administrators. | Good to Have |  |
| 2.11 | Dynamic Groups - supports addition/deletion of users to group dynamically based on rules or set of rules. | Good to Have |  |
| 2.12 | Password policy and account lockout – Use policies to enforce rules related to password complexity, expiry, length, password aging, password composition and password history enforcement. | Must Have |  |
| 2.13 | Self-service password resets - Allows users to manage their passwords and to reset a forgotten password without the help of an administrator. | Must Have |  |
| 2.14 | Password synchronization – Synchronization of passwords across manged systems. | Must Have |  |
| 2.15 | User ID provisioning and de-provisioning based on event - Provisioning and de- provisioning of users based on events such as approval and updation of all dependent target department. | Must Have |  |
| 2.16 | Solution should be able to manage previously disparate data repositories, applications, and user data stores anywhere in the infrastructure stack. | Must Have |  |
| 2.17 | solution must be able to provision access based on department roles defined within the solution using custom criteria for membership. | Must Have |  |
| 2.18 | The solution must allow to import roles using manual and automated interfaces. | Must Have |  |
| 2.19 | Solution should allow automated provisioning and deprovisioning of users. | Must Have |  |
| 2.20 | solution should support a ‘least privilege’ security model by decentralizing control with delegated administration. | Good to Have |  |
| 2.21 | Solution should be able to integrate application deployed on on-premises and public cloud platforms besides just Active Directory, including databases, other directories, platforms, and ERPs. | Must Have |  |
| 2.22 | End users can request additional access from a self-service interface. | Must Have |  |
| 2.23 | The solution must support provisioning into a variety of on-premises and cloud-based business applications. | Must Have |  |
| 2.24 | The solution should support configuration of workflow based on joiner, mover, or leaver scenarios. | Must Have |  |
| 2.25 | The solution should be able to generate unique attributes at provisioning time based on data collected, or by calling the system to validate attribute values. | Must Have |  |
| 2.26 | The solution should be able to do Provisioning/Deprovisioning of accounts based on transfers and promotions. | Must Have |  |
| 2.27 | User provisioning and de-provisioning should be possible in the Active Directory as well as in all applications (new-age, legacy, on-premises and cloud with and without API’s) | Must Have |  |
| 2.28 | The solution should support provisioning/de-provisioning of users as well if the user ID of the users in the application is different from the user ID in the Active Directory. | Must Have |  |
| **3** | **Password Management and Authentication** |  |  |
| 3.1 | Password policy and account lockout – Use policies to enforce rules related to password complexity, expiry, length, password aging, password composition, password history enforcement etc. | Must Have |  |
| 3.2 | Self-service password resets - Allows users to manage their passwords and to reset a forgotten password without the help of an administrator. | Must Have |  |
| 3.3 | Password synchronization – Synchronization of passwords across manged systems. | Must Have |  |
| 3.4 | Solution should support MFA capabilities including FIDO2/Web Authentication, OATH (TOTP/HOTP) for access management in IDAM solution. | Must Have |  |
| 3.5 | The solution should have authentication options for users/groups, it should supports authentication of users via Integrated Windows Authentication (Kerberos) or NTLM (NTLM v1 and v2 in Session Security), or LDAP. | Must Have |  |
| 3.6 | Solution should allow for secure passwordless authentication of users. | Good to Have |  |
| **4** | **Role Management and Identity and User Account** |  |  |
| 4.1 | Role lifecycle management based on Approval - Supports creation/ updating / deletion/ assignment/ de-assignment of roles based on requests and / or workflow. | Must Have |  |
| 4.2 | The solution should be able to perform 'Role Mining', in a fully automated way. | Must Have |  |
| 4.3 | The solution should be able to provide membership context for mined (identified) roles. | Good to Have |  |
| 4.4 | The solution should be able to ingest data from an existing IDAM solution to determine existing access. | Must Have |  |
| 4.5 | The solution should be able to identify users that have been provided access to systems directly by admins instead of by the IDAM solution. | Must Have |  |
| 4.6 | Solution shall allow user identities to be created utilizing data from multiple identity sources, with support for multiple authoritative sources. | Must Have |  |
| 4.7 | The solution must provide the ability to split identities into different user populations (employees, contractors, vendors, etc.) and apply different management controls of each including separate password policies, provisioning rules, lifecycle management, authentication controls & strong authentication requirements. | Must Have |  |
| 4.8 | The identity construct in the solution should have the ability to use any username format as a unique identifier to link identities across all applications and user directories, rather than an obscure identifier such as GUID. Additionally, the solution should support multiple different username conventions for different populations of users. | Must Have |  |
| 4.9 | Solution should support the implementation of Role Based Access Controls (RBAC) for controlling access to functions within an application | Must Have |  |
| 4.10 | Solution should Support for different employee types, e.g., Full-time employees, Contractors, Guests, Vendors, must be provided as a result of connection to relevant Identity data sources. The solution should support disparate sources of identity working in combination, sourcing identity attributes from each source and applying varied controls and options per population of identities. | Must Have |  |
| 4.11 | The solution offers the ability to define your own identity attributes and control the data mappings and values. | Must Have |  |
| 4.12 | The solution should support multiple accounts from a variety of sources. | Must Have |  |
| 4.13 | The solution identifies unused, uncorrelated or unauthorized accounts and allows administrators to manage, and if desired disable or delete these accounts. | Must Have |  |
| 4.14 | Solution should provide the ability for user’s who has forgotten his/her password to trigger a password reset and receive a new solution-generated password sent to the email address associated with their user account. | Good to Have |  |
| 4.15 | Solution should provide a clear audit log of “impersonation” events to enable investigation of who has performed the functions or changed data using an admin / root account. | Must Have |  |
| 4.16 | Solution should be capable of automatically sending a notification email to the user when changes are made to their role membership or the definition of a role of which they are a member. | Must Have |  |
| 4.17 | Solution should have the ability to dynamically assign and revoke access rights based on user role changes | Must Have |  |
| 4.18 | Solution should incorporate a consolidated user management facility to "front-end" a variety of systems, allowing a security administrator to manage one user across a variety of systems with a single program / GUI | Must Have |  |
| 4.19 | The bidder shall either provide or design a customizable ‘landing page’ for all external access. | Must Have |  |
| 4.20 | Solution should have the ability to customize mappings of key attributes (for example, map unique user ID to email or password to alternate attribute) | Must Have |  |
| 4.21 | Solution should have the configurable ability to synchronize user account data with other authoritative data sources or repositories. (Specify if in real-time or scheduled and if can synchronize one-way or two-way) | Must Have |  |
| 4.22 | The solution must allow to easily identify high-risk via reporting and analytics. | Must Have |  |
| **5** | **Connections** |  |  |
| 5.1 | The solution must be able to integrate with multiple Active Directory domains/forests and multiple LDAP directory technologies beyond just a single Active Directory. | Must Have |  |
| 5.2 | The solution must provide connectivity to non-UI based applications, like Linux and Unix. | Must Have |  |
| 5.3 | The solution should support ability to develop and build custom connectors and integrations with other platforms. | Must Have |  |
| 5.4 | The solution must support standard account operations - create, modify, delete, enable, disable, and unlock. | Must Have |  |
| 5.6 | Admin should be able to build custom workflows to integrate with application from frontend. | Must Have |  |
| 5.7 | solution provide Azure Admin connector to assign licenses to employees, vendors, and external user’s on O-365 Apps based on various categories of licenses. | Must Have |  |
| **6** | **API Management and Integrations** |  |  |
| 6.1 | Proposed solution should provide APIs for integration with Legacy Applications | Must Have |  |
| 6.3 | The solution shall integrate with third-party Service Request Management systems or ITSM. | Must Have |  |
| 6.4 | solution integrate with other systems and enable the consolidation of multiple identity silos to create a single view of a user across the organization. | Must Have |  |
| 6.5 | The solution should feature integration with leading PAM solution to facilitate visibility, governance and lifecycle management/provisioning over users with access to privileged accounts managed by the PAM system. | Must Have |  |
| 6.6 | The solution should be deployed on premises and should be able to integrate with on premises as well as cloud-based applications. | Must Have |  |
| 6.7 | The solution must support the ability to integrate with business-oriented chat systems - such as Microsoft Teams. | Good to Have |  |
| 6.8 | Solution should provide the ability to manage identities through policies. Solution should utilize policy to manage work flows. | Must Have |  |
| 6.9 | Solution should provide the ability to grant system "authority" to particular Identity attributes, i.e. designate different authoritative sources for different attributes. | Must Have |  |
| 6.10 | Solution should provision users and grant entitlements based on user “Role”. | Must Have |  |
| 6.11 | Solution should allow users provisioned to a target system based on a “Rules”, “Roles” or “Workflow”. Solution should provide a single connected system allow for more than one method simultaneously. | Must Have |  |
| 6.12 | Solution should provide the ability to manage groups, individual users or both. | Must Have |  |
| 6.13 | Solution should provide end-users initiate workflow requests. Workflow requests should be used for non-connected systems as well. | Must Have |  |
| 6.14 | Solution should provide the delegation functionality in Workflow tool. Solution should also provide an Approver select specific Delegates feature. | Must Have |  |
| 6.15 | Solution should provide the ability to run correlation analysis with log-generated data from non-Identity connected systems. | Must Have |  |
| 6.16 | System should be able to integrate with legacy applications that have no API's (both, native as well as web applications) | Must Have |  |
| 6.17 | System should allow a combination of UI automation, DB queries and Api's to integrate with each application. | Good to Have |  |
| 6.18 | Solution should have the ability to customize mappings of key attributes (for example, map unique user ID to email or password to alternate attribute) | Must Have |  |
| 6.19 | Solution should have the configurable ability to synchronize user account data with other authoritative data sources or repositories. (specify if in real-time or scheduled and if can synchronize one-way or two-way). | Must Have |  |
| **7** | **Access Request and Access Certification** |  |  |
| 7.1 | The solution must support requests for access to applications that are not integrated for automatic provisioning, so that uniform request and approval processes can be applied to every application. | Must Have |  |
| 7.2 | Enable the approver (manager, owner, etc.) to approve at a group or fine-grained entitlement level. | Must Have |  |
| 7.3 | Access requests should be able to support end-dates for when access should be granted on a temporary basis. | Must Have |  |
| 7.4 | Access request end-dates will remove the access whenever the approved time and date is reached. | Must Have |  |
| 7.5 | Solution should be able to send reminder’s 30 days before to the users as an expiry alert to the applications they have access on. | Must Have |  |
| 7.6 | Solution should be able to identify users that have been provided access to systems directly by admins instead of by the IDAM solution. | Good to Have |  |
| 7.7 | Access requests should be able to be extended into a custom platform of choice - like MS Teams, or even custom portals. | Good to Have |  |
| 7.8 | Automatically provision user access after access has been approved/authorized. | Must Have |  |
| 7.9 | Solution should allow users to request access on applications behalf of others? | Must Have |  |
| 7.10 | Access requests should support approval workflows. | Must Have |  |
| 7.11 | The access request approval process should support multiple approvers. | Must Have |  |
| 7.12 | The solution must support requests for access to applications that are not integrated for automatic provisioning, so that uniform request and approval processes can be applied to every application. | Must Have |  |
| 7.13 | Solution should provide a page whereby users can view the current status of requests they have made to application administrators using the self-service interface. | Must Have |  |
|  | solution should enable risk mitigation actions (e.g., certifications or activity monitoring) to be targeted at high-risk users. |  |  |
| 7.14 | A comprehensive user-friendly interface for conducting certification campaigns, including access reviews and certification-triggered remediations such as access revocation from target systems shall be included in the cloud identity solution. | Must Have |  |
| 7.15 | The certification process must provide closed-loop validation that revoked access of the user’s if provisioned directly by passing IDAM solution to the target application. | Must Have |  |
| 7.16 | The solution shall automatically scale to accommodate spikes in usage, such as quarterly or annual certifications. | Must Have |  |
| 7.17 | The solution will certify all access data, including accounts and complex entitlement data. | Must Have |  |
| 7.18 | The solution provides reports of all certification activity for auditor review and to meet compliance requirements. | Must Have |  |
| 7.19 | The solution will automatically notify managers when the campaign begins and remind them before the campaign is due. | Must Have |  |
| 7.20 | The solution allows certifiers to make bulk actions on any reviews that they can see. | Must Have |  |
| 7.21 | The solution provides certifiers AI-based recommendations to help provide guidance around access within a certification. | Good to Have |  |
| 7.22 | A user-friendly searchable, and informative certification interface that can allow for making decisions based on the identity or the access. | Must Have |  |
| 7.23 | Certifications can be triggered based on identity-related events, such as a department change, termination, manager change, etc. | Must Have |  |
| 7.24 | Solution should validate data entered both manually and through data feeds (through user interaction and bulk loads) | Must Have |  |
| 7.25 | The solution must provide tools for identifying and managing orphan accounts | Must Have |  |
| 7.26 | The solution must provide reports which outlines defined security risks by application. | Must Have |  |
| 7.27 | The solution must provide approvers with additional support for access certification decision making. I.e., Context and recommendations. | Good to Have |  |
| 7.28 | The solution must provide signals for filtering certifications based on a defined risk score. | Good to Have |  |
| 7.29 | The solution must provide a signal for the automation of certifications based on defined risk score, both on a bulk and individual item basis. | Must Have |  |
| 7.30 | The management console should maintain audit logs that provide summaries about user access, app-related actions, setting changes, and other configuration modifications that occurred using the console or APIs. | Must Have |  |
| 7.31 | The proposed solution should have API keys to allow third-party applications to access data through authorized accounts. | Must Have |  |
| 7.32 | The proposed solution should have the capability to allow integration with 3rd party solutions via API. | Must Have |  |
| 7.33 | The solution must provide signals for enabling the automation of Access Requests approvals. | Must Have |  |
| **8** | **Audit and Compliance** |  |  |
| 8.1 | Solution should offer the ability to review and certify user access periodically to ensure that users have the right access. | Must Have |  |
| 8.2 | Solution should support Four different access certification campaign for periodic access review:  1. Entitlement Campaign.  2. Role Certification Campaign.  3. Application Account Campaign.  4. User Identity Account Campaign. | Must Have |  |
| 8.3 | Solution should provide the ability to specify exclusionary roles that prevent assignment of conflicting roles. | Must Have |  |
| 8.4 | Solution should have the capability to perform access reviews on an ad-hoc or event-driven basis, such as when a user changes roles. | Must Have |  |
| 8.5 | Solution should be capable of automatically sending a notification email to the user when changes are made to their role membership or the definition of a role of which they are a member. | Must Have |  |
| 8.6 | solution should have capability for a multi-step access review process so that more than one reviewer can verify the user access. | Must Have |  |
| 8.7 | solution should contain governance administration capabilities integrate tightly with the provisioning solution so that any access that is denied is immediately revoked? | Must Have |  |
| 8.8 | The solution must provide comprehensive analytical reporting capabilities, including outlier detection to assist with the cleansing of risky or excessive access. | Must Have |  |
| 8.9 | solution should alert or notify managers, application owners or compliance officers based on changes to an identity or resource risk score | Must Have |  |
| 8.10 | The solution must support the definition of account or identity attribute access policies. | Must Have |  |
| 8.11 | The solution must provide a business-friendly UI for defining and editing access policies without requiring coding. | Must Have |  |
| 8.12 | The solution must provide a single policy repository that is leveraged by all identity processes, including both detective and preventive access controls. | Must Have |  |
| 8.13 | The solution must automatically scan and detect policy violations. | Must Have |  |
| 8.14 | The solution must notify responsible parties / application owner when policy violations are detected. | Must Have |  |
|  | solution should support bulk corrective or mitigating actions (such as an ad hoc certification) be taken against high-risk user populations discovered via reporting or analytics. | Must Have |  |
| 8.15 | Solution should have the ability to dynamically assign, and revoke access rights based on user role changes | Must Have |  |
| 8.16 | Solution should provide the ability to specify exclusionary roles that prevent assignment of conflicting roles. | Must Have |  |
| 8.17 | Does the provider allow users to search and request additional access for themselves? | Must Have |  |
| 8.18 | The solution shall be able to generate, schedule, and view reports based on custom requirements. The solution shall provide out-of-box reporting templates to create one-time or recurring reports based on security events. | Must Have |  |
| 8.19 | Proposed solution should support to pull & generate reports in different logs format such as pdf and csv. | Must Have |  |
| 8.20 | Solution should be able to manage segregation of duties in applications as well as infrastructure systems. | Must Have |  |
| 8.21 | The solution must allow users to quickly and easily create a library of Separation of Duties (SoD) policies from the entitlemens and access specific to our environment. | Must Have |  |
| 8.22 | SoD policies must allow for tagging against specific compliance practices (such as SOX, HIPAA, GDPR.) or other business criteria (such as "Region: US" or "Bus\_Unit: Finance"). | Must Have |  |
| 8.23 | Solution should track and monitor the risk of each user based on that user’s access to sensitive applications and data (identity risk scoring). | Must Have |  |
| 8.24 | solution should support configurable risk factors and weightings for calculating identity or risk scores?  Can risk scores on access be used to calculate the overall risk score of an identity within the organization. | Must Have |  |
| 8.25 | Notifications must be sent when violations are discovered. | Must Have |  |
| 8.24 | solution should allow for a preventative Separation of Duties check against policy when access is requested. | Must Have |  |
| 8.25 | The system should have the capability of actioning policy violations in an automated manner. | Must Have |  |
| 8.26 | The solution must support the ability to define and enforce access policies, including Separation of Duties (SoD) policies, between individual roles, between individual entitlements, and between roles and entitlements. | Must Have |  |
| 8.27 | solution should recommend risk mitigation actions for high-risk users, such as activity monitoring, ad hoc certifications, or remediation of policy violations. | Must Have |  |
| 8.28 | solution should support the assignment of unique risk values to each application, entitlement and role within the system. | Good to Have |  |
| 8.29 | Solution should capture all activity information as part of audit logging & forward it to SIEM. | Must Have |  |
| 8.30 | The solution must support granular access control and authorization to facilitate gathering of logs of users access. | Must Have |  |
| 8.31 | The solution should support real time graphical and chart based dashboard for the summary of activities. Solution should have capability to maintain records for 12 Months and to generate trend reports for 12 months. | Must Have |  |

## Technical Scoring Matrix

|  |  |  |
| --- | --- | --- |
| **TECHNICAL SCORING MATRIX** | | |
| **Sr. No** | **Description** | **Score** |
| **Technical Evaluation Part – A** | | 70 |
| 1 | Technical Requirements compliance (60) |
| 2 | Clarity of requirements specified in RFP (10) |
| **RFP Presentation Part – B (Bidder Evaluation Matrix)** | | 10 |
| 1 | Customer BFSI reference in India (5) |
| 2 | Size of the deployment in terms of number of Application Integration. (5) |
| **Proposed Solution Part – C** | | 10 |
| 1 | Bidder credentials, Experience and past performance on similar contracts. (3) |
| 2 | Comprehensiveness of the documents & Project Management Plan (4) |
| 3 | Clarity & thought of project delivery (3) |
| **RFP Presentation Part – D** | | 10 |
| 1 | RFP presentation (5) |
| 2 | Q and A  (5) |
|  | **Total Score of Part - A, B, C and D** | **100** |

## Key deliverables

Supply software, Licenses, installation, maintenance, training and post implementation support for the Identity and access management solution. (Software, License for OS core based, license for DB core based with unlimited device/user integration). Bidders to provide the item wise details along with quantity in Bill of materials.

1. Implementation of the complete IDAM solution.
2. Dedicated Premium Support for 3 years with SLA defined.
3. Integration of IDAM solution with all existing and new NPCI applications.
4. OEM Technical Training for NPCI officials with minimum of 2 Certifications (Detailed technical training before Project Kick off and post implementation training)
5. Post Implementation: OEM is annually required to review the deployment and suggest fine tuning, a minimum 7-10 days per year review & fine-tuning effort of the OEM needs to be factored for implemented solution.

## Delivery Schedules

Delivery, installation, commissioning & integrations of Identity and access management solution with NPCI applications as per scope define should be completed within 16 weeks from the date of receipt of purchase order.

• Delivery of software and licenses should be within 2 weeks.

• Installation, commissioning and integrations should be completed within next 14 weeks.

• Installation Certificate for each installation should be signed by NPCI and the bidder.

• Training and certification has to be completed within 16 weeks of time.

## Warranty

The successful bidder(s) shall provide comprehensive on-site warranty for 3 years for complete solution with back-to-back arrangements with the respective OEM from the date of acceptance of software / application.

The deliverable(s) should not have been declared End of Sale as on the date of submission of the bid and on the date of delivery.

The successful bidder(s) should ensure that the equipment proposed in this RFP, should not be declared as End of Life (EOL) or End of Support (EOS) by the OEM within the 3 years contract period.

If the deliverable(s) is declared End of Life (EOL) or End of Support anytime during the contract period, the successful bidder shall forthwith replace the equipment at no additional cost to NPCI.

Bidder shall also update necessary OS / application patches and should support the software for the period of three years from the date of acceptance of the entire system.

The upgrades, new releases (Minor/major) versions, bug fixes etc. for the system software will be supplied to NPCI at no extra cost, with the necessary documentation during contract period.

Bidder shall implement all software updates, new releases & version upgrades on the supplied components during the warranty period. The bidder should update and maintain all supplied components to correctly reflect actual state of the setup at any point in time during the warranty period.