Annex “A”

Terms of Reference (TOR’s)

IDENTITY AND ACCESS MANAGEMENT (IAM) SOLUTION

Table of Contents

Scope of Work (SoW) /Functional Requirements (FRs) for IAM solution

Scope of Work (SoW):

Following is the scope of work:

1. Supply, installation, configuration of Identity and Access Management (IAM) solution at Head office, Branch offices and DRC, covering:

   A. IDG;
   B. AM;
   C. Self-Service provision and workflow;
   D. Logging, monitoring and reporting;
   E. Hybrid Identity and Access Management.

2. The bidder shall be responsible to configure and implement default and customized policies, policy fine tuning and monitoring as per SECP requirements.

3. The bidder /Principal shall provide maintenance and support for one (01) Year.

4. The bidder shall prepare and provide following documents: Guides /Manuals (will be part of the contract):

   A. Administration;
   B. Policy Management and Fine Tuning; and
   C. Reporting.

5. The bidder shall provide /arrange professional instructor-led, hands on training of the proposed solution for Administrators, End Users.

6. Final Requirements and Evaluation Criteria:

1	Total Marks in addition to GOOD TO HAVE requirements	40
2	Minimum Marks in addition to MUST requirements	50%

Technical bid found in compliance to all the MUST requirements and securing 50% marks shall only be considered qualified for financial bid opening and at par/equivalent. Bid found lowest in financial bid opening shall be selected.

APPENDIX A – IDENTITY AND ACCESS MANAGEMENT SYSTEMS SPECIFICATIONS

SECP requires a comprehensive solution with a full complement of IDG, IAM, Self-Service provision and workflow with logging, monitoring and reporting capabilities to meet current and future needs of users, external resources and guests.

1. IDENTITY GOVERNANCE (IDG)

1.1. Attestation / Access Certification

Sn.	Description	Requirement
1	The solution provides account certification/attestation engine	MUST HAVE
2	The solution provides "Risk" based access certification	MUST HAVE
3	The solution provides the certification of account privileges as well as roles	MUST HAVE
4	The solution supports access certifications be performed in bulk	MUST HAVE
5	The identity governance (IDG) solution should be part of the Identity Management and Access (IAM) solution	MUST HAVE
6	User certification task should be accessible from the same user self-service console as the proposed Identity Management and Access (IAM) solution	MUST HAVE

1.2. Role Mining / Rule Management

Sn.	Description	Requirement
1	The solution supports roles-based access control (RBAC)	MUST HAVE
2	The solution supports role mining and rule mining	MUST HAVE
3	The solution provides a workflow engine for role creation	MUST HAVE
4	The solution provides roles nesting	MUST HAVE
5	The solution provides association of metadata with roles	MUST HAVE

1.3. Identity Lifecycle Management (ILM)

Sn.	Description	Requirement
1.	The solution provides unique identifier –unique, unchangeable identifier associated with each identity maintained. If a user leaves and later returns to the Organization in a former or new role, the same original unique identifier is used.	MUST HAVE
2.	The solution provides a centralized identity directory/repository that supports multiple concurrent identity-related roles and affiliations and stores both current and historical data	MUST HAVE
3.	The solution provides an extensible identity directory/repository schema that allows the solution to capture additional user-defined roles, attributes, and metadata, above and beyond the vendor's standard identity repository	MUST HAVE
4.	The solution can accept/capture identity and entitlement data using REST Services, SOAP Services or plain text file.	MUST HAVE
5.	The solution's platform supports dynamic linking of accounts	MUST HAVE

6.	The solution provides includes methods for matching an identity to disparate applications, user accounts and entitlements	MUST HAVE
7.	The solution provides the ability to migrate, consolidate and/or leverage pre-existing unique identifiers in the new IAM directory/identity repository	MUST HAVE
8.	When an identity-related change occurs in a non-authoritative system or outside of normal IAM processes, the solution provides a mechanism for reconciling connected (source or target) systems	MUST HAVE
9.	The solution provides flexible views and management - the identity directory/repository data may be filtered, sorted, viewed and managed in a variety of ways, based upon defined access permissions for administrators, department designees, or others	MUST HAVE
10.	The solution provides method for identifying orphaned accounts and for allowing an administrator to flag the account for remediation	MUST HAVE
11.	The solution provides APIs to allow access to the identity repository data for federated local Authorization	MUST HAVE
12.	The solution provides the ability to detect identity life cycle events as they occur in an authoritative source and transform them into add, modify or delete events	MUST HAVE
13.	The solution provides ability to Individual/Department sponsorship for nonemployee can be added by designees via granular access to the system	MUST HAVE
14.	The solution has the ability to connect to multiple authoritative sources for identity creation, maintenance and de-activation	MUST HAVE
15.	The solution provides Manual entry capability for ILM events - Ability for administrators to directly create, update or remove identities and associated identity attributes in the identity repository	MUST HAVE
16.	Batch-driven identity life cycle events are supported – the ability to import identity data files that have been extracted from an authoritative source into the identity repository, for both full batch processing (entire identity record is replaced) and change-log batch processing (only affected identity attributes are updated)	MUST HAVE
17.	The solution provides ability for both On-premise and Cloud-hosted authoritative sources are able to be leveraged for ILM event detection and synchronization	MUST HAVE
18.	The solution supports Single Sign-On capabilities including SAML, Header, Token or Form Based or any other integration type.	MUST HAVE

2. ACCESS MANAGEMENT (AM)

2.1. Authentication and Authorization

Sn.	Description	Requirement
1	The solution provides authentication and authorization for applications	MUST HAVE
3	The solution supports session timeout for idle sessions	MUST HAVE
4	The solution supports global idle session timeout	MUST HAVE
5	The solution supports granular idle session timeout per application	MUST HAVE
8	The solution supports the integration of web authentication with Service Oriented Architecture layer	MUST HAVE
9	The solution supports forms authentication	MUST HAVE
10	The solution supports multi-factor authentication	MUST HAVE

12	The solution provides mobile authenticator on iOS or android	MUST HAVE
13	The solution provides mobile authenticator support authentication via PUSH notification, as a second factor	MUST HAVE
14	The solution supports advanced rules to switch authentication scheme	MUST HAVE
15	The solution supports authentication mechanisms that have support for JAAS, LDAP, Kerberos, Client Certificate	MUST HAVE
16	The solution provides single sign on (SSO) capability for front end of applications and from windows desktops (CTRL+ALT+DEL)	MUST HAVE
17	The solution provides access portal to support Single Sign on (SSO) to on-premise and cloud applications	MUST HAVE
18	The solution provides cross domain single sign on (SSO) without using federation	MUST HAVE
19	The solution provides integration with external authentication providers such as Google, Facebook, Yahoo, Twitter	MUST HAVE
20	The solution provides secure token services for token translation	MUST HAVE
21	The solution supports fine grained authorization for external applications	MUST HAVE
22	The solution provides centralized Policy Administration Point (PAP)	MUST HAVE
23	The solution supports Policy Enforcement Point (PEP) to work in offline mode	MUST HAVE
24	The solution supports LDAP or RDBMS as policy store	MUST HAVE
25	The solution supports for XACML standard 2.0 and 3.0	MUST HAVE
26	The solution supports out of the box integrations with WebLogic, WebSphere, JBoss, Tomcat, .NET and SharePoint	MUST HAVE
27	The solution enforces web services security from within a service bus	MUST HAVE
28	The solution secures a web services endpoint based on fine grained authorization policies	MUST HAVE
29	The solution secures SharePoint documents based on attributes	MUST HAVE
30	The solution supports authorization of objects structured as hierarchy	MUST HAVE
31	The solution supports: 1. Context attributes 2. Resource attributes 3. Action attributes 4. Identity attributes	MUST HAVE
32	The solution supports central repository for Access Control Policies	MUST HAVE
33	The solution supports multi-vendor directory, for example: 1. Active Directory 2. Oracle Directory Server Enterprise Edition 3. Open LDAP 4. Any LDAP v3 compliant directory	MUST HAVE
34	The solution authenticates users against multiple identity stores	MUST HAVE
35	The solution supports definable security roles on per-resource basis as well as globally	MUST HAVE
36	The solution supports pre and post authentication rule	MUST HAVE
37	The solution supports policy evaluation ordering	MUST HAVE

2.2. Password Management

Sn.	Description	Requirement
1.	The solution provides an option to set the initial password for user accounts and force the user to change the password upon first login	MUST HAVE

2.	The solution enforces all typical password policy constraints, including password expiration, password length, password history, complexity, and restrictions against dictionary words, repeating characters, sequential characters, use of full or partial names, etc.	MUST HAVE
3.	The solution supports password recovery using customizable knowledge-based security questions	MUST HAVE
4.	The solution supports a locally configurable number of security questions the user MUST HAVE establish	MUST HAVE
5.	The solution includes an “option” to force users to establish security questions at the time of account claiming or first logon	MUST HAVE
6.	The solution supports options for streamlined, early (yet secure) account claiming and activation process for new hires.	MUST HAVE
7.	The solution supports password aging and warning	MUST HAVE
8.	The solution supports password composition rules	MUST HAVE
9.	The solution supports password history enforcement	MUST HAVE
10.	The solution supports one-time passwords (OTP)	MUST HAVE
11.	The offered solution should have ability to manage privilege passwords independently and offer multiple password policies management options.	MUST HAVE
12.	The solution should be able to automatically discover privilege passwords, service accounts and generate a report regarding state of security of these credentials.	MUST HAVE
13.	Solution should be able to automatically discover privileged credentials on the target and can import these credentials to start managing it	MUST HAVE

2.3. Session Management

Sn.	Description	Requirement
1	The solution supports both stateful and cookie-based session management	MUST HAVE
2	The solution supports detailed security context information in stateful sessions and further propagation	MUST HAVE
3	The solution provides high performance distributed caching	MUST HAVE
4	The solution provides admin to specify session lifetime	MUST HAVE
5	The solution supports automatic session failover	MUST HAVE
6	The solution provides admin to specify session limit	MUST HAVE
7	The solution supports out-of-band session termination to prevent unauthorized access to systems when a user has been terminated	MUST HAVE
8	The solution supports persistent login with unique token to device/browser	MUST HAVE
9	The solution provides admin UI to monitor and control active sessions	MUST HAVE

2.4. Federation

Sn.	Description	Requirement
1	The solution supports WS-Federation and SAML 1.1/2.0	MUST HAVE
2	The solution support OAuth 1.0/2.0 and OpenID	MUST HAVE

3	The solution supports 2-legged and 3-legged architecture	MUST HAVE
4	The solution supports federated single sign on (SSO) and global logout	MUST HAVE
5	The solution supports attribute mapping without the need to write custom code	MUST HAVE
6	The solution supports importing of federation metadata and then editing it in the administrative GUI	MUST HAVE
7	The solution supports SAML attribute query	MUST HAVE
8	The solution supports name-id mapping without customization or coding	MUST HAVE
9	The solution supports hierarchical policy enforcement and management i-e enterprise policy, domain policy, group policy, etc	MUST HAVE
10	The solution supports role and rule-based authorizations	MUST HAVE
11	The solution provides authorizations decisions based on attributes stored in an external repository such as RDBMS/LDAP/Web Services	MUST HAVE

2.5. Directory Services

Sn.	Description	Requirement
1	The directory services scales into tens of millions while supporting low response times (<20 ms).	MUST HAVE
2	The directory supports unlimited multi-master replication	MUST HAVE
3	The directory supports multi master replication over a WAN	MUST HAVE
4	The directory supports fractional replication	MUST HAVE
5	The directory services provide a virtual directory	MUST HAVE
6	The solution synchronizes passwords and other attributes with Active Directory without installing any agent or DLL on the Domain Controller	MUST HAVE
7	List all the LDAP RFC supported by your directory services.	MUST HAVE

2.6. Access Management Deployment

Sn.	Description	Requirement
1	The solution supports consolidated name space behind a reverse proxy, that allows users to remember a single URL (extranet.example.com) instead of a unique URL per application.	MUST HAVE
2	The solution supports web-based access control for users through industry standard browsers e.g., Internet Explorer, Firefox etc	MUST HAVE
3	The solution provides methods of redundancy/high availability for hosted websites	MUST HAVE
4	The solution provides features to perform load balancing on its own and should be able to work behind any external load balancing methods such as F5 switches.	MUST HAVE
5	The solution provides protection for internal applications via reverse proxy	MUST HAVE
6	The solution supports IPv6 for all client-server communications	MUST HAVE
7	The solution supports IP-based conditions for authorization policies	MUST HAVE
8	The solution provides strong encryption for the Web access components, e.g. SHA-2	MUST HAVE
9	The solution supports cookie encryption and unique host scoping	MUST HAVE
10	The solution supports authorization caching	MUST HAVE

11	The solution operates within and supports multiple data centres (active-active environment)	MUST HAVE
12	The solution supports automated replication of policies and configuration from master to clones	MUST HAVE
13	The solution provides independency from how applications are deployed	MUST HAVE
14	The solution supports customizable error pages	MUST HAVE

2.7. Access Management Security

Sn.	Description	Requirement
1	The solution supports secured communication between different components of the solution using SSL/TLS	MUST HAVE
2	The solution provides a credential collector so that solution can be deployed in DMZ	MUST HAVE
5	The solution supports proactive real-time fraud detection and prevention during authentication as well as transactions. This includes but not limited to 1. Risk Based Scoring 2. Anti-Phishing 3. Anti-Malware	MUST HAVE

Sn.	Description	Requirement
1.	The solution provides ability to track admin sessions when the admin logs in.	MUST HAVE
2.	The solution provides ability to record those admin sessions.	MUST HAVE
3.	The solution provides ability to archive admin sessions for auditing purposes.	MUST HAVE
4.	The solution provides ability to search session audit logs and recordings for specific activity (by user, by system, by type of action performed).	MUST HAVE
5.	The solution provides ability to integrate with SIEM with logs.	MUST HAVE
6.	The solution provides ability to integrate with platforms, such as AD and LDAP	MUST HAVE
7.	The solution should have ability to work in both agent-based and agent-less mode	MUST HAVE
8.	The solution should be able to secure save the session recordings from privileged users and encrypt these recordings on database as well as storage drives.	MUST HAVE
9.	The solution should have ability to record privilege users screen activity as well as activities performed by automated scripts on the backend.	MUST HAVE
10.	The solution should have ability to manage privilege passwords independently and offer multiple password policies management options.	MUST HAVE
11.	The solution should be able to automatically discover privilege passwords, service accounts and generate a report regarding state of security of these credentials.	MUST HAVE

12.	The solution provides should have ability to capture keystrokes, processes and tools that PAM users uses during their session.	MUST HAVE
13.	The solution should be able to automatically discover privileged credentials on the target and can import these credentials to start managing it	MUST HAVE

3. SELF-SERVICE, PROVISIONING AND WORKFLOW

3.1. Self-Service Features

Sn.	Description	Requirement
1.	The solution provides Self-service request engine	MUST HAVE
2.	The solution provides self-service and delegated identity administration, for both new and existing users	MUST HAVE
3.	The solution provides self-service password reset including forgotten password reset, by passing challenge response questions or providing authentication information using second factor.	MUST HAVE
4.	The solution provides a user friendly “Services inventory” for self-service request portal.	MUST HAVE
5.	The solution provides a user-friendly self-service request catalogue. This catalogue provides the types of items a user can request (e.g. roles, entitlements, permissions, systems, etc.) and provides ability to view access request status	MUST HAVE
6.	The solution supports Request Profiles i.e. group of similar permissions, roles or accounts to facilitate end users to request for profile rather searching for individual items. The solution should be capable of identifying dependencies &/or parent/child relationships to facilitate identification & request of all roles needed.	MUST HAVE
7.	The solution supports customization of end-user forms (e.g. user, resource, role, etc.).	MUST HAVE
8.	The solution provides the ability to view the workflow steps of a given access request, including the ability to identity the appropriate approver	MUST HAVE
9.	The solution provides the ability for requestor or approver to enter effective dates (start and end) for the requested access	MUST HAVE
10.	The solution provides the ability to Approvers to approve, reject, or modify access requests at fine grained levels	MUST HAVE
11.	The solution provides auditing and reporting features available on Self Services	MUST HAVE

3.2. Provisioning and Deprovisioning

Sn.	Description	Requirement
1	The solution supports for automated provisioning and de-provisioning of a user’s access rights.	MUST HAVE
2	The solution should have Out-of-box Connectors available for known packaged applications beside other platform connectors like LDAP-directory connectors, database connectors, Unix/Linux connectors etc.	MUST HAVE

3	The solution provides out of the box connectivity with following minimum services: 1. Active Directory 2. Open LDAP 3. Database (Table) based user management system 4. Tivoli LDAP Server	MUST HAVE
4	The solution provides identity and account reconciliation process.	MUST HAVE
5	The solution provides de-provisioning process. Deletion of account or disabling of account with notification to user	MUST HAVE
6	The solution maps identity attributes to corresponding account attributes for provisioning	MUST HAVE
7	The solution supports de-provisioning of accounts based on an HR termination events from HR	MUST HAVE
8	The solution captures the logon date/ time for the account for a definable period	MUST HAVE
9	The solution captures the last logon date/ time for the account before de-provisioning	MUST HAVE
10	The solution provides date/ time-based provisioning	MUST HAVE

3.3. Workflow

Sn.	Description	Requirement
1.	A workflow engine and workflow processing should be included, as part of the IAM solution offering with a web-based user-friendly interface for managing all work list items and shows history, status, and progress etc.	MUST HAVE
2.	The solution provides approval base workflows for provisioning and de-provisioning of users	MUST HAVE
3.	The solution supports the ability to import application roles, or responsibilities, from HRMS	MUST HAVE
4.	The solution provided workflow engine supports attachments of known format i.e. Microsoft Office doc format, Pictures/ PDF doc	MUST HAVE
5.	The solution provided workflow engine includes a graphical editor	MUST HAVE
6.	The solution supports template-based workflows for user account creation, management, group assignments, de-activation and deletion etc. A set of predefined workflow templates, that can be modified, is provided	MUST HAVE
7.	The solution supports workflow escalation based on configurable response time windows or a per workflow basis function	MUST HAVE
8.	The solution supports email notifications/alerts to specific accounts or groups of accounts for certain activities performed by the identity management system	MUST HAVE
9.	The solution supports request-driven workflows initiated by authorized users for activities like activation, de-activation, including approvals	MUST HAVE
10.	The solution supports event-driven account de-activation (i.e. not deletion) with or without workflow approval	MUST HAVE
11.	The solution supports event-driven account re-activation with or without workflow approval	MUST HAVE
12.	The solution supports the removal of accounts from target systems / applications	MUST HAVE

13.	The solution provided workflow engine supports integration with external applications and services (e.g. outbound calls) via Web services, APIs, etc., with the ability to accept return codes, process data and monitor the status of activity from the external application	MUST HAVE

4. LOGGING, MONITORING AND REPORTING

4.1. Logging and Monitoring

Sn.	Description	Requirement
1	The solution provides different level of logging (event, errors, warnings) and ability to logging, tracing and turn on configuration settings per component	MUST HAVE
2	The solution provides quick troubleshooting of issues with structured messaging, and enables dynamic tracing without restarting the application	MUST HAVE
3	The solution provides running of reports on system	MUST HAVE
4	The solution provides logging of administrative tasks	MUST HAVE
5	The solution supports logging of contextual information about user access such as connecting device and location	MUST HAVE
6	The solution maintains logs of user activity and behaviour and supports monitoring against patterns and configurable risk-based policies	MUST HAVE
7	The solution supports different options of viewing log files such as web-based monitoring console, command line utilities or downloadable log files to be viewed by external tools	MUST HAVE
8	The solution provides a diagnostic framework that can help in detecting, diagnosing and resolving problems	MUST HAVE
9	The solution automatically and continuously measures run-time performance	MUST HAVE
10	The solution provides tools and utilities to support performance analysis and diagnostics	MUST HAVE
11	The solution provides monitoring capabilities to send out alerts (e.g. SNMP)	MUST HAVE
12	The solution provides a web-based system administration and monitoring dashboard for system components	MUST HAVE
13	The solution provides rolled up summary information on dashboard such as availability of all components and application deployment summary; as well as ability to drill down into more details such as request and load processing charts, service uptime information, throughput and resource usage (such as CPU and memory)	MUST HAVE

4.2. Usage and Reporting

Sn.	Description	Requirement
1.	The solution provides detailed usage report that include end user authentication events including successful logons	MUST HAVE
2.	The solution provides detailed usage report that include filters for different user categories such as external organizations and networks	MUST HAVE
3.	The solution provides detailed user account reports that include breakdown of different user account events such as accounts created, accounts deleted,	MUST HAVE

	accounts disabled, accounts enabled, accounts locked out and password changes	
4.	The solution provides detailed user account reports that include breakdown of different user services types such as password resets, self-service requests and certifications	MUST HAVE
5.	The solution creates dashboards to display summary of end user usage and activities	MUST HAVE
6.	The solution supports categorization and configuration of different types such as agencies, applications, risk level, etc in summary dashboards and reports	MUST HAVE
7.	The solution supports extendable and customizable reports based on usage and activity of end users	MUST HAVE
8.	The solution provides scheduling and distribution of reports	MUST HAVE
9.	The solution supports different report formats such as HTML, PDF, RTF and MHTML	MUST HAVE
10.	The solution supports configuration or customization of usage and activity reports using web-based UI or familiar tools such as Word or Excel	MUST HAVE
11.	Ability to maintain a historical snapshot of identity data and report on a user's access at any time	MUST HAVE
12.	A comprehensive set of predefined audit reports on common security-related functions are provided	MUST HAVE
13.	Audit reports can be scheduled to run at particular times and intervals, upon particular events, or upon demand	MUST HAVE
14.	Dormant or inactive account detection capability exists	MUST HAVE
15.	Provides the ability to restrict what data elements are available to the third-party reporting tool	MUST HAVE

4.3. Identity Reporting

Sn.	Description	Requirement
1	The solution provides a central reporting engine across all of its components (provisioning, access, federation, directory etc.)	MUST HAVE
2	The solution provides out of the box, as well as customizable reports	MUST HAVE

5. SYSTEM SPECIFICATIONS

5.1. Swift installation, configuration and operation

Sn.	Description	Requirement
1.	The solution provides ability to full install, configure, and operational onsite at user facility	MUST HAVE
2.	The solution provides an install wizard, for deployment of the software	MUST HAVE
3.	The solution is configurable for high availability (e.g. the system architecture supports standard industry concepts of redundancy, synchronization across redundant components, DR, and high availability monitoring)	MUST HAVE

4.	The solution includes a mechanism for strong authentication/MFA for administrators	MUST HAVE
5.	The solution supports SAML integrations for Single Sign On and has been proven to work with multiple partners.	MUST HAVE
6.	The solution includes integration APIs to allow third-party systems to access IAM data and functions	MUST HAVE
7.	The solution includes a robust set of configurable system security policies to ensure fine-grained security controls that restrict access to data and functions in the system	MUST HAVE

5.2. Integration and Internationalization

Sn.	Description	Requirement
1.	The solution supports customized JSP changes for internationalization	MUST HAVE
2.	The solution integrated suite that provides: 1. Federation 2. Web Access Management 3. Secure Token Services 4. RESTful web services 5. Policy Administration	MUST HAVE
3.	The solution provides a single Administrative and Monitoring Console	MUST HAVE
4.	The solution supports integration with identity manager to enforce dormant account policy	MUST HAVE

5.3. Performance and Scalability

Sn.	Description	Requirement
1	The solution provides caching ability for authentication and authorization decision at the Policy Enforcement Point (Agent)	MUST HAVE
2	The solution provides ability to expand both horizontally and vertically to meet the need of growing applications	MUST HAVE
3	The solution provides built in functionality or features to take advantage of available server resources when required. Example Product should not be restricted to one CPU and should be able to use other CPU cycles available on the server when load increases for CPU processing.	MUST HAVE

5.4. Availability and Support

Sn.	Description	Requirement
1	The solution provides a highly available environment (>99.9 %) and ability to function without periodic restarts	MUST HAVE
2	The solution provides 24x7 support Online or email. Only support for off hours is not acceptable	MUST HAVE

3	The solution provides quick response time for problem tickets (< 2hrs for severity 1 tickets, <6 hours for Severity 2 tickets, one business day for severity 3 tickets)	MUST HAVE
4	The solution provides online product documentation / information library / tech WIKI and online video presentations and training	MUST HAVE
5	The solution provides product release notes and white papers available online	MUST HAVE

6. HYBRID IDENTITY AND ACCESS MANAGEMENT

Sn.	Description	Requirement
1	The solution integrates an on-premise IAM solution with the vendors own cloud IAM solution and supports hybrid IAM	GOOD TO HAVE
2	The cloud solution supports System for Cross-domain Identity Management (SCIM) Identity Provider for user management	GOOD TO HAVE
3	The cloud solution provides self-service based profile and password management	GOOD TO HAVE
4	The cloud solution provides a consistent admin interface for User, Group and Bulk Load Management	GOOD TO HAVE
5	The cloud solution acta as an OAuth Token Broker	GOOD TO HAVE
6	The cloud solution acts as a SAML Assertion Broker	GOOD TO HAVE
7	The cloud solution supports federated SSO using SAML2.0, OAuth2.0 and OpenID Connect 2.0	GOOD TO HAVE
8	The cloud solution supports SSO between Oracle Public Cloud, External SaaS, On-premise and custom applications	GOOD TO HAVE
9	The cloud solution integrates with on premise access management for federated authentication	GOOD TO HAVE
10	The cloud solution acts as a SAML IDP and OpenID Connect Provider	GOOD TO HAVE
11	The cloud solution provides a single administration and end user view of connected applications	GOOD TO HAVE
12	The cloud solution integrates with applications on PaaS and IaaS	GOOD TO HAVE
13	The cloud solution integrates with on-premise Identity Access Management	GOOD TO HAVE
14	The cloud solution supports OpenID Connect for browser-based user authentication	GOOD TO HAVE
15	The cloud solution supports OAuth2 for securing REST API calls	GOOD TO HAVE
16	The cloud solution supports HTTP cookies for tracking user's active session	GOOD TO HAVE
17	The cloud solution supports JWT-based tokens for applications to map authenticated cloud identity into local application identity	GOOD TO HAVE
18	The cloud solution supports SAML for providing SSO for Cross Domain applications	GOOD TO HAVE
19	The cloud solution supports SCIM to simplify user management in the cloud	GOOD TO HAVE

20	The cloud solution provides RESTful APIs for all identity functions for customization and headless operations	GOOD TO HAVE
21	Multi-tenanted and highly scalable based on Microservices architecture cloud solution	GOOD TO HAVE
22	The cloud solution uses a Cloud Directory for Cloud Apps	GOOD TO HAVE
23	The cloud solution supports multi factor authentication	GOOD TO HAVE
24	The cloud solution supports hybrid integration with on-premise IDM system	GOOD TO HAVE
25	The cloud solution supports customer branding through configuration	GOOD TO HAVE

NOTE:

1. The bidders **MUST** submit a compliance sheet against all requirements mentioned in the technical evaluation criteria
2. Bids NOT in compliance with any MUST items in the evaluation criteria will NOT be evaluated

FORMAT FOR TECHNICAL COMPIANCE SHEET

SR	ATTRIBUTE	SPECIFICATION	COMPLIANCE (YES/NO/ PARTIAL)

7. APPENDIX B – BIDDER FIRM -MANDATORY REQUIREMENTS

1. Bidder MUST have local Presence and offices at Islamabad/Rawalpindi
2. Manufacturer authorization letter for participation in tenders
3. The bidder MUST have performed minimum three **03** local or international similar deployments (Please attach relevant document(s) as proof)
4. Bidder MUST have at-least three (03) years' experience of similar deployments. (Please attach relevant document(s) as proof)
5. Bidder MUST have at least 2 certified resources of the proposed solution.

Note: Non-provision of any above required information in the bid shall lead to rejection of the bid.

1. Training Details

Selected bidder shall provide/arrange professional instructor led, hands on training of administrators:

a. The training should include the architecture, hardware, software, integration, and customization, policy installation, troubleshooting reporting and other aspects of the solution.
b. The Bidder shall train SECP personnel for independent operation, creation of policies /rules, generation of reports, and analysis of the reports, troubleshooting and familiarization of features and functionalities, policy configuration, alert monitoring etc. post implementation
c. Bidder should submit detailed course content and provisional agenda along with the bid.

2. Project Activities

1	Deployment of solutions in SECP HO Data Centre & SECP Disaster Recovery Centre and all relevant clients	Installation & Configuration of Controls, Policies & Access rules etc.
2	Reporting & Dashboards	Configuration of real time performance dashboard Daily, Weekly & Monthly reports
3	DR Readiness	Configuration and testing with DR perspective
4	Documentation	Design Documents, SOPs, User /Configuration /Admin Manuals
5	Trainings	Trainings for at least 04 participants as mentioned in training details

3. Project Management

1	Start of the Project	a	Presentation from the vendor at SECP HO, explaining the comprehensive project plan that includes tasks, procedures, tools, timelines, impacts, responsible persons, and report formats (Microsoft PowerPoint)

2	Middle of the Project	a	Weekly progress report on all tasks (Microsoft Excel /Project)
3	End of the Project	a	A detailed report covering the overall progress of the project
		b	A consolidated product deployment report covering the whole commitment, including different tests results and recommendations about best practices
		c	An executive-level presentation from the vendor at SECP HO explaining the project results and final reports (Microsoft PowerPoint)

General Requirements and Evaluation Criteria

Sn.	Requirement	Criteria	Compliance	Comments
1	Complete compliance with SOW, Functional requirements, Training requirement, Project Activities and Project Management			
2	The service provider should have delivered and deployed similar solutions in public or private sector. Work order from at least 01 client should be attached as proof with contact details of reference. The feedback may be obtained from the reference provided.			
3	The service provider should have at least one (01) certified resource of the solution with minimum of 02 years' experience of the offered product. Attach copy of all relevant certificates as proof.			
4	The bidders MUST submit a technical compliance sheet against all requirements mentioned in the Functional and General evaluation criteria			
5	Professional hands on and instructor led training for at least four (04) resources of the offered solution(s)			
6	Gartner Magic Quadrant 2019 /2020 rating of offered solution (Challengers & Leaders only), attach proof			
7	Principal Authorization Letter for Tender Participation			
8	Valid Partnership Letter with Principal/ Manufacturer			
9	Annual technical support from the Principal included with the license			

NOTE:

1. The bidders **MUST** submit a compliance sheet against all requirements mentioned in the technical evaluation criteria
2. Bids NOT in compliance with any MUST items in the evaluation criteria will NOT be evaluated