Annexure F: Technical Compliance

All the requested services in the scope are to be provided by the bidder. All the clauses which are Mandatory are to be complied for successful qualification.

#	Category	Requirement Description	Mandatory/ Desirable	Evidence	Compliance	Remarks
1	Access Certification	The identity and access management solution should provide the history of certification decisions previously made on entitlements and roles.	Mandatory			
2	Access Certification	The identity9 and access management solution should display each user's risk profile within the certification report as additional context for reviewers.	Mandatory			
3	Access Certification	The identity and access management solution should highlight privileged user accounts and other high-risk accounts (e.g., service accounts) during the certification process.	Mandatory			
4	Access Certification	The identity and access management solution should provide an administrative dashboards and reports to track aggregated certification metrics across the enterprise and certification campaigns.	Mandatory			
5	Access Certification	The identity and access management solution should provide an option to support bulk remediation for all former employees' access privileges prior to beginning an access certification, thereby reducing the workload of reviewers.	Mandatory			
6	Access Certification	The identity and access management solution should provide capability to automatically forward/assign work items to a manager or application owner if the person leaves the company during an access certification.	Mandatory			
7	Access Certification	The identity and access management solution should provide capability, when certifiers review a user's access privileges,	Mandatory			

#	Category	Requirement Description	Mandatory/ Desirable	Evidence	Compliance	Remarks
		can they approve, revoke or allow exceptions.				
8	Access Certification	The identity and access management solution should provide historical information included in active certifications to help reviewer determine the appropriateness of access.	Mandatory			
9	Access Certification	The identity and access management solution should provide user access certifications be set up to auto-generate on a periodic cycle.	Mandatory			
10	Access Certification	The identity and access management solution should provide visibility to certification activities (e.g., completion status) on a user's dashboard.	Mandatory			
11	Access Certification	The identity and access management solution should send automatic notifications be generated and sent out to certifiers when a new certification is created. Does the application support the ability to send reminder notifications periodically during an active certification?	Mandatory			
12	Access Certification	The identity and access management solution should support automated report routing to the appropriate certifiers.	Mandatory			
13	Access Certification	The identity and access management solution should support delegation of users to another certifier.	Mandatory			
14	Access Certification	The identity and access management solution should support filtering of users during a certification to simplify and speed completion (e.g., filter users by customer-defined attributes, entitlements, business roles).	Mandatory			
15	Access Certification	The identity and access management solution should support where identity attributes such as HR data and user risk profiles be used to	Mandatory			

#	Category	Requirement Description	Mandatory/ Desirable	Evidence	Compliance	Remarks
		automatically define populations of users for certification.				
16	Access Certification	The Identity management solution should ensure that internal employees do not aggregate access as they move throughout the organization and that both internal and external users do not retain access when their relationships with the organization end.	Mandatory			
17	Access Certification	The Identity management solution should facilitate for scheduling access reviews to ensure, users are assigned the minimum access necessary to do their jobs. The access certification should trigger based on events triggered by new hires, transfers, promotions, or terminations.	Mandatory			
18	Access Certification	The Identity management solution should handle remediation when revoking entitlements and accounts during a certification process.	Mandatory			
19	Access Certification	The Identity management solution should report on certification status, policy violations, and other access-related information while reducing the need to manually gather this type of data for compliance and audit purposes.	Mandatory			
20	Access Certification	The Identity management solution should support these certification types - manager certifications, application owner certifications, user certifications, access certifications etc.	Mandatory			
21	Access Certification	The Identity management system should provide following Access Certification capabilities. - Access Certification Workflow - User access review and certification - Resource review and certification	Mandatory			

#	Category	Requirement Description	Mandatory/ Desirable	Evidence	Compliance	Remarks
		- Role review and certification - Accounts and entitlement review and certification - Scope access review - Flexible scheduling - Ad-hoc certification - Full certification - Highlight privileged or high-risk accounts and entitlements - Status reports and dashboards - Access History - Bulk or “approve all” feature - Required Criteria Evaluated/Score: - Support for Orphaned accounts - Continuous (micro) certification - Challenge period - Risk score display - Outlier detection - Recommendation engine - Mobile optimized access certification - Integration with fulfilment engine - Certify privileged user access via integration with PAM solutions				
22	Auditing & Logging	The Identity management solution should ensure that provisioning activities are recorded for audit purposes.	Mandatory			
23	Auditing & Logging	The Identity management solution should facilitate for the actions performed by all users of the system are audited, the system should timestamp all actions logged and audited.	Mandatory			
24	Auditing & Logging	The Identity management system should provide following Auditing capabilities - Log identity events - Protection and tamper-resistance of audit log - Maintain historical data - Define audit policies - Support for multiple audit policy types - Policy violation handling and corrective controls	Mandatory			

#	Category	Requirement Description	Mandatory/ Desirable	Evidence	Compliance	Remarks
		- Alerts - Notifications - Workflow - Autocorrect - Assign respondents - Complex SOD policy handling - Audit dashboard - Audit of automated events as a result of identity analytics and machine learning decisions				
25	Compliance Management	The identity management solution should ensure the ability to enforce compliance with industry regulations and standards such as SOX, PCI-DSS, GDPR and IRDAI.	Mandatory			
26	Compliance Management	The identity management solution should have predefined compliance controls, policies, and reports.	Mandatory			
27	Identity & Access Intelligence and Reporting	The identity and access management solution should allow users to set specific parameters when running reports and should allow configuration of reports be saved for later recall.	Mandatory			
28	Identity & Access Intelligence and Reporting	The identity and access management solution should provide a report which outlines defined security risks by application.	Mandatory			
29	Identity & Access Intelligence and Reporting	The identity and access management solution should provide a way to search on activity information according to various search parameters related to the system/activity and the target user base. For example, show all login activity on application Y for users in cost centre 1139 with risk scores over 600.	Mandatory			
30	Identity & Access Intelligence and Reporting	The identity and access management solution should provide capability for identifying and managing orphan accounts.	Mandatory			

#	Category	Requirement Description	Mandatory/ Desirable	Evidence	Compliance	Remarks
31	Identity & Access Intelligence and Reporting	The identity and access management solution should provide pre-defined reports out-of-the- box.	Mandatory			
32	Identity & Access Intelligence and Reporting	The identity and access management solution should provide report scheduler that allows user-specified reports to be run on a regularly scheduled basis and results should be automatically sent via email.	Mandatory			
33	Identity & Access Intelligence and Reporting	The identity and access management solution should provide reports that are targeted towards proving compliance with various regulatory requirements (e.g., SOX, HIPAA, Basel II, PCI).	Mandatory			
34	Identity & Access Intelligence and Reporting	The identity and access management solution should support saving reporting results in downloadable file formats (e.g., PDF, Excel or CSV).	Mandatory			
35	Identity & Access Intelligence and Reporting	The Identity management system should provide following ID Analytics & Reporting capabilities - Comprehensive library of default reports - Customizable reports - Filter report - Time and ad-hoc scheduling of report execution - Export report to CSV or HTML format - IGA dashboard - Default dashboard metrics - Create IGA report with third-party reporting tool - Dormant account detection - Risk-based policies - Methods for risk-score calculation - Static risk-score evaluation - Dynamic risk-score evaluation - External risk-score evaluation - Identity analytics dashboard for account	Mandatory			

#	Category	Requirement Description	Mandatory/ Desirable	Evidence	Compliance	Remarks
		correlation and application onboarding - Capability to Build custom reports - Dashboard filters - Capability to restrict third-party access to identity data - Peer-group analysis and outlier detection - Threat response through behavioural analytics integration - Integration of identity analytics with access request and access certification processes - Integration of identity analytics with fulfilment processes - Advanced visualization capabilities - Offline reporting - Integrate identity data and processes with security analytic systems - Support for Native machine learning				
36	Risk Modelling	The identity and access management solution should aggregate risk scores and display it graphically for easy identification of risk "hot spots".	Mandatory			
37	Risk Modelling	The identity and access management solution should allow to identify high-risk users via reporting and analytics.	Mandatory			
38	Risk Modelling	The identity and access management solution should allow to view risk scores on demand as part of each user's identity information.	Mandatory			
39	Risk Modelling	The identity and access management solution should dynamically calculate a user's risk score based on changes to access within the environment.	Mandatory			
40	Risk Modelling	The identity and access management solution should profile aggregate risk scores, e.g., by manager, department, location, or company wide.	Mandatory			

#	Category	Requirement Description	Mandatory/ Desirable	Evidence	Compliance	Remarks
41	Risk Modelling	The identity and access management solution should recommend risk mitigation actions for high-risk users, such as activity monitoring, ad-hoc certifications, or remediation of policy violations.	Mandatory			
42	Risk Modelling	The identity and access management solution should support configurable risk factors and weightings for calculating identity or risk scores. Risk scores on access can be used to calculate the overall risk score of an identity within the organization.	Mandatory			
43	Risk Modelling	The identity and access management solution should support the assignment of unique risk values to each application, entitlement and role within the system.	Mandatory			
44	Risk Modelling	The identity and access management solution should track and monitor the risk of each user based on that user's access to sensitive applications and data (identity risk scoring).	Mandatory			
45	Access Requests and Workflow Management	The Identity management should provide capabilities to isolate users and access based on their location, business unity and legal entity.	Mandatory			
46	Access Requests and Workflow Management	The identity management solution should create workflows to reduce the administrative burden of entering, updating, and deleting user information across all systems in the enterprise. These workflows should provide a web-based interface for users to manipulate distributed identity data that triggers workflows as necessary.	Mandatory			
47	Access Requests and Workflow Management	The Identity management solution should enable customization of workflows that are upgrade safe.	Mandatory			

#	Category	Requirement Description	Mandatory/ Desirable	Evidence	Compliance	Remarks
48	Access Requests and Workflow Management	The Identity management solution should have properly defined internal authorization model which can be configured based on business needs.	Mandatory			
49	Access Requests and Workflow Management	The Identity management solution should provide elaborate access governance capabilities.	Mandatory			
50	Access Requests and Workflow Management	The Identity management solution should provide out of the box request based access module with following capabilities - Self-service and delegated administration - Request for IT level Access with integration with leading privileged access management products - Intuitive description of roles and entitlement - Capability to Add, modify and remove access - Request access to roles, entitlements or accounts - Request access to multiple entitlements in one request - Flag high-risk or out-of-compliance requests - Search and browse for roles, entitlements or accounts - Narrow search results by application - Narrow search results by role - Narrow results by user - Customized search - View access request workflow and approver(s) - View access request status - Access request optimized for mobile devices - System provided suggestions - View request history - Single-page, free-form access request - Cancel access requests - Request with effective date	Mandatory			
51	Access Requests	The Identity management solution should provide	Mandatory			

#	Category	Requirement Description	Mandatory/ Desirable	Evidence	Compliance	Remarks
	and Workflow Management	standard/reference workflows.				
52	Access Requests and Workflow Management	The Identity management solution should provide utilities for tracking requests, workflow execution and fulfilment operations.	Mandatory			
53	Access Requests and Workflow Management	The Identity management solution should support delegation of approval requests to other users within the system and this information shall be tracked and audited.	Mandatory			
54	Access Requests and Workflow Management	The Identity management solution should support re-usable workflow sub-processes.	Mandatory			
55	Access Requests and Workflow Management	The Identity management system should provide following workflow capabilities - Independent workflow engine - Central workflow interface and work list - Email notifications - Process monitoring - Reminders - Delegation - Reassignment - Serial processing - Combination of Static and dynamic approval routing - Dynamic approval routing - Static approval routing - Conditional workflow processing - Multiple approvers - Approval escalation based on organizational hierarchy - Integration with external applications and services (outbound approval calls) - Mobile-optimized interface - Return for additional input - Integration with external applications and services (inbound)	Mandatory			
56	Administration	The Identity management solution should provide a GUI for performing manual correlation of user account privileges and support an	Mandatory			

#	Category	Requirement Description	Mandatory/ Desirable	Evidence	Compliance	Remarks
		approval process for the manual correlation of accounts.				
57	Administration	The identity management solution should provide a single point of administration for managing user additions, removals, and updates for all groups across all channels.	Mandatory			
58	Administration	The Identity management solution should provide a web-based interface for administration and configuration of application connectors.	Mandatory			
59	Administration	The identity management solution should provide the user-friendly administration interface which ensures seamless support capability for all administration activity.	Mandatory			
60	Risk Modelling	The identity and access management solution should provide capability where certification status or time since last certification be used as a risk factor in the model.	Mandatory			
61	Alerts and Notifications	The identity and access management solution should provide alerts and send notifications on following cases to end users: - New registration - Profile data update - Password expiry - Password reset - Contact preferences - PII data preferences - Any policy change	Mandatory			
62	Alerts and Notifications	The Identity and access management solution should provide alerts and send notifications on following cases to security or governance team: - Suspicious attempts - Locked out account alerts	Mandatory			
63	Alerts and Notifications	The identity management system should alert administrators and/or re-execute process in case of an error at updating	Mandatory			

#	Category	Requirement Description	Mandatory/ Desirable	Evidence	Compliance	Remarks
		identity information at any environment.				
64	Data Collection/Aggregation & Correlation	Describe how the solution collects user access privileges from enterprise and cloud IT systems, including platforms, databases, directories and business applications (e.g., AD, SAP, Mainframes, UNIX and other applications with different file formats).	Mandatory			
65	Data Collection/Aggregation & Correlation	The identity management solution should allow bulk user upload and aggregate information change at the same time as all users or specified users.	Mandatory			
66	Data Collection/Aggregation & Correlation	The Identity management solution should allow transformation of data and execution of validation rules as part of the data load processing.	Mandatory			
67	Data Collection/Aggregation & Correlation	The Identity management solution should collect/derive the employee/manager relationship from an authoritative identity source, such as the central HR application.	Mandatory			
68	Data Collection/Aggregation & Correlation	The Identity management solution should ensure the communication between graphical interface, central system and servers must be encrypted. All passwords and user account information must be secured during transmission over the network.	Mandatory			
69	Data Collection/Aggregation & Correlation	The Identity management solution should support both automated and manual updates to entitlement metadata.	Mandatory			
70	Data Collection/Aggregation & Correlation	The Identity management solution should support collecting data from enterprise applications based in public or private clouds as well as managing enterprise IT systems deployed in public or private clouds.	Mandatory			

#	Category	Requirement Description	Mandatory/ Desirable	Evidence	Compliance	Remarks
71	Data Collection/Aggregation & Correlation	The Identity management solution should support importing and evaluating activity data (e.g., SIEM feeds and application log files) from target systems.	Mandatory			
72	Data Collection/Aggregation & Correlation	The identity management system should allow transformation of data and execution of validation rules as part of the data load processing.	Mandatory			
73	Data Collection/Aggregation & Correlation	The identity management system should create a single view of each user within the enterprise and their associated access privileges.	Mandatory			
74	Data Collection/Aggregation & Correlation	The identity management system should provide a user interface for performing manual correlation of user account privileges.	Mandatory			
75	Data Collection/Aggregation & Correlation	The identity management system should provide capability to view all user entitlements, roles, policy information and activity data within the context of an individual identity.	Mandatory			
76	Data Collection/Aggregation & Correlation	The identity management system should support following file import options: CSV files Flat files	Mandatory			
77	Data Collection/Aggregation & Correlation	The identity management system should support multiple authoritative sources for identity data.	Mandatory			
78	Data Collection/Aggregation & Correlation	The identity management system should support the collection of data using agent-less connectors.	Mandatory			
79	Entitlements Management	The Identity management solution should include a centralized catalogue of all entitlements in the system.	Mandatory			
80	Entitlements Management	The Identity management solution should provide capabilities to invoke Identity, access and entitlements provisioning on need basis as per manual intervening events.	Mandatory			
81	Entitlements Management	The Identity management system should provide	Mandatory			

#	Category	Requirement Description	Mandatory/ Desirable	Evidence	Compliance	Remarks
		following entitlements management capabilities - Capture entitlement data using comma-separated values (CSV) files - Entitlement discovery using connectors - Identity and account correlation - Static linking - Dynamic linking - Discover and correlate orphaned accounts - Discover and correlate privileged accounts - Multiple application instances or accounts - Account classification and metadata - Administrative dashboard for entitlements - Anomalous entitlement detection - Application inventory - Correlate identities and accounts using account claiming - New entitlement recognition				
82	Entitlements Management	The Identity management system should provide role and entitlement mining capabilities.	Mandatory			
83	Identity Lifecycle Management	The identity and access management solution should provide ability to remove employee access when they leave organization or long leave, information flow from LDAP/Database.	Mandatory			
84	Identity Lifecycle Management	The identity and access management solution should support Identity life cycle management including workflow (where needed) for below cases: - User Registration - Provisioning - Activating - Tracing - Locking - Unlocking - Suspending - Unsuspending - Resetting - Deleting	Mandatory			

#	Category	Requirement Description	Mandatory/ Desirable	Evidence	Compliance	Remarks
85	Identity Lifecycle Management	The identity management module should provide following identity lifecycle capabilities - Centralized identity repository - Complex data model - Extensible identity schema - Identity matching engine - Support for Multiple identity types - Batch-driven identity life cycle events - Event-driven identity life cycle events - Transition individuals between identity types and states - Relationship linking - Sponsorship (Manager/SPOC) management for nonemployee populations - Support for multiple identity authoritative sources - Multiple different authoritative sources for identity attributes - Multiple authoritative sources for various user populations - Cloud-hosted authoritative sources - Web-based interface to identity record - Request-driven identity life cycle events - Data normalization - Different Unique identifiers for different types of users - Reconciliation - Flexible views and management of data - Identity-centric view for application users, IT administrators, Managers and IGA administrators - Application-centric view - Policy- or role-centric view - Entitlement- or account-centric view - Data corruption detection - Support for future-dated items	Mandatory			

#	Category	Requirement Description	Mandatory/ Desirable	Evidence	Compliance	Remarks
		- Complex relationship models - Multiple personas for users - Self-service based Registration portal/API				
86	Identity Lifecycle Management	The Identity management solution should provide capability to configure user lifecycle events from the user interface.	Mandatory			
87	Identity Lifecycle Management	The Identity management solution should allow to define automatic escalation rules within the solution.	Mandatory			
88	Identity Lifecycle Management	The Identity management solution should automatically determine the need to create new accounts associated with adding entitlements and roles.	Mandatory			
89	Identity Lifecycle Management	The Identity management solution should be able to sync identity changes for ~ 90000 Identities across different geographies within 600 seconds	Mandatory			
90	Identity Lifecycle Management	The Identity management solution should dynamically generate forms to capture additional information from the user based on pre- configured provisioning policies for applications and roles.	Mandatory			
91	Identity Lifecycle Management	The Identity management solution should manage the complete user account lifecycle (create, update, delete, enable and disable).	Mandatory			
92	Identity Lifecycle Management	The Identity management solution should orchestrate changes to user access based on self-service access requests and lifecycle events across disparate provisioning processes.	Mandatory			
93	Identity Lifecycle Management	The Identity management solution should provide an administrative interface to track aggregate request activity across the enterprise.	Mandatory			

#	Category	Requirement Description	Mandatory/ Desirable	Evidence	Compliance	Remarks
94	Identity Lifecycle Management	The Identity management solution should provide capability to access changes initiated through automated change events — e.g., new hire, promotion, termination.	Mandatory			
95	Identity Lifecycle Management	The Identity management solution should provide capability where access change triggers call specific workflows to manage the change process from initiation through provisioning.	Mandatory			
96	Identity Lifecycle Management	The Identity management solution should provide dynamic and event-based identity lifecycle capabilities.	Mandatory			
97	Identity Lifecycle Management	The Identity management solution should provide flexible approval routing for changes initiated through self-service request or automated lifecycle events — e.g., manager, data owners, role owners, and security administrators.	Mandatory			
98	Identity Lifecycle Management	The Identity management solution should provide out of the box Identity lifecycle and operations workflows. The solution should also provide a workflow development toolkit.	Mandatory			
99	Identity Lifecycle Management	The Identity management solution should request additional information from users involved in the access request process — e.g., requester, approver, application/data owners.	Mandatory			
100	Identity Lifecycle Management	The Identity management solution should support delegation of approval requests to other users within the system and information should be tracked and audited.	Mandatory			
101	Identity Lifecycle Management	The Identity management solution should support dynamic rerouting of approval requests based on the outcome of other workflow steps. — e.g., change approval routing if a policy violation is	Mandatory			

#	Category	Requirement Description	Mandatory/ Desirable	Evidence	Compliance	Remarks
		identified or if the user's risk score is greater than defined limit.				
102	Identity Lifecycle Management	The Identity management solution should support the automation of lifecycle events — e.g., joiner, mover, leaver (e.g., new hire, promotion, termination etc.).	Mandatory			
103	Identity Lifecycle Management	The Identity management solution should support tracking and reporting on service-level metrics. Metrics should be available at the business process as well as the individual workflow step levels.	Mandatory			
104	Identity Lifecycle Management	The Identity management solution's access request and lifecycle management module should track aggregated request metrics and workflow statistics.	Mandatory			
105	Non-functional Requirements	The Identity management solution end-user screens should be served in English language.	Mandatory			
106	Non-functional Requirements	The Identity management solution should cater to user preferences and personalization options and this shall be stored in between sessions.	Mandatory			
107	Non-functional Requirements	The Identity management solution should support user interface and reporting templates (colour, fonts, headers, footers, logos, etc.). These templates should be modified to meet customer's branding requirements.	Mandatory			
108	Password Management	The Identity management solution should allow configurable number of challenge questions presented to the user based on the organization’s security policies.	Mandatory			
109	Password Management	The Identity management solution should allow delegated password administration.	Mandatory			

#	Category	Requirement Description	Mandatory/ Desirable	Evidence	Compliance	Remarks
110	Password Management	The Identity management solution should enforce password strength requirements. The Identity management solution should support the following constraints: • Minimum/maximum length • Minimum letters/numbers/special characters • Password history constraints • Exclusion dictionary • Allowable characters • Number of character types • Triviality checks (old password) • ID in password check	Mandatory			
111	Password Management	The Identity management solution should force the user to answer their authentication questions.	Mandatory			
112	Password Management	The Identity management solution should provide administrators with a report detailing users who have not completed answers to challenge questions.	Mandatory			
113	Password Management	The Identity management solution should provide an option to help users reset forgotten passwords with a Windows desktop (i.e., GINA or Credential Provider plugin).	Desirable			
114	Password Management	The Identity management solution should provide capability to integrate end-user password management user interfaces with the solution's access request user interfaces for a seamless user experience.	Mandatory			
115	Password Management	The Identity management solution should provide capability where password changes be synchronized across multiple systems at the same time. e.g. The Identity management solution should provide out of the box capabilities for password synchronization across Active Directory,	Mandatory			

#	Category	Requirement Description	Mandatory/ Desirable	Evidence	Compliance	Remarks
		leading ERPs, CRMs and database based applications.				
116	Password Management	The Identity management solution should provide GINA based forgot password functionality.	Desirable			
117	Password Management	The Identity management solution should provide/support challenge questions for password recovery.	Mandatory			
118	Password Management	The Identity management solution should support multiple password policies on a single application. It should allow to apply different policies to users based on identity attributes (e.g., employee and contractor policies).	Mandatory			
119	Platform and Architecture	Describe the logical components and all tiers of the solution architecture.	Mandatory			
120	Platform and Architecture	The Identity management should provide both on premises and cloud based deployment options. It should provide both software and appliance based deployments. On premises software based deployment is preferred.	Mandatory			
121	Platform and Architecture	The Identity management solution configurations should be easily deployable and to be migrated between environments (i.e., development, test, staging, and production).	Mandatory			
122	Platform and Architecture	The identity management solution should adhere to the industry standard guidelines w.r.t. sizing schemes for hardware, application server and database. Please describe the fulfilment of the compliance requirement for virtual servers - if used.	Mandatory			
123	Platform and Architecture	The identity management solution should allow for extensibility or configuration via a scripting language, API or other. What programming language proprietary or	Mandatory			

#	Category	Requirement Description	Mandatory/ Desirable	Evidence	Compliance	Remarks
		other may be used for the customization? Please explain.				
124	Platform and Architecture	The Identity management solution should be software based and should provide access to it's underlying application server environment for hosting custom applications created for customer's Identity management use cases.	Mandatory			
125	Platform and Architecture	The identity management solution should expose web services for initiating internal compliance and provisioning processes (REST, SPML).	Mandatory			
126	Platform and Architecture	The identity management solution should handle a large number of users, roles, and access requests.	Mandatory			
127	Platform and Architecture	The identity management solution should pass performance benchmarks and reference deployments in similar financial enterprise environments.	Mandatory			
128	Platform and Architecture	The Identity management solution should provide a robust repository for identity attributes and capability to define custom attributes.	Mandatory			
129	Platform and Architecture	The identity management solution should provide scalability options to accommodate future growth and increasing workload demands.	Mandatory			
130	Platform and Architecture	The Identity management solution should provide simulated or closed system testing environment for performing testing of newly created workflows before deployment.	Mandatory			
131	Platform and Architecture	The Identity management solution should run in a clustered environment for load balancing and/or fail-over purposes.	Mandatory			
132	Platform and Architecture	The Identity management solution should run on a	Mandatory			

#	Category	Requirement Description	Mandatory/ Desirable	Evidence	Compliance	Remarks
		wide variety of enterprise platforms, application servers and database combinations. Technical details should be provided.				
133	Platform and Architecture	The Identity management solution should support discovery of flat-file or database schemas to speed-up deployment activity.	Mandatory			
134	Platform and Architecture	The identity management solution should support integration with 3rd party applications via web services.	Mandatory			
135	Platform and Architecture	The Identity management solution should support running in a virtualized application environment such as VMware.	Mandatory			
136	Platform and Architecture	The Identity management solution should support the ability to scale tasks such as aggregations, identity refresh and certification generation across multiple hosts and threads.	Mandatory			
137	Platform and Architecture	The identity management solution should support the deployment of High Availability and Disaster Recovery requirements as per the industry standard guidelines.	Mandatory			
138	Platform and Architecture	The Identity management system should provide following Deployment and support capabilities - Support for common platforms - Support for common application servers - Support for common data repositories - Support LDAPs - Support for Databases - Provision of REST APIs - Self-service capabilities available through a single web interface - Administration capabilities are available through a web interface - Customizable web forms - Wizard-based installation - Protection of sensitive data - Localization Support	Mandatory			

#	Category	Requirement Description	Mandatory/ Desirable	Evidence	Compliance	Remarks
		- Version control - Migration between environments - Preference of configuration over customization - Support for commodity scripting languages for IT serviceability functions - Integration with access management systems - Mobile optimized user experience - Appliance-type delivery form factor - Software-type delivery form factor - Strong authentication for administrators - data partitioning/multitenancy - Flexible delivery of updates/patches - Integration with PAM solutions for administrative access to IGA functions - Support for Disaster recovery - Support for High availability - Horizontal and Vertical Scalability - Support for service-based architecture				
139	Policy and Role Management	The identity and access management solution detect and report on: - Inactive roles - Users with no roles	Mandatory			
140	Policy and Role Management	The identity and access management solution provide a single policy repository that is leveraged by all identity processes, including both detective and preventive access controls.	Mandatory			
141	Policy and Role Management	The identity and access management solution should allow policy owners to specify a unique risk score for each policy rule in the system.	Mandatory			
142	Policy and Role Management	The identity and access management solution should automatically scan and detect policy violations.	Mandatory			

#	Category	Requirement Description	Mandatory/ Desirable	Evidence	Compliance	Remarks
143	Policy and Role Management	The identity and access management solution should automatically notify responsible parties, when policy violations are detected.	Mandatory			
144	Policy and Role Management	The identity and access management solution should clearly highlight policy violations during access reviews to allow for rapid remediation.	Mandatory			
145	Policy and Role Management	The identity and access management solution should detect and alert on role violations before assigning roles to users.	Mandatory			
146	Policy and Role Management	The identity and access management solution should escalate policy violations if not addressed in a defined period of time.	Mandatory			
147	Policy and Role Management	The identity and access management solution should maintain all previous versions of role definitions. The solution should easily roll back to previous versions of role definitions.	Mandatory			
148	Policy and Role Management	The identity and access management solution should provide a business-friendly UI for defining and editing access policies without the need for coding.	Mandatory			
149	Policy and Role Management	The identity and access management solution should provide a business-friendly user interface for managing policy violations by both business managers and compliance administrators.	Mandatory			
150	Policy and Role Management	The identity and access management solution should provide capability to expand policies using a scripting or programming language interface.	Mandatory			
151	Policy and Role Management	The identity and access management solution should provide the ability to assign and de-assign roles to users. Assignment can be done both manually and through automated	Mandatory			

#	Category	Requirement Description	Mandatory/ Desirable	Evidence	Compliance	Remarks
		assignment and de-assignment rules associated with a role.				
152	Policy and Role Management	The identity and access management solution should support execution of a business process or workflow when policy violations are detected, allowing varying responses based on criteria such as the calculated risk of the violation.	Mandatory			
153	Policy and Role Management	The identity and access management solution should support role mining to discover potential roles using various pattern search algorithms.	Mandatory			
154	Policy and Role Management	The identity and access management solution should support temporary assignment of a role to a user (e.g., sunrise and sunset dates).	Mandatory			
155	Policy and Role Management	The Identity management solution should provide a batch scheduling utility.	Mandatory			
156	Policy and Role Management	The Identity management solution should provide attribute-based provisioning capabilities with functionality for override as per manual intervening events.	Mandatory			
157	Policy and Role Management	The Identity management system should provide following Policy and Role Management capabilities - Centralized policy management - Granular policy definition - Multiple access policy types - Assignment policies - Approval policy - Visibility - Rule-based access policy assignment - Role-based access policy assignment - Workflow-based access policy assignment - Out-of-the-box policy configuration - Business and technical roles - Role views	Mandatory			

#	Category	Requirement Description	Mandatory/ Desirable	Evidence	Compliance	Remarks
		- User role assignment - Role entitlement view - Flat role model - Static segregation of duty (SOD) policy definition - Retrofit/reapply role and policy permissions - Detect out-of-policy entitlements - Policies are customizable using standard scripting language - Support for access assignment expiration dates - Automated role discovery/mining - Role suggestions - Role reporting and analytics - Machine learning-driven role and policy definition - Approval workflows for role assignment changes - Integration with external applications and services (inbound and outbound procedure calls) - Policy templates - Data access governance (DAG) integration - Cloud access governance (CAG) integration - Application roles				
158	Provisioning & Connectivity	Identity Manager solution should provide the event forwarding capabilities to Security Event Log Management solutions so that this caters to all audit related activities.	Mandatory			
159	Provisioning & Connectivity	The identity and access management solution should integrate with non-automated provisioning systems, such as help desk/service request systems.	Mandatory			
160	Provisioning & Connectivity	The identity and access management solution should provide out-of-the-box connectors for automatically pushing changes to enterprise IT systems.	Mandatory			
161	Provisioning & Connectivity	The identity and access management solution should provide users with	Mandatory			

#	Category	Requirement Description	Mandatory/ Desirable	Evidence	Compliance	Remarks
		detailed information about all provisioning tasks related to a request for access.				
162	Provisioning & Connectivity	The identity and access management solution should receive updates on ticket status and display the information to users when tracking requests.	Mandatory			
163	Provisioning & Connectivity	The identity and access management solution should support delta aggregation of application accounts and access rights.	Mandatory			
164	Provisioning & Connectivity	The identity and access management solution should support the automatic generation of "tickets" through service/help desk integrations.	Mandatory			
165	Provisioning & Connectivity	The identity and access management solution should support the retrieval of entitlement information through provisioning connectors without the need to directly connect to the target system, if required.	Mandatory			
166	Provisioning & Connectivity	The Identity management solution integrated with customer's HR system should update attributes of the users in real time or in batches.	Mandatory			
167	Provisioning & Connectivity	The Identity management solution should ensure that integration with AD does not require any changes to the schema.	Mandatory			
168	Provisioning & Connectivity	The Identity management solution should expose an API for integrating with third-party provisioning solutions to bulk re-provision users based on role model changes.	Mandatory			
169	Provisioning & Connectivity	The Identity management solution should have out of the box integrations with market leading PAM, IAM, Access Management, SSO etc. solutions for both application and IT access.	Mandatory			

#	Category	Requirement Description	Mandatory/ Desirable	Evidence	Compliance	Remarks
170	Provisioning & Connectivity	The Identity management solution should have the tool to provide access to all connectors free of charge. The connectors developed in future releases should be in line with this statement. If not, details including cost should be explained.	Mandatory			
171	Provisioning & Connectivity	The Identity management solution should integrate help desk/service desk systems and should support automatic generation of tickets. The system should receive updates on ticket status and display the information to users when tracking requests.	Mandatory			
172	Provisioning & Connectivity	The Identity management solution should integrate with different domains within the same forest on the AD or with different domains that do not have any trust relationship between each other independently should be supported.	Mandatory			
173	Provisioning & Connectivity	The identity management solution should possess the ability to integrate with existing IT systems, applications, and directories, such as HR systems, LDAP, and cloud platforms.	Mandatory			
174	Provisioning & Connectivity	The Identity management solution should provide a toolkit for creating connectors for custom applications. Usage and abilities of the toolkit should be explained.	Mandatory			
175	Provisioning & Connectivity	The Identity management solution should provide elaborate access provisioning capabilities for IT layer i.e., Servers, Cloud, Network, Databases and Security & IT Mgmt. systems.	Mandatory			
176	Provisioning & Connectivity	The Identity management solution should provide out of the box connectors with SAP with capability of SAP	Mandatory			

#	Category	Requirement Description	Mandatory/ Desirable	Evidence	Compliance	Remarks
		Roles, Groups and Tcode management.				
177	Provisioning & Connectivity	The Identity management solution should provide out-of-box integration with any third-party provisioning systems. Details and integration methods should be explained.	Mandatory			
178	Provisioning & Connectivity	The Identity management solution should provide out-of-the-box connectors for the following categories of enterprise systems. Complete list of out-of-the-box connectors should be provided. - Directories - Databases - Platforms - Business Applications - Messaging Applications - SaaS Applications	Mandatory			
179	Provisioning & Connectivity	The identity management solution should provide the synchronization of interfaces with external directories. (i.e., synchronization of the user database with LDAP/Active Directory).	Mandatory			
180	Provisioning & Connectivity	The Identity management solution should support all industry standard file format for file import options. Example: CSV, XML, Flat files etc.	Mandatory			
181	Provisioning & Connectivity	The identity management solution should support APIs and connectors to facilitate customization and integration with other security and IAM solutions.	Mandatory			
182	Provisioning & Connectivity	The identity management solution should support for industry-standard identity protocols (e.g., SAML, OAuth) for seamless integration with third-party systems.	Mandatory			
183	Provisioning & Connectivity	The Identity management solution should support integration with the following systems. - Microsoft Azure AD - Microsoft 365 - Microsoft Active Directory	Mandatory			

#	Category	Requirement Description	Mandatory/ Desirable	Evidence	Compliance	Remarks
		- Privileged Account Management - SAP GRC AC - SAP SuccessFactors Employee Central - LIC business applications listed in the scope of work of RFP				
184	Provisioning & Connectivity	The Identity management solution should support integration with third-party provisioning systems and use industry standards such as the service provisioning markup language (SPML) or the system for cross-domain identity management standard (SCIM) when supported by integrated systems.	Mandatory			
185	Provisioning & Connectivity	The identity management solution should support integration with threat intelligence and risk assessment tools for enhanced risk visibility.	Desirable			
186	Provisioning & Connectivity	The Identity management solution should support multiple authoritative sources for identity data.	Mandatory			
187	Provisioning & Connectivity	The Identity management solution should support sending account creation and change requests to third-party provisioning systems for execution in a target resource.	Mandatory			
188	Provisioning & Connectivity	The Identity management solution should support the definition of custom schemas for each connected application.	Mandatory			
189	Provisioning & Connectivity	The Identity management system should provide following Fulfilment and Connector capabilities - Direct fulfilment - Flat-file connectors - Java Database Connectivity (JDBC)/Open Database Connectivity (ODBC) connector - LDAP connector - Web services connector - Indirect fulfilment - Support for Multiple target systems	Mandatory			

#	Category	Requirement Description	Mandatory/ Desirable	Evidence	Compliance	Remarks
		- Support for Add, read, modify and delete operational - Account creation policies - Support for Mandatory/Required attributes - Support for Conditions - Account deletion policies - Delete, disable or suspend - Data synchronization - SCIM 2.0 support - Dynamic account creation and deletion policies - HR system connector(s) - Database connector(s) - Directory connector(s) - Platform connector(s) - Business application connector(s) - ITSM/help desk system connector(s) - Content and collaboration system connector(s) - Application/system log connector(s) - SaaS application connector(s) - Support for connectivity to authentication and access management systems - Integration with SaaS-delivered IAM systems - Cloud platform connector(s) - Integration with privileged access management (PAM) systems - SDK for building custom connectors - Support for connectivity to industry-specific applications - Support to integrate with Robotic process automation (RPA) based fulfilment - Data access governance support - Cloud access governance support - Unified endpoint management (UEM) support				
190	RBAC and SOD	The identity management solution should detect real-	Mandatory			

#	Category	Requirement Description	Mandatory/ Desirable	Evidence	Compliance	Remarks
		time SoD conflict during access requests and provisioning processes.				
191	RBAC and SOD	The identity management solution should have ability to define and manage remediation workflows for resolving SoD conflicts.	Mandatory			
192	RBAC and SOD	The identity management solution should have SoD policy definition and enforcement to prevent conflicts of interest and mitigate access-related risks.	Mandatory			
193	RBAC and SOD	The Identity management solution should support for dynamic and attribute-based roles to accommodate complex access requirements.	Mandatory			
194	Self Service Access Management	All user entitlements, roles, policy information and activity data should be viewable within the context of an individual identity.	Mandatory			
195	Self Service Access Management	The Identity management solution should allow anyone in the organization to request access for anyone else and should be able to manage who can request access for others.	Mandatory			
196	Self Service Access Management	The identity management solution should allow attributes to be used to define the requestor relationship.	Mandatory			
197	Self Service Access Management	The identity management solution should allow capability of self-service management for adding, changing, and removing access from the same interface.	Mandatory			
198	Self Service Access Management	The Identity management solution should allow editing identity attributes of existing users and updating target systems.	Mandatory			
199	Self Service Access Management	The identity management solution should allow the user to specify a priority for access requests.	Mandatory			
200	Self Service Access Management	The Identity management solution should allow the users to specify start date, end date, period of time	Mandatory			

#	Category	Requirement Description	Mandatory/ Desirable	Evidence	Compliance	Remarks
		and priority for access requests.				
201	Self Service Access Management	The Identity management solution should allow users to track the full details of an access request, including the status of approvals and fulfilment tasks.	Mandatory			
202	Self Service Access Management	The Identity management solution should be able to limit the data that is editable from the user interface.	Mandatory			
203	Self Service Access Management	The Identity management solution should be able to restrict users to only requesting certain roles or access rights.	Mandatory			
204	Self Service Access Management	The Identity management solution should create a single view of each user within the enterprise and their associated access privileges.	Mandatory			
205	Self Service Access Management	The Identity management solution should enable the users to track access requests made by them and for them.	Mandatory			
206	Self Service Access Management	The Identity management solution should facilitate requesting of different types of access including roles, entitlements and accounts.	Mandatory			
207	Self Service Access Management	The Identity management solution should facilitate self-service access requests to allow requesting new access as well as changing and/or removing access rights.	Mandatory			
208	Self Service Access Management	The identity management solution should give end users a business-friendly dashboard to view status of pending and completed requests.	Mandatory			
209	Self Service Access Management	The Identity management solution should offer self-service registration for external or “non-employee” users e.g., contractors, partners, consultants, and other types of external stakeholders.	Mandatory			

#	Category	Requirement Description	Mandatory/ Desirable	Evidence	Compliance	Remarks
210	Self Service Access Management	The Identity management solution should provide a business-friendly interface / dashboard for requesting changes to user access and to view status of pending or completed requests.	Mandatory			
211	Self Service Access Management	The Identity management solution should provide a graphical user interface for configuring/editing business processes and workflows associated with manually initiated access requests (including self-service and delegated requests) .	Mandatory			
212	Self Service Access Management	The Identity management solution should provide users to search for access using configurable metadata attributes such as name, description, owner or other keywords.	Mandatory			
213	Self Service Access Management	The identity management solution should scope who can request access for others.	Mandatory			
214	Self Service Access Management	The identity management solution should support configurable workflows to manage self-service access requests/changes.	Mandatory			
215	Self Service Access Management	The identity management solution should support creating new identities from scratch within the user interface (e.g., act as the authoritative source for creating identities).	Mandatory			

Authorized Signatory of the bidder

Name:
Designation:
Date:
Place:
Seal of the company