Request for Proposals

Identity Governance and Administration

Issue Date: June 1, 2022

Closing Date&Time: June 22, 2022 18:00 (GMT+4)

Contents

1. Summary of Opportunity

Unibank (after Bank) accepts proposals from qualified vendors to provide an Identity Governance and Administration (IGA) solution. The IGA solution must have the ability to support a large user population and integrate critical business applications.

This Request for Proposals (RFP) outlines the basic requirements for the solution to be provided by the proponents.

Proponents shall base their proposal on full compliance with the provisions and requirements of this RFP document. Any deviation from the requirements set out in this document must be fully disclosed in the proposal.

2. Background

Unibank is one of the largest private banks established in Azerbaijan in July 1992 under the name of MBank. On October 15, 2002, after the merger of Mbank with PROMTEXBANK, one of the leading banks of Azerbaijan, the bank's name was changed to Unibank.

Bank has a head office and 29 branches in Baku and the regions of Azerbaijan.

The solution must specifically support:

- 2000 end-users (including employees and non-employees)
- Integration with enterprise directories and critical applications, including Active Directory (AD), HR System, Core Banking Systems, SWIFT, Card Processing System, Instant Money Transfer Systems, Accounting, CRM, Jira etc. **At the initial stage, the scope of this RFP will be limited to the integration of AD and HR system.**
- Integration with key security technologies, including Security Information & Event Management (SIEM) platforms and Data Loss Prevention (DLP) platforms.

3. Management Summary

Provide a management summary which includes, but is not limited to, the following:

- Provide an overview of your proposal and highlight the benefits – identify factors that make your services different and/or unique
- Describe your company's core capabilities and business approach
- Address why your proposed services are best suited to meet the needs of Bank
- Include your company's mission statement and/or core values

4. Capabilities

An Identity Governance and Administration solution for Bank will provide all of the following core components and capabilities described in Appendix 1.

5. Technical Requirements:

Proponent shall supply a list of technical requirements for operating the IGA platform. The ability to host the platform in a virtualized environment within the Bank's data center is preferred. The following features are desired:

- Capability of being managed on premises in the Bank's data center
- Support for running in a virtualized environment
- Capability of running in a clustered environment for load balancing and/or fail-over purposes

6. Support Services

The following support services and service level agreements (SLAs) are required as a minimum:

- 24X7 standard support coverage
- 2 hour response for severity 1 issues with critical business impact
- 4 hour response for severity 2 issues with significant business impact
- By end of next business day for severity 3 issues with some to minimal business impact
- Escalation options and enhanced support for critical issues

7. Schedule, Implementation, Staffing, and Training Plans

Bank will require consulting resources to assist in the implementation of the IGA solution and would like the vendor to provide response to the following regarding implementation services and/approaches. Vendors can incorporate partner services if necessary.

- Provide a Roadmap – an illustration for Bank, which depicts the proposed IGA solution implementation road map and phases. Vendor must break down each phase and provide a description of the implementation taking place
- Provide an estimated timeline – a table or graphical representation providing Bank with an overview of estimated timelines for all phases
- Provide Estimated Level of Effort (LOE / Staffing Plan) – Demonstrate the level of effort (time) required by vendor and Bank resources – indicate the type of Bank resource needed (System Administrator, Network Administrator, Business Software, Project Manager) and the amount of projected time for each resource and each task
- LOE/Staffing Plan must clearly indicate the percentage of time (or estimated hours) Bank and vendor resources required for this effort, divided by phases
- Provide a detailed training plan – include estimated timeframes and deliverables for each phase of project
- Include methodology, training options, and documentation/user manuals for the following:
  - Implementation team
  - System administrators
  - Network administrators
  - Managers and end users

8. Delivery of Proposals (June 22, 2022 18:00 (GMT+4))

An original (clearly marked as such) plus one copy (2 total) of concise proposals in booklet or notebook form with supporting documentation shall be delivered in a sealed envelope or container to Bank's Administrative Affairs Department.

Proposals must be signed, and the authority of the individual signing must be stated thereon. All responses are to be addressed to:

ATTN.: Faig Huseynov, Chairman of the Management Board, Unibank OJSC

RFP: Identity and Access Governance

55, Rashid Behbudov Street, Baku, AZ 1014, Azerbaijan Republic

Deadline for receipt of proposals by Administrative Affairs Department is, **June 22, 2022 by 18:00 (GMT+4)**. Date and time will be stamped on the proposals by Administrative Affairs Department. Proposals received after that time will not be accepted.

9. Proposal Evaluation and Decision

1. Proposals will be evaluated, and award will be based on the vendor's ability to offer the best value (quality, past performance and price), and on anticipated quality of service. Items considered include but are not limited to:

    - Ability to meet core components and capabilities of this RFP;
    - Cost of Services; Compensation and Fees; **(Bank is looking for fixed price contracts and licenses starting at the first day of going live of the product)**
    - Financial Strength of the vendor;
    - Proposal Documentation / Presentation;
    - Vendor's Experience;
    - Vendor's Profiles/References;

2. Vendor proposals will be evaluated by Tender Commission of the Bank. A preliminary screening will be used to identify competitive vendors who have met the mandatory requirements. Administrative Affairs Department may subsequently request selected vendors to make a presentation at a set time and date, to clarify information provided in the proposals. **Final consideration, evaluation, and recommendation may be made at this point on or before August 1, 2022**. However, the Bank reserves the right to take additional time for reference review, site visits and/or proposal negotiations.

3. Negotiation of contracts with vendor and implementation partner will start after final decision of Tender Commission and will be finalized **on or before August 31, 2022.**

Appendix 1. Core components and capabilities

Identity Data Management

The solution shall support the ability to synchronize and store identity, entitlement, and role information from various information resources across the enterprise (e.g., AD, Core Banking System, HR System, SWIFT, databases, etc.).
The solution shall provide the ability to perform simulation run before actual synchronization starts to validate the correctness of configuration.
The solution shall have an attribute mapping management interface that supports mappings of attributes from one system to another system.
The solution shall support bi-directional synchronization of identity attributes, groups, and group memberships.
The synchronization shall support filtering and scoping capability to ensure only the desired data is included.
The solution shall support the ability to integrate with other resources in order to acquire and store user access data and business data such as organization structure, cost center, location, mailbox server, etc.
The solution shall support multiple mechanisms of data synchronization via native connector, flat file, database and web services call.
The solution shall support users with multiple accounts (e.g., different types of accounts with separate roles and responsibilities).
The solution shall support account management for users who have multiple accounts on the same resource (e.g., a person who has an administrative account and a normal user account on AD).
The solution shall support the ability to designate any account as privileged user account.
The solution shall support the ability to import and manage organizational information for each person such as, but not limited to, manager, job title, description, department, location, cost center, address, join date, leave date, last working date, etc.
The solution shall provide report or user interface that easily presents the visibility of how each resource and entitlement are granted to a user. For example, you can easily identity AD account was automatically granted via a role, while Core Banking System access was granted through a request.
The solution shall provide search functionality to locate identity information with customizable filters, e.g., information based on attributes, roles, organizations, etc.

Process Automation and Provisioning

The solution shall support new hire process whereby relevant accesses and entitlements for the user across the enterprise are granted automatically.
The solution shall support transfer process whereby user's excess accesses and entitlements are removed and new accesses and entitlements are granted automatically.
The solution shall support challenge of role removal during transfer process scenario.
The solution shall support termination process whereby user's accesses are disabled and subsequently removed after limited period.
The solution shall support process orchestration for handling requirements such as, but not limited to, provisioning, file operation, execute external command/script, file transfer operation, emailing, import/export external content, etc. to facilitate the core identity lifecycle management processes.
Graphical user interface shall be provided to manage process orchestration workflow.
The solution shall support both event and schedule driven fulfillment process.
The solution shall support auto provision/de-provision through role which inherits access(s) and entitlement(s).
The solution shall provide administrative interface for authorized user to create, modify attributes, delete, enable, disable account and assign/un-assign roles manually in connected system.
The solution shall provide a list of out of box connectors for managing identity and entitlement in enterprise systems. Provide the list of out-of-box connectors available from the solution.
The solution shall provide user friendly interface for configuration of connectors without coding.

Workflow

The solution shall provide built-in workflow engine with graphical user interface for managing workflows.
The solution shall support the ability of creating workflows for user self-service access and attestation request.
The solution shall provide set of predefined workflows.
The workflow shall support multiple levels of approval and multiple approvers per approval level.
The solution shall support workflow routing to specific approver(s) dynamically (e.g., administrators, application owners, group owner, managers, roles) based on department, cost center, group ownership, role or other specific attributes.
The rules for determining specific approver(s) in each workflow shall be easily configurable.
The solution shall support workflow routing to specific approver in real time when specific job or personal information is updated while the workflow is still in progress.
The solution shall support delegation at each approval stage in a workflow.
The solution shall support email notification at each approval stage in a workflow for actions such as request, approve, rejection, reminder, delegation and escalation.
The workflow shall support different email template for different approval action.
The solution shall support email notification to remind approver at each approval level after certain elapse time based on working hour.
The solution shall support automated timeout actions such as approved, escalate, reject, and abort at each approval level after certain elapse time based on working hour.
The solution shall support the ability of keeping record of each workflow actions performed by users or system with timestamp for audit purpose.
Different workflows shall be able to apply to different resource accounts, entitlements or roles.

User Self-Service Management

The solution shall provide business friendly web portal for user to perform self-service activities.
The web portal shall be fully customizable without the need of coding.
The self-service shall provide graphical representation of accounts and entitlements assigned to the user, along with access to key unstructured data such as files, folders or shares.
The self-service shall support the ability of delegating selected roles or entitlements to other users with limited period of duration.
The self-service shall allow user to view detailed delegation history, including all permissions or entitlements delegated to others as well as permissions or entitlements the user has received through delegations.
The self-service shall allow user to list all requests made as well as requests other people made on his/her behalf.
The self-service shall allow user to view historical list of all his/her approvals for a given date range. Details displayed include the processing status, approval workflow summary, request ID and recipient.
The self-service shall allow manager to view profiles of their subordinates, as well as review their requests, entitlements, risk scores, historical changes. The manager can also drill down into an entitlement for more details.
The solution shall support the ability of restricting what a user can request based on user's organizational status such as department, rank, role, or other attributes.
The solution shall support preventive policy violation check such as segregation of duty (SoD) before a request is being submitted.
The solution shall support exceptional approval process when policy violation is detected upon user submitting a request.
The solution shall allow user to specify start and end date for a request and auto-provisioning/de-provisioning shall perform according to specified start and end date respectively.
The self-service shall allow user to lookup for a reference user's existing requested accesses or entitlements to make request decision.
The self-service shall allow user to request access or entitlement on behalf of his/her subordinates in the organization.
The self-service shall provide visibility of request process and who will be the next approver(s).
The self-service shall allow approver to add additional approver(s) during an approval step.
The self-service shall allow approver to delegate the approval decision to another selected user.
The solution shall support auto-provisioning for requested access or entitlement upon approval.
The self-service shall allow user to check the status and progress of request and view the full history of pass requests.

The solution shall support the ability to allow user to remove an account access or entitlement that is obtained from request and the removal process shall subject to approval workflow if necessary. The removal shall also results in de-provisioning account access or entitlement automatically.

Role Management

The solution shall support the management of enterprise role modeling.
The Role-based access control (RBAC) capability shall not be provided by separate product. It shall be part of built-in feature from the solution and the RBAC data model shall be integral part of the solution that can be leveraged by provisioning, compliance, access request, reporting functions.
The solution shall support role lifecycle management that covers the basic CRUD (Create, Update and Delete) operations on roles.
The role management function shall support adding of new entitlements that should be assigned to a role and inherited to role members.
The role management function shall support removing entitlements from a role, as a result the permissions are removed from role members.
The solution shall support definition of hierarchical role structure so that company resources can be inherited by members through these hierarchies.
Role hierarchy shall support top-down inheritance model whereby company resources are inherited from top to bottom. For example, entitlements that are valid in a country are also valid for each individual location in this country (top-down inheritance).
Role hierarchy shall support bottom-up inheritance model whereby company resources are inherited from bottom to top. With this, company resources assigned to project members in lower hierarchy are inherited by members in upper hierarchy.
The solution shall support blocking of inheritance in any level within the hierarchy model. For example, this allows specific data from sub-projects to be marked as confidential and concealed, even from the top project leader.
The solution shall support the definition of role type such as business role, functional role, application role, etc. to support various business requirements.
The solution shall support the ability of defining assignment constraints on roles, e.g. business role can't contain direct entitlements but only application role, functional or can contain group membership, etc.
The solution shall support flexible way of including variety type of entitlements contained in a role (groups, accounts, sub-roles, granular entitlements).
The solution shall support role delegation whereby user can delegate his/her role to other authorized user for a limited period of duration, and permissions and entitlements from the role shall be granted to delegate accordingly.
The solution shall support adequate role attributes such as manager, description, department, location, remark, custom attributes.
The solution shall provide user interface to allow assignment or de-assignment of role to user manually.
The solution shall support the ability to dynamically assign role to user by evaluating user's attributes. For example, a branch manager can receive a class of permissions that have specific local characteristics, or all employees of a particular department can be granted access to a specific web-application.
Graphical user interface shall be provided for defining evaluation criteria for dynamic role assignment.
The solution shall support the ability of allowing user to request for role for a limited period of duration via self-service with approval workflow.
The solution shall support the ability of defining conflicting role to prevent user from being assigned to several roles at the same time and from obtaining mutually exclusive company resources through these roles (Segregation of Duties).
The solution shall support simulation to test all the effects of proposed role changes and uncover possible rule violations before the changes are put into operation.
The solution shall support role mining for analyzing user-to-resource mapping data to determine user entitlements for role-based access control.
The solution shall provide graphical user interface for performing role mining activities.
Role mining shall support role discovery based on HR data such as but not limited to department, job title, location, cost center, etc.
Role mining shall support role discovery by analyzing cross-target-system entitlement sets.
Role mining shall support building out role structures based on various cluster algorithms.
Role mining shall support flexible way of confine the scope of analysis by selecting a group of user based on locations, job title, manager, cost center, etc. against certain applications.

For example, only analyze user in department A with job title senior manager against SAP and SharePoint access.
Role mining user interface shall show the accuracy of matching employees' real entitlements to the entitlements given by the new roles.
The solution shall support the ability of exploring and modifying the generated role structure in the role mining process.
Role mining user interface shall support comparing entitlement sets of different users given by a role.
Role mining user interface shall allow viewing detail entitlement of each discovered role.
The solution shall support creating roles from role mining results with or without an attestation process.

Attestation and Certification

The solution shall support attestation out-of-box without depending on separate product.
The solution shall provide business user friendly web portal for compliance officer and attestor to perform attestation activities.
The solution shall support comprehensive attestation use cases for attesting user, role, department, location, cost center, entitlement such as group membership.
The solution shall support attestation by user manager, department manager, system owner, group owner, data owner, etc.
The solution shall support automatic generation of user certification upon a new user on-boarding.
The solution shall support automatic generation of role certification upon a new role is created.
The solution shall support generation of attestation on schedule basis.
The solution shall support the ability of changing attestation settings inflight and existing attestations reflect the changes accordingly.
The solution shall support the ability to define population of objects (users, roles, entitlements, etc.) to be included in each attestation based on attributes of attested object.
The solution shall support the ability to define population of objects based on risk index of to be attested objects (such as user, application, role, etc.) so that only high risk objects are included for attestation process.
The solution shall provide compliance office the visibility of what objects (users, roles, entitlements, etc.) will be included in each attestation before actually rolling out.
The solution shall support flexible workflow configuration for routing the attestation to appropriate attestor(s).
The attestation workflow shall support routing to specific attestor(s) dynamically such as user manager, group owner, department manager, etc.
The rules for determining specific attestor(s) for each attestation shall be easily configurable.
The solution shall support email notification to attestor(s) upon initiation of attestation process.
The solution shall provide graphical user interface to manage email templates for attestation in WYSIWYG mode.
The solution shall allow attestor to review attestation content (such as user's full entitlements, group members, role members, etc.) for each item online or in offline PDF report format before making informed decision.
The solution shall allow attestor to delegate attestation decision for specific items to others as needed.
The solution shall allow attestor to request for help from other user before making decision.
The solution shall support email notification to remind attestor at each approval level after certain elapse time based on working hour.
The attestor shall allow making bulk approval decision for all items in an attestation.
The solution shall support setting duration for each attestation.
The solution shall display due date for each item within the attestation.
The solution shall display progress of each attestation process in the form of percentage of completion.
The solution shall highlight overdue items so that attestor can take necessary action promptly.
The solution shall display risk profile for each attestation item as additional information.
The solution shall support the ability to track and display the full history of each attestation item, including approve, deny and delegation decisions.
The solution shall display history of attestation decisions made previously for each item such as user, entitlement or role.
The attestation interface shall be user friendly to allow attestor to add, remove and group columns and filter information on each column.
The solution shall provide authorized user access governance dashboard that display various metrics of attestation status in the whole enterprise.
The solution shall allow attestation administrator (compliance officer) to send reminding message to all or selected attestor(s) via email.

The solution shall allow attestation administrator (compliance officer) to extend attestation process that is overdue.

Business Rule and Policy Management

The solution shall support the definition of detective and preventative compliance policy that are corresponding to regulatory requirements (i.e. PCI, SOX, ISO) and company specific policies.
The solution shall support the ability to define and enforce policy across all identity information and combination of entitlements. Example policies are: • An employee may not obtain two entitlements A and B at the same time. • Only employees with a particular department can have a particular entitlement. • Every employee must have a manager assigned.
The solution shall support definition of company policy based on fine grained employee data or attributes. Sample policies are: • Every employee must have a manager assigned. • All employees must have employee ID assigned. • All departments must have employees assigned. • All employees must be certified/attested.
The solution shall support definition of access policy based on user accesses and fine grained entitlements. Sample policies are: • Only employees in a particular department can have a particular access or role. • Full access must not be granted on a folder to the predefined group "Everyone".
The solution shall support definition of SoD policies. Sample policies are: • An employee may not obtain two entitlements A and B at the same time.
Business friendly wizard driven user interface shall be provided for defining policy.
The solution shall support definition of complex policy using script or programming language.
The solution shall automatically detect violations based on defined policies.
Designated user shall be notified via email upon detecting policy violation.
The solution shall support granting exception by designated user in the event of violation.
The solution shall support granting of exception for a limited period of duration.
The solution shall support assigning mitigation controls to each policy. The mitigation controls are implemented the moment the policy is violated to reduce the risk exposure.
Detail policy violation reports shall be provided out-of-box and readily accessible by compliance officer.
Business friendly web portal shall be provided for compliance officer to manage violation.
Policy violation history report shall be provided out-of-box.
The solution shall support assigning risk index to each policy for risk assessment criteria in the event that violation is detected against a policy.
The risk index assigned to policy shall be used by the solution to calculate final risk score of an individual to indicate risk level in the organization.
The solution shall provide authorized user access governance dashboard that displays various metrics of policy violations.

Access Risk Management

The solution shall support comprehensive risk assessment framework for measuring identity and access risk level on enterprise such as user, resource access, entitlement, role, policy violation, etc.
The solution shall support assigning risk value to target system access (for example, Active Directory account, SAP account, Unix account)
The solution shall support assigning risk value to target system entitlements (for example, Active Directory groups, SAP groups/roles/profiles)
The solution shall support assigning risk value to compliance policy (for example, SoD policy) to evaluate the risk of rule violations.
Mitigation controls can be assigned to compliance policy. The mitigation controls are implemented the moment the policy is violated to reduce the risk exposure.

The solution shall support assigning risk value to attestation policy if an attestation item is certified or denied.
The solution shall automatically calculate final risk level for the user based on all associated user accounts, directly and indirectly assigned applications, resources, membership in application roles and rule violations.
The solution shall automatically calculate final risk level for resource account based on all assigned target system entitlements.
The solution shall automatically calculate final risk level for company resources including department, location, cost center, role.
The solution shall support definition of rules that define how aggregated risk values are calculated.
The solution shall supply a comprehensive collection of default rules for calculating the risk value of all company resources assigned.
The solution shall support both weighting and normalization for calculating risk value.
Aggregated risk value can be derived by taking the highest risk value of all assigned company resources.
Aggregated risk value can be derived by taking the average of all assigned company resource risk values.
Aggregated risk value can be derived by taking the highest weighted risk value of all assigned company resources.
Aggregated risk value can be derived by taking the sum of all normalized to 1 and weighted assigned company resource risk values.
Risk calculation rule shall support the method of incrementing risk by a fixed value when certain condition is met.
Risk calculation rule shall support the method of decrementing risk by a fixed value when certain condition is met.
The solution shall provide dashboard and report to easily identify high risk objects such as users, user accounts.

Identity Audit

The solution shall support creation of custom attributes for user and account, track changes to the account, and audit attribute values.
The solution shall provide read-only overview of any item for which managers or compliance officers/auditors are responsible. You can use this to investigate any security issues that arise, or to verify activity.
Compliance officer or auditor shall have detailed view of users in the enterprise. The information shall include request, approval history, rule violation, roles, access, entitlements and history.
The detailed view of request shall show all the items that the user has requested, or that have been requested for him or her by another user.
The detailed view of approval history shall show the approvals in which the selected users participated within the selected time period.
The detailed view of policy violation shall show a list of violations within the selected time period.
The detailed view of access and entitlements shall provide an overview of all the user's resource accounts and their memberships.
The detailed view of history shall list all the property, membership and managerial changes and policy violations for the chosen time period.
Compliance officer or auditor shall have the view of roles and entitlements that can further drill in and examine the details that include memberships, permissions, policy violation and attestation history.
Compliance officer or auditor shall have the view of request that lists all requests that have been submitted with the selected time period.
For each request, compliance officer or auditor shall be able to see a variety of information including details of the requested item, status indicates the latest action performed on the request, details of the recipient and requester and any policy violations for the request.
Compliance officer or auditor shall have the view to review attestation processes within a specified time period.
Compliance officer or auditor shall have the view of all policy violations within a selected time period.

Report and Dashboard

The solution shall provide many out-of-box reports that cover organization, identity, entitlement, compliance, risk, provisioning, etc.
The solution shall provide built-in capability for creating custom report without relying on separate product.
Report shall support flexible presentation format with header, footer, title, text, font, style, table, chart, graph, image, etc.

The solution shall support building of custom report based on all available identity and access data including identity, resource access and entitlement, attestation, request, role, risk, etc.
Report can be saved or downloaded in multiple formats such as PDF, PowerPoint, Word, HTML, Excel, Text, Rich Text, CSV and image file.
The solution shall support creating custom report based on ad-hoc search results.
The solution shall support fine grained access control for report whereby a defined set of reports can only be viewed or downloaded by designated group of users.
The solution shall provide self-service function for user to download report on ad-hoc basis or schedule report to be sent via email with preferred format.
The report self-service shall allow user to send report via email to other users who are not authorized to run the report on ad-hoc or schedule basis.
Email template for sending report shall be customizable.
The solution shall provide out-of-box dashboard from web portal that provides business user or administrators overview of identity and access status in the whole enterprise.
The dashboard shall provide overview information related to compliance status, risk, policy, organization, request, attestation, target system and unstructured data access.
The dashboard shall support displaying statistic information such as number of pending request, requests from last month, number of user in certain department, etc.
The dashboard shall be easily customizable without coding.
The dashboard shall support various way of presentation using bar chart, pie chart, number, etc.
The content of dashboard shall be customizable without coding.
User shall be able to drill down from each dashboard item to look at detail content and relevant supporting data.

Solution Architecture

The solution shall support 3-tier architecture.
The solution shall support both vertical and horizontal scaling. Explain how both scaling methods can be achieved.
The solution shall support high-availability to eliminate any single point of failure.
The solution shall support running in virtualized environment.
The solution shall not require integration or customization among multiple products in order to provide comprehensive identity access governance capabilities.
The solution shall be modularized to allow deploying only required components to reduce the footprint and complexity of the implementation.
The solution shall embrace the concept of configuration as opposed to customization with tools for configuring workflow, web portal, and report.
The solution shall store all identity data, configuration changes and customizations in a central back-end repository instead of dispersed locations or repositories.
The central repository can be backed up and restored in the event of disaster recovery.
The solution shall support the ability to encrypt sensitive data stored in back-end repository.
The solution shall support extension of back-end repository database schema.
The solution shall provide application programming interfaces (APIs) or web services (e.g. SPML, SOAP, REST) that allow integration from other enterprise applications.
The solution shall support role base access control within the application that allows only authorized accesses for users which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.
The solution shall provide set of pre-defined roles within the application that are commonly used such as employee manager, role administrator, auditor, compliance officer, etc.
The solution shall support creation of custom role within the application.
The solution shall provide web portal for business user.
The web portal shall support Mozilla Firefox, Internet Explorer, Safari and Chrome.
The web portal shall provide HTML5 support for mobile end devices.
The solution shall support multiple authentication mechanisms such as Active Directory, LDAP, OAuth2, HTTP Header that can leverage on existing authentication source in the enterprise.
The solution shall support Single Sign-On using Windows Authentication out-of-box if users use Active Directory credential to access the solution.
The web portal shall support multiple languages and automatically show the language that is set in the web browser. Every user can also set a preferred language in his user profile.

The web portal shall support personalization capabilities that allow saving view configurations, such as sorting and filtering options and bookmark pages for quick access.
The solution shall support change management capability that allows configuration and customization changes be easily prompted from one environment to another.
The solution shall provide documentation capability that can generate reports to show current configurations and any customizations.