TechCorp IAM Solution Framework

Enhancing user lifecycle management:

* Custom client portal for customers, employees and vendors. Employees and vendors can have unique IDs that are different from the customer base. Employees can be given login credentials for first time sign-in. The employee credentials can have a fixed credential given by the IT Admin, and a changeable password for the employee to change to their preferred password. If TechCorp issues specific workplace devices to its employees, then SSO can be enabled with MFA. Clearly defined user access policies can be configured to automate the process for onboarding and offboarding of employees. Newer employees can get access to resources they need to start training while former employees can be removed from accessing resources, all through the access policies.
* For vendors, clearly defined RBAC policies, issuing vendor IDs, and MFA using OAuth 2.0
* For customers, clearly defined RBAC policies, providing usernames and passwords, MFA with SSO through email, and account recovery method.

Strengthening access control mechanisms:

* OAuth 2.0 and SAML can be used for passwordless authentication. SAML for web-based SSO for customers, and OAuth 2.0 for vendors.
* Privileged access management (PAM) for safeguarding access to critical data and systems to privileged users in the company.

The suggested solution for user lifecycle management simplifies the process of onboarding and offboarding, provisioning and deprovisioning of user account and access rights. Having clearly defined role-based access policy for employees allows to quickly revoke and delete access of former employees and easily provide access to new employees. This streamlines with the company’s goal of fortifying access control mechanisms, user access during onboarding and offboarding, and provisioning and deprovisioning of user accounts and access rights.

SAML provides a web-based SSO which will not degrade user experience. SAML provides MFA while maintaining good user experience.

PAM streamlines with the company’s objective to have RBAC and least privilege access in the system.Example technologies to use is Okta.