

2. Authorization Governance

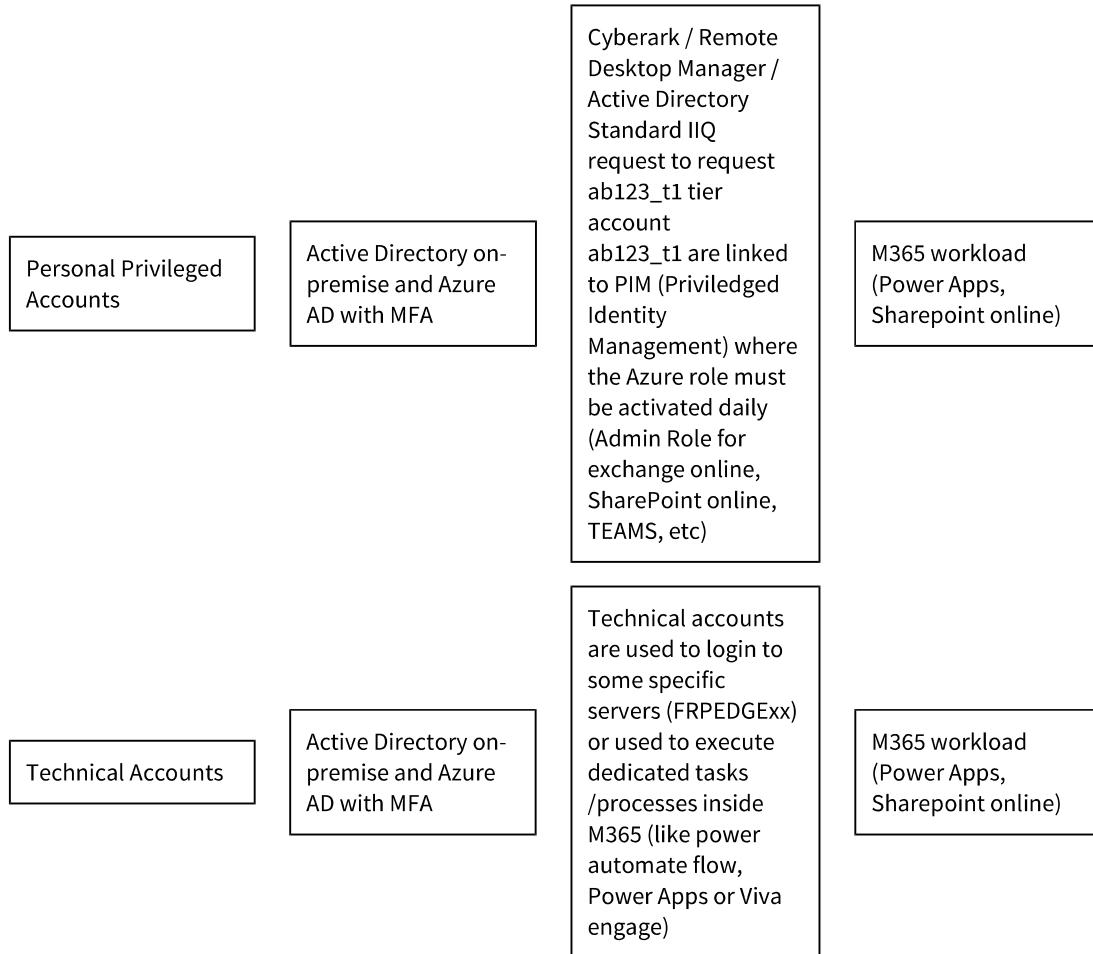
2 Authorization Governance

Authorization is a central part of the IAM processes once the user has been authenticated. Users are granted authorizations according to their role at an organization (“role-based access control” (RBAC)). Authorizations determine a role’s resources and level of access to the IT Asset.

Please describe how authorization of authenticated users is managed in the table below.

Note: Only user access types should be mentioned here. No external users are required. Only internal users (= internal and external employees, which are managed by HR).

User access type	Authorization source /store	Description	Further information
Personal Accounts	Active Directory on-premise and Azure AD with MFA	<p>All user id (including their field properties like name, user id, smtp address, phone, unit, etc) are synced from our active directory on-premise to Azure Active Directory. This is done with Azure AD Connect (AD Connect)</p> <p>ADFS</p>	<p>User password is checked in AD during the authentication process</p> <p>Standard IIS request when a new user is on-boarding</p>



Comments:

See in section 4.3 the technical user ids used by the different M365 workload (Exchange online, SharePoint Online, Power Automate, Power Apps, Viva Engage, etc)

* The term “authorization” refers to the procedure of granting access to the IT Asset’s data or functions during run-time. Not to be mixed with Access Governance topics, e.g. request of role-based access, user recertification, etc.