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	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) ADFS	User password is checked in AD during the authentication process Standard IIQ request when a new user is on-boarding

Personal Privileged Accounts	Active Directory on-premise and Azure AD with MFA	Cyberark / Remote Desktop Manager / Active Directory Standard IIQ request to request ab123_t1 tier account ab123_t1 are linked to PIM (Priviledged Identity Management) where the Azure role must be activated daily (Admin Role for exchange online, SharePoint online, TEAMS, etc)	M365 workload (Power Apps, Sharepoint online)
Technical Accounts	Active Directory on-premise and Azure AD with MFA	Technical accounts are used to login to some specific servers (FRPEDGExx) or used to execute dedicated tasks /processes inside M365 (like power automate flow, Power Apps or Viva engage)	M365 workload (Power Apps, Sharepoint online)

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.