

3. Access Governance

3 Access Governance

Access governance description is subdivided into several processes, such as Request and Approval process, Provisioning and Assignment of Access rights, Recertification and Reconciliation. In this chapter access governance should be described for all types of accounts, which have diverse access procedures.

3.1 Request & Approval of Access

Request and approval are a procedure of how access to an IT Asset is requested and how it is formally approved or rejected.

Please describe access governance for each user type accordingly.

Note: Description of request and approval access per user type is only required in case if the procedure differs for each type. In the 5th column, please specify whether the requested access rights are on role level (default) or on entitlement level (requires justification) – see Figure 1.

Account Type	Process	Onboarded IIQ?	Short process description or link to existing documentation	Role, policy, attribute or entitlement level?

Personal Account	<p>All users created in Active Directory on-premises are automatically onboarded with IIQ. Then users are sync to Azure AD. Users are added as well to O365-LG-E5-std and O365-LG-EXO to get the M365 licenses. For PowerBI, Visio, Projects and other M365 licenses are provided through Jira and/or IIQ request</p>	yes	<p>For specific licenses (Visio, Project, Visual studio enterprise, Teams Premium), the jira request is raised then users are added to a windows group. The license provisioning is linked to these windows AD group.</p>	
Personal Privileged Account	<p>ab123_t1 users created in Active directory on-premises are automatically onboarded with IIQ and CyberArk. Then users are sync to Azure. ab123_t1 have to active their Azure Admin role to grant accesses to exchange, sharepoint, Teams, etc administrator</p>	yes	<p>PIM is used to grant access to the ab123_t1 , Privilege Identity Management</p>	

Shared Account	<p>Account which are disabled are automatically created when a shared mailbox is created. Disabled user id are created in Active Directory on-premises, then sync to Azure /Exchange online</p>	yes		
Technical Account	<p>All users created in Active Directory on-premises are automatically onboarded with IIQ. Then users are sync to Azure AD. Users are added as well to O365-LG-E5-std and O365-LG-EXO to get the M365 licenses. These users are used to execute some tasks /processes in M365 (like power Automate flow, power apps, viva engage port messages)</p>	yes		