

For cloud IT assets:

Note: For Cloud IT Assets, accounts cannot be discovered via IIQ. Hence, it is mandatory to describe in detail how they are being provisioned.

Account Name / Tag	Assignment Condition	Provisioning process / mode	Description of applied controls to tagged object

Comments:

See the list of technical accounts in chapter 4.3

3.3 Recertification

Recertification of a role and / or user access is a process of regular review of each formerly requested and currently assigned access rights with the possibility of either approve or revoke the access. The verification / regular recertification of the user’s or role’s assigned access rights must be carried out on a least-privilege and need-to-know basis in accordance to the Access Control Standard and the IAM Guideline.

Please describe the recertification process for roles and user access in the table below.

Note: Please describe the way of recertification of Cloud end-point assets when they are not done via IIQ directly. Description of recertification per user type is only required in case if the procedure differs for each type.

Account Type	Process	Onboarded IIQ?	Process description or link to existing documentation
Personal Account	Once the user is leaving the company, there is an automatic off-boarding process done by "Security IT Access & File transfer Center (U)" which is removing the M365 license and automatically the access to the M365 feature (M365 apps, One drive online, sharepoint online, Teams, Viva Engage, etc)	yes	
Personal Privileged Account	Yearly review of the ab123_t1 who got access to the different PIM azure group which are providing the accesses to the different Azure Admin role	no	Currently the recertification is done manually by the global admin of the M365 tenant. Once IIQ implemented (as explained previously), the review of the PIM-T1-xxxx administrator will be part during the IIQ recertification timeframe window.
Technical Account	Yes recertification done twice a year to access some resources 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)	yes	

Comments:

Recertification for users accessing some M365 custom apps (DBG intranet, Power Apps, SharePoint online customized , etc) : As integrated in IIQ, recertification is done based on yearly process like all other IIQ accesses