# 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)<br><br>ADFS | User password is checked in AD during the authentication process<br><br>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.

# 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 | 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 | yes | 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. | |
| Personal Privileged Account | 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 | yes | PIM is used to grant access to the ab123_t1 , Privilege Identity Management | |

| | | | | |
|---|---|---|---|---|
| Shared Account | 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 | yes | | |
| Technical Account | 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 messsages) | yes | | |

Comments:

* Teams' creation and access: Users who needs a TEAMS can raise a JIRA request. The Teams group is created, and the owners of the Teams are responsible to manage their different access rights for internal member and guests.

* SharePoint online Site creation: Intranet link request, the user will ask for site creation, and it must be approved by SharePoint Admin Team with some requirements (Site owner list (minimum 2 owners), name of the site,). Every 3 months, a report with all the user's accesses is generated and sent to the sharepoint online site's owners.
https://deutscheboerse.sharepoint.com/sites/SPONewSiteRequest

* Access management on sites on sharepoint online: Owners must provide access to users who need it. This part is managed by owners because they are also responsible for content management and content sharing.
A report of sharepoint site access is provided every 3 months to the sharepoint site owner for review.

## 3.2 Provisioning & Assignment of Access

**Please describe how the access change is technically enforced and how the access rights assignment process is structured (how the provisioning of access rights is executed, is it an automated or a manual process) once access is requested.**

Note: Description of provisioning and assignment of access per user type is only required in case if the procedure differs for each type. Bi-directional means automated fulfilment via the IIQ connector to the app and a response to IIQ that it has been completed. Uni-directional is only one way and manual would be that there are work items generated for a user access administration to manually fulfil.

**For all IT assets:**

| Account Type | Process | Onboarded IIQ? | Short process description or link to existing documentation |
|---|---|---|---|

| | | | |
|---|---|---|---|
| Personal Account | All DBG employees are automatically assigned to a windows security group during the user id provisioning. The users will receive automatically a M365 license and got access to the main M365 feature (Office apps, One drive and sharepoint online, Exchange online, Teams) | yes | |
| Personal Privileged Account | User ab123_t1 are using the PIM (Priviledge Identity Management) system to receive their M365 administrator role like exchange online, admin, sharepoint online admin, Teams administrator, Intune admin, etc are done with built-in Azure AD role. | yes | An excel sheet is used for the moment to have a view of each admin user assigned to each M365 azure admin Role.<br><br>With PIM (Privilege Identity Management), each administrator azure role must enable his role daily. The ab123_t1 tier user id is member of PIM-T1-xxxxxx azure group to be eligible to have this azure administrator role right.<br><br>IIQ unit is working to onboard the membership of these azure AD groups (PIM-T1-xxxxxx) in IIQ role. These IIQ role will be linked to AID415 (Corporate IT Active Directory – IIQ role: EntraID - Production - Role Owner) |
| Technical Account | 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 messsages) | yes | |

**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.<br>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<br>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 messsages) | 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

## 3.4 Reconciliation

Reconciliation of access is a periodic, automatic review process, which checks if the assigned access rights in the target systems (as-is state) are matching with the initially requested ones (to-be state). In case of discrepancies between as-is and to-be state, reconciliation also rectifies the gap by enforcing the to-be state to be implemented.

**Please describe the reconciliation process accordingly.**

Note: Description of reconciliation per user type is only required in case if the procedure differs for each type. If you are not sure if reconciliation for an IT Asset is activated, please contact IIQ Team:

| Account Type | Process | Onboarded IIQ? | Short process description or link to existing documentation |
|---|---|---|---|
| Personal Account | Not required as each user who has a valid user id received by "Security IT Access & File transfer Center", has a M365 license and can access the basic M365 feature. | yes | |
| Privileged Personal Account | Done every 6 months manually by the global administrator of the tenant. IIQ recertification of the PIM-T1-xxx administrator group on-going | no | |

| | | | |
|---|---|---|---|
| Technical Account | Yes recertification done twice a year to access some resources<br>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 messsages) | yes | |

Comments:

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