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. 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. 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.