Core Process (No.)	Sub Process (No.)	Target
MAINTAIN ACCOUNTS (1)	Add 'User', account (1.1) (including creation of the unique User-id)	• Timely creation of all 'User' accounts for new 'employees' (including contractual staff), which are necessary for User's job. • A formal 'User' registration procedure is a basic security requirement. • To create personal accounts and system/technical accounts via one process. • To ensure that each 'User' on the system is identifiable by a global unique User-id (each request form must contain a unique User-id).
MAINTAIN ACCOUNTS (1)	Delete 'User', account (1.2)	• Timely deletion of all 'User' accounts for 'employees' (including contractual staff) who have left the company. • Deletion of 'User' accounts, which are no longer necessary for User's job. • To delete personal accounts and system accounts via one process.
MAINTAIN ACCOUNTS (1)	Automatical triggered changes (1.3) - Change 'User' name - Change expiry date	• 'User' names are up to date in all relevant systems. • For correct referencing across Systems and Databases consistent updates of 'User' names are of paramount importance. • Every name change of any 'User' has to be maintained via this process. • There is no manual request for changing the name allowed. Only name changes in the HR database will trigger this process automatically. • 'User' accounts with an expiry date (mainly external staff) are available only when needed, no shorter and no longer. After the expiry date is reached, the account is automatically disabled by the system itself or manually by the responsible 'System Administrator'. • Every expiry date change of any account has to be maintained via this process. • There is no manual request for changing the expiry date allowed.
MAINTAIN ACCOUNTS (1)	Manual triggered changes (1.4) - Change account name	• To support a process of changing account names for name based accounts, without loosing access rights or 'User' data. • Each account name change has to be maintained via this process. • There is no automatic request for changing the account name allowed.
MAINTAIN ACCOUNTS (1)	Enable/Disable account (1.5)	• To restore access rights for a previously disabled 'User' account. • Disable 'User' accounts without deleting, so they can be restored easily by the enabling process if necessary. • Disable 'User' directly after their expiry date in the HR database is reached. • Offer a quick process for disabling, as it is usually a time critical task (including emergency route).

Core Process (No.)	Sub Process (No.)	Target
MAINTAIN ACCOUNTS (1)	Set password (1.6)	• Provide a secure and efficient process for password requesting and delivery. • Has to include Out-of-band Verification for Password Resets
ASSIGN ACCESS RIGHTS (2)	Add/Remove access rights (2.1)	• To ensure that all accounts have proper authorisation. • To maintain also system accounts via this process. • To maintain also changing of special account-information (e.g. system specific fields) via this process. • Assignment/Deletion of access rights according to the functional needs is a fundamental requirement of security.
ASSIGN ACCESS RIGHTS (2)	Change department (2.2)	• To ensure all accounts have proper authorisation. • To ensure department code for ‘employee’ is valid at all times. • To ensure both departments (old and new) take part in the department change process. • To avoid an ‘employee’ having inappropriate access to data from the old department. • All department changes for all ‘employee’s must be maintained via this process. • There is no manual request for changing the department allowed.
MAINTAIN ACCESS RIGHTS (3)	Create/Modify/Delete group/profile/role	not defined yet
DETECT INCONSISTENCIES (4)	Show unknown people (in the IdM system, not on the HR database) (3.1)	• To identify the missing persons in the HR database and improve the quality of the the HR database data through the IdM system. • To ensure that nobody uses a system without being in the HR database. • To provide management with information about the the HR database data quality.
DETECT INCONSISTENCIES (4)	Show leavers (on Should, not on Belong) (3.2)	• To identify the open ‘Should’ records for users who have already left the company. • To improve the quality of the the IdM system data. • To reduce the risk of misuse of unused accounts.
DETECT INCONSISTENCIES (4)	Show mistakes (on Actuality, not on Belong) (3.3)	• To identify the open system accounts for users who have already left the company. • To improve the quality of the system data. • To reduce the risk of misuse of unused accounts.

Core Process (No.)	Sub Process (No.)	Target
DETECT INCONSISTENCIES (4)	Show execution error/hacker (on Actuality, not on Should) (3.4)	• To ensure that all accounts (access rights), which find their way into a system without going through administration will be detected and could be checked (could be an indication of intruders on the system). • To identify problems with the execution of account deletion and/or removing of authorities.