MICROSOFT OFFICE 365 Authorization concept

Introduction

Introduction

Welcome to the digital authorization concept of the application MICROSOFT OFFICE 365 (AID551)!

The authorization concept is a systematic approach to managing and controlling access rights and authorizations within an IT system or organization. Its primary objective is to ensure that only authorized individuals can access specific data, applications, or resources, thereby safeguarding the confidentiality, integrity, and availability of information. All pertinent information should be documented centrally to meet regulatory requirements.

The current authorization concept template comprises the following chapters: General Information, IT Asset Description, Authorization Governance, Access Governance, Authorization Objects, Entitlements, IT Roles, Account Management, Segregation of Duties, References, and List of Abbreviations. Each chapter is briefly outlined below:

General Information

The General Information chapter includes the Introduction (this page) and Change History. This chapter outlines the basics of the authorization concept and the structure of the document. The Change History section logs versions of the document, detailing the author, date, and comments. A new version is created automatically when the authorization concept successfully passes the approval process.

IT Asset Description

This chapter documents general information about the IT asset, including master data about the application, the environment landscape, and the infrastructure components in use.

Authorization Governance

This chapter describes the implementation of authorization and authentication.

Access Governance

The Access Governance chapter details the entire process of assigning access to the application.

Authorization Objects

This section documents the central authorization objects, including entitlements, IT roles, accounts, and their attributes.

Entitlements

The Entitlements section includes two key pages: Entitlements General Information and Entitlement Services. The Entitlements General Information page provides basic information about entitlements, while the Entitlement Services page allows for the editing of master data for imported entitlements. Additionally, this section accommodates the documentation of entitlements not present in IIQ.

IT Roles

The IT Roles chapter is comprised of IT Roles General Information and IT Role Services pages. The IT Roles General Information page offers basic details about IT roles, whereas the IT Role Services page facilitates the creation and management of IT Roles.

Account Management

The Account Management chapter includes pages for Special Accounts General Information and Special Account Services. Special Accounts General Information explains the various types of special accounts, while Special Account Services allows for the creation of accounts for documentation purposes and the editing of master data.

Segregation of Duties

This chapter serves to document violations of segregation of duties (SoD). It allows for the documentation of SoD areas for applications not onboarded to IIQ, as well as the visualization of the functional area matrix in general.

References

Provides references to further documents.

List of Abbreviations

Lists all abbreviations used in this document.

Change History

Change History

Created by	Created at	Comment	Version	Action	Changed pages	Workbook version
Linnevers, Carolyn (8a7e5969577640ff01591d99efa535c3)	Nov 4, 2025, 4:39 PM		69			
Deschamps, Stéphane (8a7e5969577640ff01591da383d54d2a)	Nov 3, 2025, 9:08 AM		68			
Moravec, Andreas (8a7e5969577640ff01591da5c05a52fd)	Oct 31, 2025, 11:36 AM		67			
O'Brien, Eamonn (8a7e596a624f2eb30162dc347e2a3d01)	Oct 31, 2025, 11:23 AM	Checks made on Privilege access for CyberArk and descriptions. Improvement opportunity. I could not find reference to Lock Box for when access is granted to the Microsoft engineer in an emergency. Perhaps could be in Special Accounts General information	66			
Leorda, Dragos (0afed9ea84471373818487eed7a64360)	Oct 31, 2025, 9:49 AM	Signed off	65			
Krier, Benoit (8a7e5969577640ff01591dadcc92670d)	Oct 31, 2025, 9:31 AM	New IIQ roles added for Paper Archive application and new technical reviewer	64			
Kreuz, Carsten (8a7e596a6fdc1895016ffa230ca20095)	Sep 19, 2025, 8:15 AM		63			

Created by	Created at	Comment	Version	Action	Changed pages	Workbook version
Deschamps, Stéphane (8a7e5969577640ff01591da383d54d2a)	Sep 11, 2025, 4:10 PM		62			
Luckenbach, Julian (8a7e5969577640ff01591da4ccdc50a1)	Sep 11, 2025, 2:14 PM	no further comments from EEX / ECC from our customer perspective	61			
Fiekert, Thorsten (8a7e59695df0640e015e128bb0410e06)	Sep 11, 2025, 1:20 PM	Approved from my side, taking into account the changes and comments made since the last approval.	60			
Malréchauffé, Anne-Pascale (8a7e5969577640ff01591daab6655f61)	Sep 11, 2025, 11:58 AM	I hereby provide my approval for the finalisation of the DAC based on the prior reviews conducted by the IT Application Owner and the Business Owner.	59			
Moravec, Andreas (8a7e5969577640ff01591da5c05a52fd)	Sep 11, 2025, 11:41 AM		58			
Linnevers, Carolyn (8a7e5969577640ff01591d99efa535c3)	Sep 11, 2025, 11:03 AM		57			
Puaud, Martin (8a7e5969577640ff01591d9ea9d14101)	Sep 11, 2025, 10:56 AM	Add several IIQ roles requested by several unit for AID551 (PaperArchice, CALTERM PowerApps, PowerBI reports, Clearstream RPA)	56			

Created by	Created at	Comment	Version	Action	Changed pages	Workbook version
Krier, Benoit (8a7e5969577640ff01591dadcc92670d)	Sep 11, 2025, 10:14 AM	several IIQ roles for several new entlitlements added recently (powerbi access, power apps accesses , etc)	55			
Luckenbach, Julian (8a7e5969577640ff01591da4ccdc50a1)	Jul 31, 2025, 1:17 PM		54			
Fiekert, Thorsten (8a7e59695df0640e015e128bb0410e06)	Jul 29, 2025, 5:12 PM	No further review comments besides the one already made in the change history.	53			
Malréchauffé, Anne-Pascale (8a7e5969577640ff01591daab6655f61)	Jul 29, 2025, 12:57 PM	I hereby provide my approval for the finalisation of the DAC based on the prior reviews conducted by the IT Application Owner and the Business Owner.	52			
Gast, Frank (8a7e5969577640ff01591dab7e846152)	Jul 29, 2025, 9:01 AM		51			

Created by	Created at	Comment	Version	Action	Changed pages	Workbook version
		Approved with some remarks to be considered for future iterations. New roles need to be created and made available. A more consistent and complete version of the documentation is expected next time. • In Chapter 4.1. - Entitlements General Information SoD relevancy: The current classification of the application as “Functional Area relevant” is inaccurate. While the application may not be relevant for business-level Segregation of Duties, it is indeed relevant from an IT SoD perspective—specifically in the context of IT Development and IT Operations. These are common IT SoD categories and should not be confused with Functional Area Tags. To ensure clarity, it is recommended to mark the application as SoD relevant. A clarifying comment should be added to indicate that the relevance pertains exclusively to IT SoD categories. • In Chapter 4.1 Entitlements, it remains unclear why no file has been uploaded				

Created by	Created at	Comment	Version	Action	Changed pages	Workbook version
Deschamps, Stéphane (8a7e5969577640ff01591da383d54d2a)	Jul 23, 2025, 4:01 PM		49			
Moravec, Andreas (8a7e5969577640ff01591da5c05a52fd)	Jul 23, 2025, 3:42 PM		48			
Caligaris, Marco (8a7e5969577640ff01591daad5cc5fa1)	Jul 23, 2025, 3:01 PM		47			
Puaud, Martin (8a7e5969577640ff01591d9ea9d14101)	Jul 23, 2025, 2:55 PM	DAC reviewed	46			
Krier, Benoit (8a7e5969577640ff01591dadcc92670d)	Jul 23, 2025, 2:43 PM	We have 10 more IIQ roles to create	45			

Created by	Created at	Comment	Version	Action	Changed pages	Workbook version
		Approved with some remarks to be considered for future iterations. New roles need to be created and made available. A more consistent and complete version of the documentation is expected next time. In Chapters 2 and 3, there is no mention of technical accounts. However, multiple technical accounts are listed in Chapter 4.3. For consistency and completeness, I recommend referencing these technical accounts accordingly in Chapters 2 and 3. This will help ensure alignment across the documentation and provide a clearer overview of account usage. In Chapter 4.1 Entitlements, under the Entitlements Services page within entitlement attribute management, the "meaningful description" field is currently not populated for all entitlements. Since some of these descriptions—particularly those originating from Active Directory—are linked to				

Created by	Created at	Comment	Version	Action	Changed pages	Workbook version
Deschamps, Stéphane (8a7e5969577640ff01591da383d54d2a)	Jul 16, 2025, 6:23 PM		43			
Luckenbach, Julian (8a7e5969577640ff01591da4ccdc50a1)	Jul 15, 2025, 4:14 PM	confirmed by July 15th with Marc Boening	42			
Linnevers, Carolyn (8a7e5969577640ff01591d99efa535c3)	Jul 9, 2025, 3:35 PM		41			
Moravec, Andreas (8a7e5969577640ff01591da5c05a52fd)	Jul 9, 2025, 11:44 AM		40			
Gast, Frank (8a7e5969577640ff01591dab7e846152)	Jul 9, 2025, 10:38 AM		39			
Leorda, Dragos (0afed9ea84471373818487eed7a64360)	Jul 9, 2025, 10:29 AM	signed off	38			
Krier, Benoit (8a7e5969577640ff01591dadcc92670d)	Jul 9, 2025, 9:29 AM	New IIQ role added to request a power apps license for the new Atlas application	37			
Deschamps, Stéphane (8a7e5969577640ff01591da383d54d2a)	Jun 17, 2025, 8:27 AM		36			
Linnevers, Carolyn (8a7e5969577640ff01591d99efa535c3)	Jun 16, 2025, 5:52 PM		35			
Gast, Frank (8a7e5969577640ff01591dab7e846152)	Jun 13, 2025, 2:27 PM		34			
Rick, Jens (8a7e59696acc1e13016b44dbab0d4757)	Jun 13, 2025, 1:19 PM		33			

Created by	Created at	Comment	Version	Action	Changed pages	Workbook version
Moravec, Andreas (8a7e5969577640ff01591da5c05a52fd)	Jun 13, 2025, 1:08 PM		32			
Leorda, Dragos (0afed9ea84471373818487eed7a64360)	Jun 13, 2025, 8:36 AM	Signed off	31			
Krier, Benoit (8a7e5969577640ff01591dadcc92670d)	Jun 12, 2025, 6:49 PM	New IIQ roles for ECC_Notification and BPR applicaitons	30			
Gast, Frank (8a7e5969577640ff01591dab7e846152)	May 28, 2025, 6:10 PM		29			
Linnevers, Carolyn (8a7e5969577640ff01591d99efa535c3)	May 27, 2025, 3:08 PM		28			
Deschamps, Stéphane (8a7e5969577640ff01591da383d54d2a)	May 27, 2025, 2:11 PM		27			
Moravec, Andreas (8a7e5969577640ff01591da5c05a52fd)	May 27, 2025, 12:45 PM		26			
Rick, Jens (8a7e59696acc1e13016b44dbab0d4757)	May 27, 2025, 11:01 AM		25			
Leorda, Dragos (0afed9ea84471373818487eed7a64360)	May 27, 2025, 10:49 AM	Signed off	24			
Krier, Benoit (8a7e5969577640ff01591dadcc92670d)	May 27, 2025, 10:42 AM	ok 15 new IIQ roles to create for Power Apps application and Copilot Studio	23			
Fiekert, Thorsten (8a7e59695df0640e015e128bb0410e06)	May 16, 2025, 3:37 PM		22			

Created by	Created at	Comment	Version	Action	Changed pages	Workbook version
Deschamps, Stéphane (8a7e5969577640ff01591da383d54d2a)	May 16, 2025, 10:50 AM		21			
Linnevers, Carolyn (8a7e5969577640ff01591d99efa535c3)	May 12, 2025, 9:39 AM		20			
Hampel, Stephan (8a7e596959c57ed6015a3b2b39fd72c6)	May 8, 2025, 10:14 AM	Approved!	19			
Gast, Frank (8a7e5969577640ff01591dab7e846152)	May 6, 2025, 5:08 PM		18			
Rick, Jens (8a7e59696acc1e13016b44dbab0d4757)	May 6, 2025, 2:16 PM		17			
Moravec, Andreas (8a7e5969577640ff01591da5c05a52fd)	May 6, 2025, 1:23 PM		16			
Leorda, Dragos (0afed9ea84471373818487eed7a64360)	May 6, 2025, 10:08 AM	Signed off	15			
Krier, Benoit (8a7e5969577640ff01591dadcc92670d)	May 6, 2025, 9:54 AM	ok reviewed the 06/05/2025	14			
Hampel, Stephan (8a7e596959c57ed6015a3b2b39fd72c6)	May 5, 2025, 1:25 PM	as agreed once more to be declined. Can be sent to approval after next Nexis Import again.	13			
Rick, Jens (8a7e59696acc1e13016b44dbab0d4757)	May 5, 2025, 1:17 PM		12			
Leorda, Dragos (0afed9ea84471373818487eed7a64360)	May 5, 2025, 1:01 PM	Signed off	11			

Created by	Created at	Comment	Version	Action	Changed pages	Workbook version
Krier, Benoit (8a7e5969577640ff01591dadcc92670d)	May 5, 2025, 12:56 PM	ok	10			
Hampel, Stephan (8a7e596959c57ed6015a3b2b39fd72c6)	Apr 25, 2025, 2:03 PM	MS Exchange - Excel Exception Roles do not have entitlements. Please ensure that all entitlements are correctly be linked to the application AID551 in IIQ. This is currently not the case.	9			
Rick, Jens (8a7e59696acc1e13016b44dbab0d4757)	Apr 25, 2025, 9:21 AM		8			
Gast, Frank (8a7e5969577640ff01591dab7e846152)	Apr 24, 2025, 9:08 AM		7			
Moravec, Andreas (8a7e5969577640ff01591da5c05a52fd)	Apr 23, 2025, 7:03 PM		6			
Linnevers, Carolyn (8a7e5969577640ff01591d99efa535c3)	Apr 23, 2025, 3:53 PM		5			
Linnevers, Carolyn (8a7e5969577640ff01591d99efa535c3)	Apr 23, 2025, 3:48 PM		4			
Deschamps, Stéphane (8a7e5969577640ff01591da383d54d2a)	Apr 23, 2025, 2:36 PM		3			
Leorda, Dragos (0afed9ea84471373818487eed7a64360)	Apr 23, 2025, 1:54 PM	Confirmed	2			
Krier, Benoit (8a7e5969577640ff01591dadcc92670d)	Apr 23, 2025, 11:02 AM	ok	1			

1. IT Asset Description

1 IT Asset Description

The current chapter is aimed to provide general information regarding the IT Asset, including environment landscape and used infrastructure components.

1.1 General Information

Please provide basic IT Asset Information

CMS Product ID	1513344
IT Asset ID:	AID551
IT Asset Name:	MICROSOFT OFFICE 365

For IT Applications, please provide the screenshot/report from APMS with the time stamp on it as an evidence in case IT Asset information changes between concept review cycles. The information extract (screenshot or report) should contain the following information:

IT Applicaton Owner	Role: AID551 - Application Owner [Krier, Benoit (8a7e5969577640ff01591dadcc92670d) | Halligan, Dean (8a7e5969577640ff01591da4497a4f50)]
Business Owner	Role: AID551 - Business Owner [Krier, Benoit (8a7e5969577640ff01591dadcc92670d) | Leveling, François (8a7e5969577640ff01591da2920d4aee)]
Contributor	Role: AID551 - Contributor [Krier, Benoit (8a7e5969577640ff01591dadcc92670d)]

Technical Reviewer	Leorda, Dragos (0afed9ea84471373818487eed7a64360)
TISO	Role: AID551 - Technical Information Security Officer [Bössow, Holger (0afed9ea7db51d06817dc59582667aac) | Jouanne, Alexis (8a7e596973a0f1b60173a1d9c87c3091)]
Max. Confidentiality	Critical
Max. Integrity	Critical
Max. Availability	Critical
Max. Authenticity	Critical
Max. Criticality	Critical
IIQ onboarded	Technical Onboarded
SIEM onboarded	Onboarded
Product Version	SaaS - Deployment Date: 2022-08-01 - Decommision Date:
Product Line	Product-14 Product-Corporate IT
Application Support Group	IT CRP MS Ex
Application Hosting	Service Provider only
Legal Entity	

Legal Entity Type	Legal Entity ID	Display name	Information Owner	Entity Usage Type	Entity Core Application	Max. Criticality	Max. Confi
Using	0001998876	Börse Frankfurt Zertifikate AG	LU274, ZZ320	Service	yes	Critical	Critic
Using	0001996593	Clearstream Banking S.A.	LD865, IK893	Application	yes	Critical	Critic
Using	0001996602	Clearstream Europe AG	OL560	Application	no	Major	Critic
Using	0001999700	Clearstream Fund Centre S.A.	LQ814, TU452	Application	no	Major	Critic
Using	0001997037	Clearstream Holding AG	TE030	Service	no	Major	Critic

Legal Entity Type	Legal Entity ID	Display name	Information Owner	Entity Usage Type	Entity Core Application	Max. Criticality	Max. Confi
Using	0001997038	Clearstream International S.A.	JH088	Application	yes	Critical	Critic
Using	0001950847	Clearstream London Limited		Application	no	Major	Critic
Using	0001997039	Clearstream Services S.A.	MG491	Application	yes	Critical	Critic
Using	0001998203	Deutsche Boerse Systems Inc.		Application	yes	Critical	Critic
Owning	0001996597	Deutsche Börse AG	SB277, TA190, RQ049, HL636		no		

Legal Entity Type	Legal Entity ID	Display name	Information Owner	Entity Usage Type	Entity Core Application	Max. Criticality	Max. Confi
Using	0001996597	Deutsche Börse AG	SB277, TA190, RQ049, HL636	Application	no	Major	Critic
Using	0001950294	Deutsche Börse Digital Exchange GmbH		Application	yes	Critical	Critic
Using	0001998967	Deutsche Börse Services s.r.o.	RS044	Application	no	Major	Critic
Using	0001996594	Eurex Clearing AG	OW272, AI423	Service	no	Major	Critic

Legal Entity Type	Legal Entity ID	Display name	Information Owner	Entity Usage Type	Entity Core Application	Max. Criticality	Max. Confi
Using	0001996598	Eurex Frankfurt AG	OQ959, OS261	Application	no	Major	Critic

Comments:

1.2 Environment Landscape

Please mark the environments where production/ production-like (live) data is used.

Note: All IT-assets hosting Production and Production-like data (e.g., Simulation) on-premise and in the cloud are subject to IIQ onboarding, in order to ensure proper access compliance in accordance with the Access Control Standard.

For all other environments, it is the task of the Information Owner to assess the criticality of information and data handled by the IT-asset. Therefore, some IT-assets from “Simulation” environments could possibly contain “production like” data / information and therefore need to be onboarded to IIQ.

Environment	Data location (on-premise vs. cloud-provider)	Production-like data hosted /used
Production	cloud-Azure	yes

Simulation		
Acceptance		
Test	cloud-Azure	no
Development		

Comments:

1.3 Used Infrastructure Components

Please indicate here which infrastructure components are necessary for the operation of your IT-asset and which kind of technology it is (Operating System=OS, Database=DB, Middleware=MW, File Share=FS, etc.). If the infrastructure component is a file share, the UNC-Path needs to be provided in the column “Description”.

Note: If you fill in the AC for an infrastructure component, please insert the list of IT Applications which use this infrastructure component as well.

CMS-Product-ID	Display name	Enviroment	Server Partnername	OS Type	SubType	Type	Server state
1591896	FRPMSOPS365	PROD	IT CRP Windows Server Management	Windows		SERVER_DEVICE	In Service

CMS-Product-ID	Display name	Enviroment	Server Partnername	OS Type	SubType	Type	Server state
1243845	FRPSPDAG01	PROD	IT CRP Windows Server Management	Windows		SERVER_DEVICE	In Service
1243843	FRPSPDAG02	PROD	IT CRP Windows Server Management	Windows		SERVER_DEVICE	In Service
1244819	FRPSPMIG	PROD	IT CRP Windows Server Management	Windows		SERVER_DEVICE	In Service
1588353	FRPSPMIG01	PROD	IT CRP Windows Server Management	Windows		SERVER_DEVICE	In Service

CMS-Product-ID	Display name	Enviroment	Server Partnername	OS Type	SubType	Type	Server state
1970111	MITMSOPS365	ACCEPT /TEST	IT CRP Windows Server Management	Windows		SERVER_DEVICE	In Service
1241797	MITSPDAG11	TEST	IT CRP Windows Server Management	Windows		SERVER_DEVICE	In Service

Add infrastructure Components:

Display name	Enviroment	Support Group	Type	Server State	SubType
Citrix Server	Prod	Windows Server Management	Windows Server		
Windows 10/11 device (Lenovo laptop /Tablet)	Prod	Endpoint Devices Operations	Windows 10/11		

Windows 365	Prod	Endpoint Devices Operations	Windows 365		
Network Infrastructure and connectivity to M365	Prod	Network Security & Services	Cisco appliance /Router /Firewall		
Microsoft 365 Office Click-to-Run	Prod	Endpoint Devices Operations	Microsoft 365 Office Click-to-Run		
Microsoft 365	Prod	Microsoft 365 Operations	Microsoft 365 / Saas		

Comments:

* Updates are necessary in alignment with the update of the Security Documentation

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) ADFS	User password is checked in AD during the authentication process 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. 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.

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 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 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.

4. Authorization Objects

4 Authorization Objects

Authorization objects play an important role for authorization checks as they determine which access can be assigned to the users. They usually contain elements to control the access specifically for the IT Asset and can group together technical elements needed to design to access control (e.g. fields, groups etc.). These objects need to be protected and stored in the authorization source.

In the current chapter the following access type classification is used (see IAM Guideline, chapter 4):

- **Business Access (BA)**

  Is defined as a subset of required access permissions to perform a well-defined and documented activity in an IT Asset. Business Access is assigned to support and / or perform operational tasks in a non-administrative context (e.g. regular user authorizes himself to release payments to certain amount). This can be/has been mentioned as Tier 3 in IIQ.

- **Business Critical Access (BCA)**

  Is derived from the criticality of an IT Asset defined by the data in the terms of information attributes (i.e. confidentiality, integrity, authenticity, and availability). If one of the information attributes of an IT Asset-hosted data is rated as “critical”, then the entire IT Asset is seen as critical from the business perspective. If an access right in a critical IT Asset allows access to critical data or even the manipulation of such data regarding one of the information attributes, then it must be flagged as Business-Critical Access (e.g. user with elevated rights to release payments of amounts above the common limit). This can be/has been mentioned as Tier 3 in IIQ.

- **Privileged Access (PA)**

  Enables the privileged user / account to circumvent the IT Asset’s security controls or allow a bypass of IT Asset operational logic. This is independent of its implemented granularity (i.e. local system / application rights, directory assigned rights, IAM entitlements, etc.). PA is subdivided into three Tiering classes (see PAM Guideline, subchapter 5.1):

  - **Tier 0:**

    Administrative access to central IT Assets which allows to circumvent system immanent security controls and thus can impact the confidentiality, integrity, authenticity, and availability of associated and consuming IT Assets (e.g. Active Directory Enterprise Admin, Active Directory Domain Admin, RACF Admin, Amazon Web Services AWS Root, Azure Root, Jenkins Global Admin, Global PKI Admin, Global CyberArk Admin).

- Tier 1:

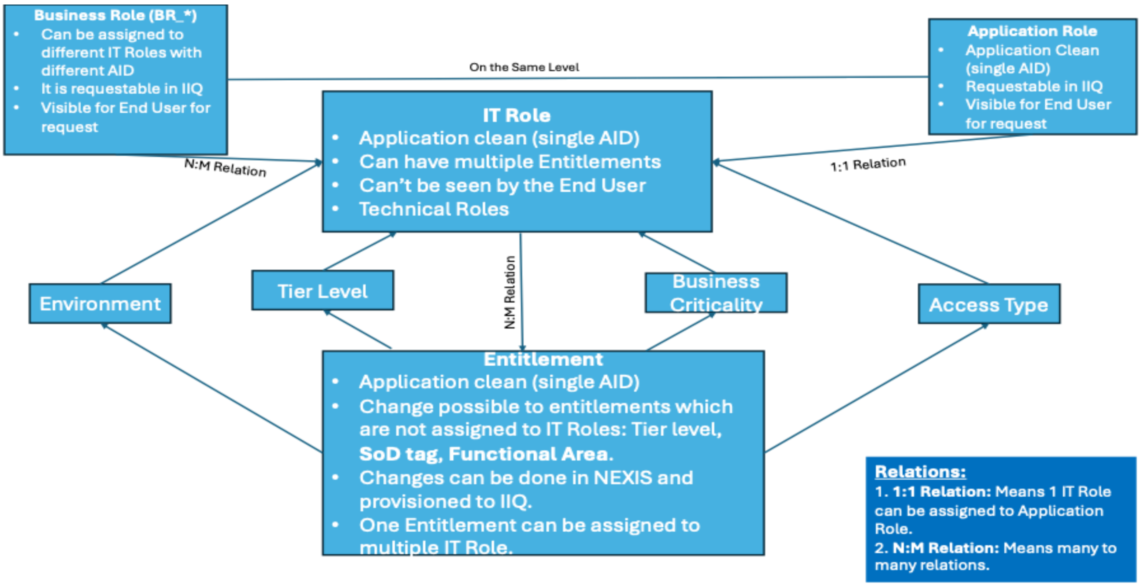
Administrative access to IT Assets which allows to circumvent system immanent security controls and thus can impact the confidentiality, integrity, authenticity, and availability of an IT Asset (e.g. Windows Local Admin, *NIX root, Network device account with ‘enable’, Operational Unit / Cluster Database Admin, Operational Unit / Cluster PKI Admin, Service Accounts used by Vulnerability Scanner, RACF Personal Accounts, Cloud Admins IAM Account).

Entitlements General Information

4.1 Entitlements

The current subchapter aims to name and describe all the relevant entitlements* available in the IT asset. This could either be a single or “bundle” of access rights** in the IT Asset. Figure 2 below represents entitlements description in IIQ system. For further details please refer to the IAM Guideline, chapter 3.

Note: Figure 2 is for information purposes only to show the connection between roles and entitlements.



Business Role (BR_*)
- Can be assigned to different IT Roles with different AID
- It is requestable in IIQ
- Visible for End User for request

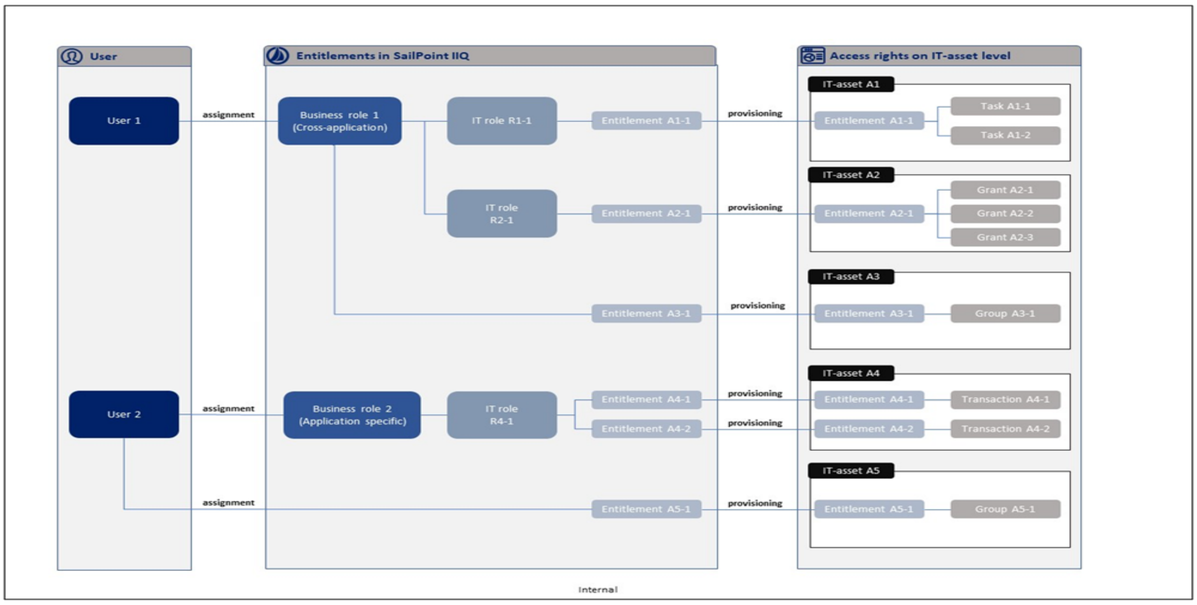
Application Role
- Application Clean (single AID)
- Requestable in IIQ
- Visible for End User for request

IT Role
- Application clean (single AID)
- Can have multiple Entitlements
- Can’t be seen by the End User
- Technical Roles

Entitlement
- Application clean (single AID)
- Change possible to entitlements which are not assigned to IT Roles: Tier level, **SoD tag, Functional Area.**
- Changes can be done in NEXIS and provisioned to IIQ.
- One Entitlement can be assigned to multiple IT Role.

Relations:
1. **1:1 Relation:** Means 1 IT Role can be assigned to Application Role.
2. **N:M Relation:** Means many to many relations.

Note: Figure 2 is for information purposes only to show the connection between roles and entitlements on IIQ example.



Comments:

Application is SoD relevant? no

Functional Area relevant? yes

Do you want to upload the entitlement composition?

* Entitlements refer to the access rights, including group memberships or access permissions, that have been granted to a user who has an account on the related source.

** Access rights are defined as individual user rights on Application level to perform tasks, grants, etc.

Entitlement Services

The page content can be found in a separate Excel file ("2025_11_11_Report_DAC_Template_Resource_MICROSOFT_OFFICE_365_Entitlement Services.xlsx").

All Entitlements

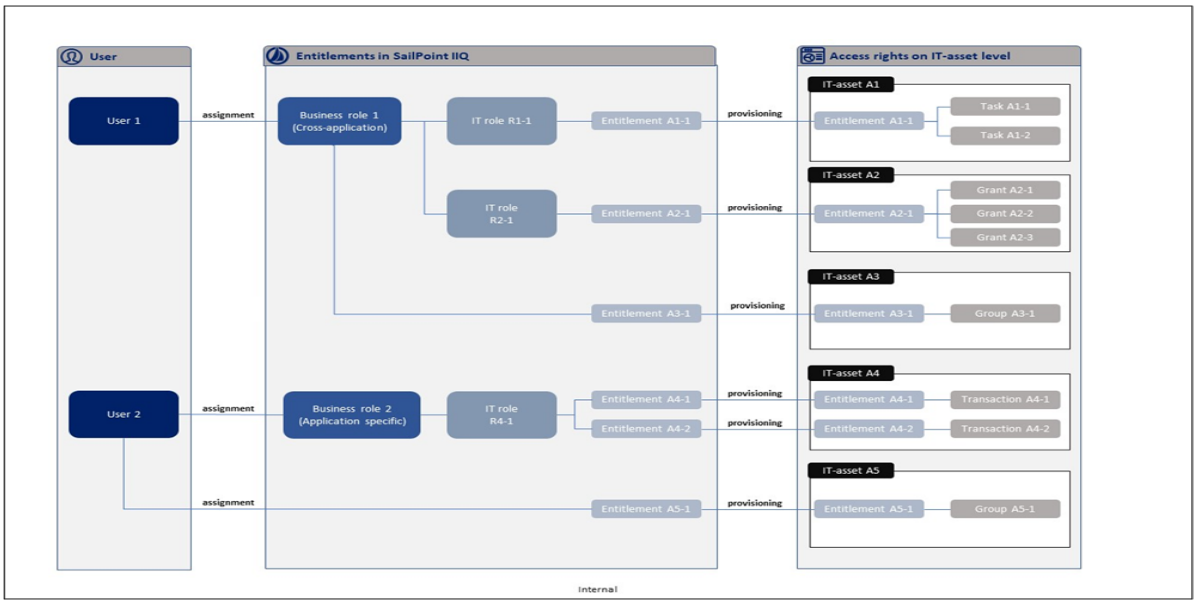
The page content can be found in a separate Excel file ("2025_11_11_Report_DAC_Template_Resource_MICROSOFT_OFFICE_365_All Entitlements.xlsx").

IT Roles General Information

4.2 IT Roles

IT Roles usually summarize a set of entitlements, so that the individual rights do not have to be defined individually for each identity / user. A role could be either a single or “bundle” of access rights in the IT Asset available for provisioning in the IAM system (e.g. IIQ).

Note: Figure 1 is for information purposes only to show the connection between roles and entitlements on IIQ example.



Comments:

Critical and Important Functions

CIF Document

Is Application a critical and important function Application?

If "CIF" is set true, all roles approval by, will be changed to "Manager in Line/ IT Role Owner

Report

IT Roles and assigned Entitlements Report

IT Roles assigned Entitlements

AID Role	IT Role Display name	IT Role Owner	Role Description	Role Tier Level	Role SoD Tag	Role Functional Area	Role Business Criticality

IT Role Services

The page content can be found in a separate Excel file ("2025_11_11_Report_DAC_Template_Resource_MICROSOFT_OFFICE_365_IT Role Services.xlsx").

All my Roles

The page content can be found in a separate Excel file ("2025_11_11_Report_DAC_Template_Resource_MICROSOFT_OFFICE_365_All my Roles.xlsx").

All my IT Roles without Application Role

The page content can be found in a separate Excel file ("2025_11_11_Report_DAC_Template_Resource_MICROSOFT_OFFICE_365_All my IT Roles without Application Role.xlsx").

All my Application Roles

The page content can be found in a separate Excel file ("2025_11_11_Report_DAC_Template_Resource_MICROSOFT_OFFICE_365_All my Application Roles.xlsx").

Special Accounts General Information

4.3 Account Management for Special Accounts

This subchapter is only for special accounts that exist once the IT Asset is installed without any configuration change, e.g. emergency or built-in accounts (for definitions of technical, shared and emergency accounts please see IAM guideline, chapter 4, for built-in accounts definition, please refer to the PAM guideline, chapter 4).

- **Technical accounts:**

  Is solely used for IT asset to IT Asset communication or system inherent processes and must always be assigned to one specific owner accountable to track activities.

- **Shared accounts:**

  Can be used by different identities but must always be assigned to one specific owner accountable to track the activities.

- **Emergency accounts:**

  Must always be assigned to one specific owner accountable to track the activities. Emergency accounts must be marked with the highest level of privileged access and the usage must be controlled in alignment with the current security controls, standards, and the defined usage in the PAM guideline. If the owner of an emergency account is leaving the company, the ownership of the shared account must be transferred to the owner's last Line Manager until ownership may be explicitly transferred.

- **Built-in accounts (or system accounts):**

  Since the accounts are built-in to the IT Asset, their life cycles follow the IT Assets' life cycles, i.e. once the IT Asset is installed, its built-in accounts become available, once it is decommissioned / deleted, its built-in accounts are deleted as well.

Please list special accounts of the IT Asset and classify them accordingly.

Note: You may provide an excerpt of your account inventory as an embedded file, if it contains all below-mentioned information. By built-in account please specify in the column "Account Type" if the account is technical, personal, shared or must not be used at all.

Comments

Special Accounts Services

The page content can be found in a separate Excel file ("2025_11_11_Report_DAC_Template_Resource_MICROSOFT_OFFICE_365_Special Accounts Services.xlsx").

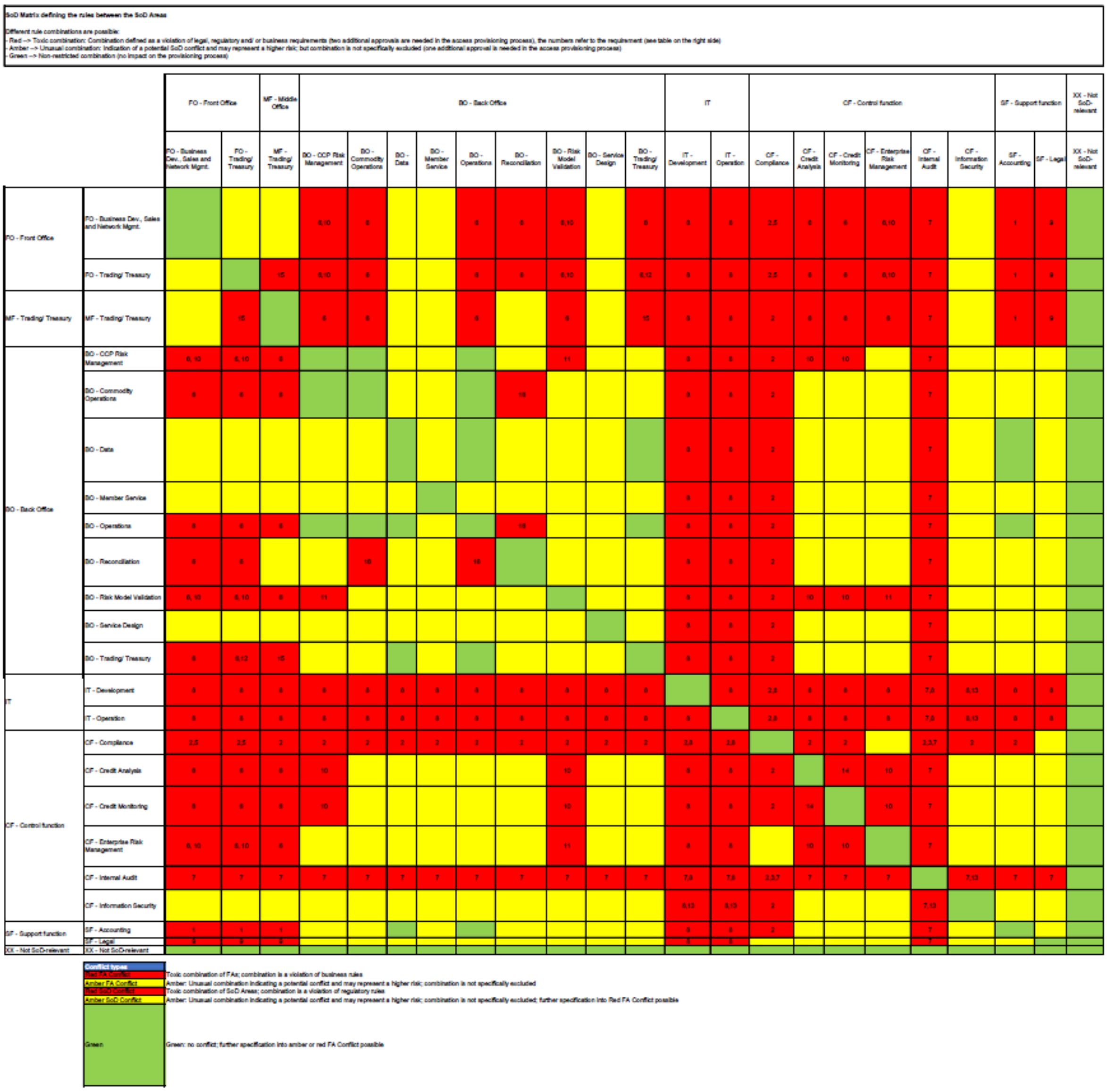
Segregation of Duties General Information

4.4 Segregation of Duties

Segregation of Duties (SoD) refers to a set of internal controls that mitigates the risk of error and fraud by requiring more than one person to complete a transaction-based task. In the traditional sense, SoD refers to separating duties of critical business areas in one user and his tasks to prevent toxic combinations of access rights and limit embezzlement. In modern IT infrastructures, managing users’ access rights to digital resources across the IT Asset ecosystem becomes a primary SoD control (for more detailed information please see SoD Matrix).

Group Compliance

Group Security



SoD Matrix defining the rules between the SoD Areas

Different rule combinations are possible:
- Red --> Toxic combination: Combination defined as a violation of legal, regulatory and/ or business requirements (two additional approvals are needed in the access provisioning process), the numbers refer to the requirement (see table on the right side)
- Amber --> Unusual combination: Indication of a potential SoD conflict and may represent a higher risk; but combination is not specifically excluded (one additional approval is needed in the access provisioning process)
- Green --> Non-restricted combination (no impact on the provisioning process)

		FO - Front Office		MF - Middle Office	BO - Back Office									IT		CF - Control function						SF - Support function		XX - Not SoD-relevant
		FO - Business Dev., Sales and Network Mgmt.	FO - Trading/ Treasury	MF - Trading/ Treasury	BO - CCP Risk Management	BO - Commodity Operations	BO - Data	BO - Member Service	BO - Operations	BO - Reconciliation	BO - Risk Model Validation	BO - Service Design	BO - Trading/ Treasury	IT - Development	IT - Operation	CF - Compliance	CF - Credit Analysis	CF - Credit Monitoring	CF - Enterprise Risk Management	CF - Internal Audit	CF - Information Security	SF - Accounting	SF - Legal	XX - Not SoD-relevant
FO - Front Office	FO - Business Dev., Sales and Network Mgmt.	🟩	🟨	🟨	🟥 6,10	🟥 6	🟨	🟨	🟥 6	🟥 6	🟥 6,10	🟨	🟥 6	🟥 8	🟥 8	🟥 2,5	🟥 6	🟥 6	🟥 6,10	🟥 7	🟨	🟥 1	🟥 9	🟩
	FO - Trading/ Treasury	🟨	🟩	🟥 15	🟥 6,10	🟥 6	🟨	🟨	🟥 6	🟥 6	🟥 6,10	🟨	🟥 6,12	🟥 8	🟥 8	🟥 2,5	🟥 6	🟥 6	🟥 6,10	🟥 7	🟨	🟥 1	🟥 9	🟩
MF - Trading/ Treasury	MF - Trading/ Treasury	🟨	🟥 15	🟩	🟥 6	🟥 6	🟨	🟨	🟥 6	🟨	🟥 6	🟨	🟥 15	🟥 8	🟥 8	🟥 2	🟥 6	🟥 6	🟥 6	🟥 7	🟨	🟥 1	🟥 9	🟩
BO - Back Office	BO - CCP Risk Management	🟥 6, 10	🟥 6, 10	🟥 6	🟩	🟩	🟨	🟨	🟩	🟨	🟥 11	🟨	🟨	🟥 8	🟥 8	🟥 2	🟥 10	🟥 10	🟨	🟥 7	🟨	🟨	🟨	🟩
	BO - Commodity Operations	🟥 6	🟥 6	🟥 6	🟩	🟩	🟨	🟨	🟩	🟥 16	🟨	🟨	🟨	🟥 8	🟥 8	🟥 2	🟨	🟨	🟨	🟥 7	🟨	🟨	🟨	🟩
	BO - Data	🟨	🟨	🟨	🟨	🟨	🟩	🟨	🟩	🟨	🟨	🟨	🟩	🟥 8	🟥 8	🟥 2	🟨	🟨	🟨	🟥 7	🟨	🟩	🟨	🟩
	BO - Member Service	🟨	🟨	🟨	🟨	🟨	🟨	🟩	🟨	🟨	🟨	🟨	🟨	🟥 8	🟥 8	🟥 2	🟨	🟨	🟨	🟥 7	🟨	🟨	🟨	🟩
	BO - Operations	🟥 6	🟥 6	🟥 6	🟩	🟩	🟩	🟨	🟩	🟥 16	🟨	🟨	🟩	🟥 8	🟥 8	🟥 2	🟨	🟨	🟨	🟥 7	🟨	🟩	🟨	🟩
	BO - Reconciliation	🟥 6	🟥 6	🟨	🟨	🟥 16	🟨	🟨	🟥 16	🟩	🟨	🟨	🟨	🟥 8	🟥 8	🟥 2	🟨	🟨	🟨	🟥 7	🟨	🟨	🟨	🟩
	BO - Risk Model Validation	🟥 6, 10	🟥 6, 10	🟥 6	🟥 11	🟨	🟨	🟨	🟨	🟨	🟩	🟨	🟨	🟥 8	🟥 8	🟥 2	🟥 10	🟥 10	🟥 11	🟥 7	🟨	🟨	🟨	🟩
	BO - Service Design	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟩	🟨	🟥 8	🟥 8	🟥 2	🟨	🟨	🟨	🟥 7	🟨	🟨	🟨	🟩
	BO - Trading/ Treasury	🟥 6	🟥 6,12	🟥 15	🟨	🟨	🟩	🟨	🟩	🟨	🟨	🟨	🟩	🟥 8	🟥 8	🟥 2	🟨	🟨	🟨	🟥 7	🟨	🟨	🟨	🟩
IT	IT - Development	🟥 8	🟥 8	🟥 8	🟥 8	🟥 8	🟥 8	🟥 8	🟥 8	🟥 8	🟥 8	🟥 8	🟥 8	🟩	🟥 8	🟥 2,8	🟥 8	🟥 8	🟥 8	🟥 7,8	🟥 8,13	🟥 8	🟥 8	🟩
	IT - Operation	🟥 8	🟥 8	🟥 8	🟥 8	🟥 8	🟥 8	🟥 8	🟥 8	🟥 8	🟥 8	🟥 8	🟥 8	🟥 8	🟩	🟥 2,8	🟥 8	🟥 8	🟥 8	🟥 7,8	🟥 8,13	🟥 8	🟥 8	🟩
CF - Control function	CF - Compliance	🟥 2,5	🟥 2,5	🟥 2	🟥 2	🟥 2	🟥 2	🟥 2	🟥 2	🟥 2	🟥 2	🟥 2	🟥 2	🟥 2,8	🟥 2,8	🟩	🟥 2	🟥 2	🟨	🟥 2,3,7	🟥 2	🟥 2	🟨	🟩
	CF - Credit Analysis	🟥 6	🟥 6	🟥 6	🟥 10	🟨	🟨	🟨	🟨	🟨	🟥 10	🟨	🟨	🟥 8	🟥 8	🟥 2	🟩	🟥 14	🟥 10	🟥 7	🟨	🟨	🟨	🟩
	CF - Credit Monitoring	🟥 6	🟥 6	🟥 6	🟥 10	🟨	🟨	🟨	🟨	🟨	🟥 10	🟨	🟨	🟥 8	🟥 8	🟥 2	🟥 14	🟩	🟥 10	🟥 7	🟨	🟨	🟨	🟩
	CF - Enterprise Risk Management	🟥 6, 10	🟥 6, 10	🟥 6	🟨	🟨	🟨	🟨	🟨	🟨	🟥 11	🟨	🟨	🟥 8	🟥 8	🟨	🟥 10	🟥 10	🟩	🟥 7	🟨	🟨	🟨	🟩
	CF - Internal Audit	🟥 7	🟥 7	🟥 7	🟥 7	🟥 7	🟥 7	🟥 7	🟥 7	🟥 7	🟥 7	🟥 7	🟥 7	🟥 7,8	🟥 7,8	🟥 2,3,7	🟥 7	🟥 7	🟥 7	🟩	🟥 7,13	🟥 7	🟥 7	🟩
	CF - Information Security	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟥 8,13	🟥 8,13	🟥 2	🟨	🟨	🟨	🟥 7,13	🟩	🟨	🟨	🟩
SF - Support function	SF - Accounting	🟥 1	🟥 1	🟥 1	🟨	🟨	🟩	🟨	🟩	🟨	🟨	🟨	🟨	🟥 8	🟥 8	🟥 2	🟨	🟨	🟨	🟥 7	🟨	🟩	🟨	🟩
	SF - Legal	🟥 9	🟥 9	🟥 9	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟥 8	🟥 8	🟨	🟨	🟨	🟨	🟥 7	🟨	🟨	🟩	🟩
XX - Not SoD-relevant	XX - Not SoD-relevant	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩

Conflict types	
🟥 Red FA Conflict	Toxic combination of FAs; combination is a violation of business rules
🟨 Amber FA Conflict	Amber: Unusual combination indicating a potential conflict and may represent a higher risk; combination is not specifically excluded
🟥 Red SoD Conflict	Toxic combination of SoD Areas; combination is a violation of regulatory rules
🟨 Amber SoD Conflict	Amber: Unusual combination indicating a potential conflict and may represent a higher risk; combination is not specifically excluded; further specification into Red FA Conflict possible
🟩 Green	Green: no conflict; further specification into amber or red FA Conflict possible

Please fill in the table below mentioning restrictions and used controls in case conflicts / toxic combinations of access rights.

Note: this subchapter is only relevant if IT Asset is not onboarded to IIQ. If the application is onboarded to IIQ, you will find it in Chapter 1 (IT Asset Description) under IIQ onboarded. If IT Asset is onboarded to IIQ.

Restriction	Description of restriction	Control used for conflicts

Comments:

4.4.1 Functional Area Matrix (Optional)

Functional Areas are process-/ LE-specific SoD rules and enable the business or asset to further specify the SoD Areas. With this additional definition, risks of fraud and security breaches can be reduced. Defining Functional Areas would be the decision of the asset owner. Here you have the possibility to document Functional Areas that are not illustrated within the additional page (matrix is automatically created based on IIQ data). Ideally, nothing should be documented here and the target state should correspond to the actual state in IIQ.

Please fill in the table below mentioning the functional areas and types of conflict of access rights.

Note: Filling out the functional area matrix is optional and is required only for specific applications. If you define functional areas, please consider the format [AIDXXX][FreeText][No*].

Functional area 1	Functional area 2	Type of conflict
		Red

Comments:

Functional Area Matrix

The page content can be found in a separate Excel file ("2025_11_11_Report_DAC_Template_Resource_MICROSOFT_OFFICE_365_Functional Area Matrix.xlsx").

5. References

5 References

Documents

IAM Guideline

PAM Guideline

ICT Risk Guidelines

Policies Database

Segregation of Duties Processes

Official SoD MATRIX

Please add additional references, if applicable.

Document name	Link

Please upload any relevant file (s).

6. List of Abbreviations

6 List of Abbreviations

Abbreviation	Description
AC	Authorization Concept
ISCP	Information Security Compliance Program
BA	Business Access
BCA	Business Critical Access
FS	File Share
GS	Group Security
IAM	Identity & Access Management
IIQ	SailPoint Identity IQ
MW	Middleware
OS	Operating System
PA	Privileged Access

PAM	Privileged Access Management
SoD	Segregation of Duties
UNC	Uniform Naming Convention