idFlow

Booklet

Version	04.08.2025
Language	English

Table of contents

1. idFlow ... 3

1.A Primary purpose ... 3
1.B Unique selling points ... 3
1.C Main functions ... 3
1.D Integration SAP & NonSAP ... 3
1.E Business-Functions / Applications ... 4
1.F Komponenten ... 5

2. identity & accessManager [IAM] ... 6

2.A Big-Picture ... 6
2.B Identity-Workplace (web browser / Fiori) ... 6
2.C Synchronizers & Providers ... 7
2.D SoD Risk Observer ... 8
2.E Authorization-Observer (Identity-Authorizations) ... 9
2.F Identity-Creator ... 10
2.G RBJITA ... 11
2.H RBAMP ... 11

3. authorizationManager [AM] ... 12

3.A Big-Picture ... 12
3.B Authorization-Workplace (Web Browser / Fiori) ... 12
3.C Business Roles ... 13
3.D Authorization Optimizer ... 14
3.E Authorization-Deriver ... 15
3.F SoD-Risk-Observer (Authorization) ... 16
3.G Authorization Distributor ... 17

4. emergency accessManager [EAM] ... 18

4.A Process ... 18
4.B Request-Workplace ... 18
4.C Activity-Risk-Observer ... 18

5. licenseManager [LM] ... 19

5.A Big-Picture ... 19
5.B License Calculator ... 20
5.C License Update ... 20

6. Requests & Workflow ... 21

6.A Request Monitor (Web Browser / Fiori) ... 21
6.B Workflow Customizing (Decision Table) ... 21
6.C Request Email ... 22

7. Activity Tracer ... 23

7.A Trace -> Profile ... 23
7.B Structure ... 23

1. idFlow

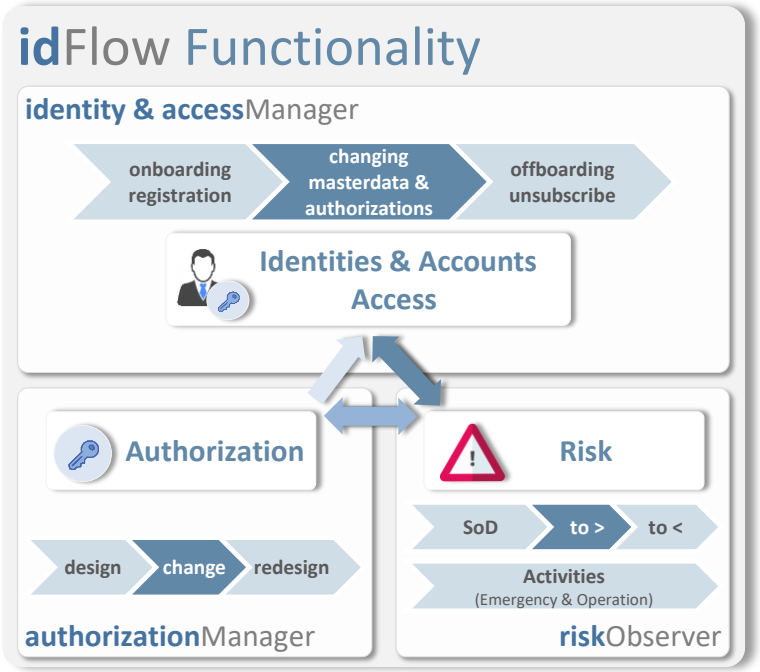
1.A Primary purpose

- **idFlow** is used to automate and optimize user **and authorization processes.**
- **idFlow** includes all the necessary functions for **synchronization**, **provisioning**, **workflow, onboarding, change, offboarding** and **risk assessment.**

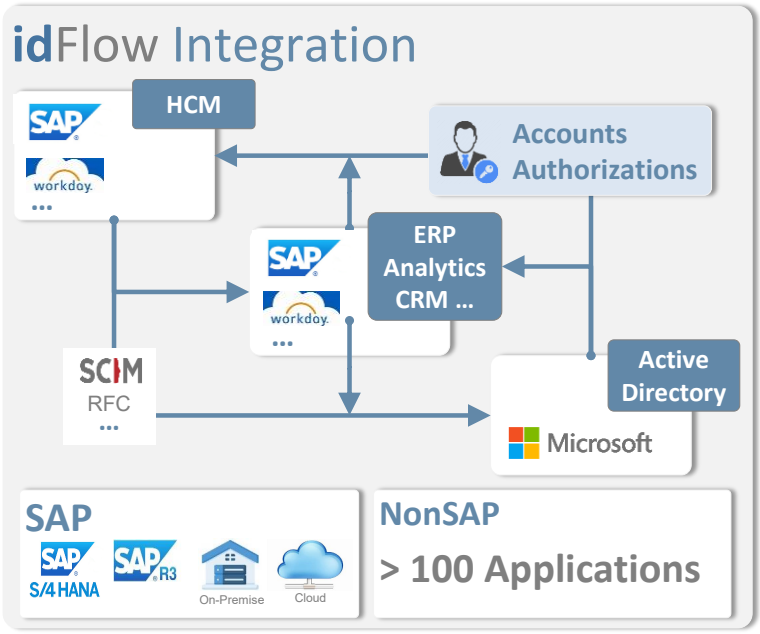
1.B Unique selling points

- **idFlow** is a highly integrated "all-in-one" product. The entire life cycle of all accounts and authorizations of the SAP and NonSAP systems is supported.
- **idFlow** is an SAP add-on **developed in ABAP** and does not require **any additional hardware investments.**
- **idFlow** enables an **unrivalled cost-><-benefit ratio.**

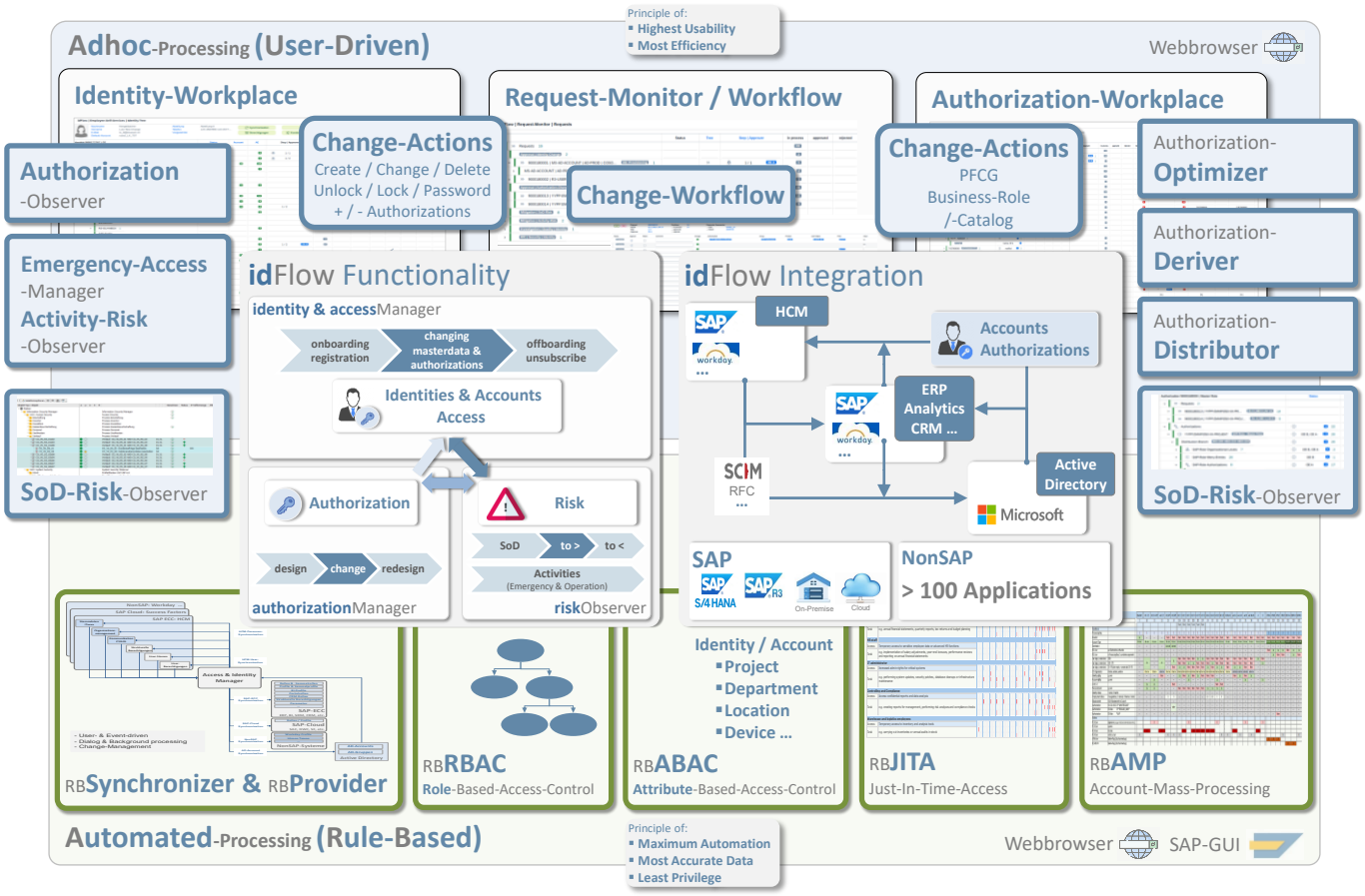
1.C Main functions



1.D Integration SAP & NonSAP



1.E Business-Functions / Applications



Adhoc-Processing (User-Driven)

Identity-Workplace	
Authorization-Observer	Too few / too many permissions?
emergency access Manager	Emergency-Authorization-Provisioning
Activity-Risk-Observer	Analysis of critical activities
SoD-Risk-Observer	Too many permissions? (-> Audit, etc.)
Authorization-Workplace	
Authorization-**Optimizer**	+ / - Transactions/applications (used/unused)
Authorization-**Deriver**	+ / - / **change**: Org.-Level of customer organizational units
Authorization-**Distributor**	Distribution of Authorization-Elements in the System-Landscape
SoD-Risk-Observer	Too many permissions? (-> Audit, etc.)

Automated Processing (Rule-Based)

Synchronizer & Provider	Account-/ & Authorization-Data-Flow (create, change, delete, provide)
Role-Based-Access-Control	Permissions based on predefined Roles
Attribute-Based-Access-Control	Permissions based on a combination of attributes
Just-In-Time-Access	Permissions that are only required for certain time windows
Account-Mass-Processing	Subtractive measures such as deletion, blocking, demarcation, etc.

Principle of Highest-Usability

- The applications are available to the various user groups via **web browser**.
- The functionalities follow the "all-in-one" approach and react **dynamically** to the respective user groups (authorizations & customizing).

Principle of Most Efficiency

- The user interactions trigger "actions". These can be configured very flexibly and can automatically trigger suitable follow-up activities themselves. This results in a considerable reduction in work steps and effort.

Principle of Maximum Automation

- Processes that follow a describable **rule** can also be **automated**!
- Customizing decision tables map the corresponding **set of rules**.

Principle of Most Accurate Data

- The necessary **data flows** are mapped **in Customizing** decision tables.
- Event recognition ensures proactive and reactive **data synchronization**.

Principle of Least Privilege

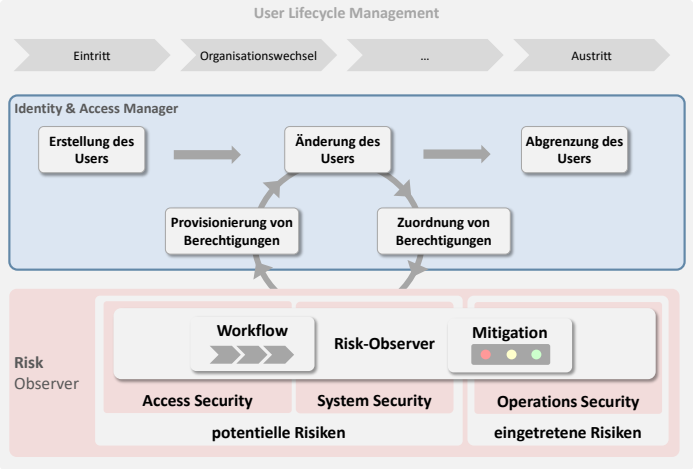
- Rule-based **just-in-time access** enables the automatic provisioning/deprovisioning of authorizations that the user only needs at certain times / time windows.
- Rule-based **account mass processing** is the counterpart to additive functions such as identity creators etc. The typical tasks are the subtractive measures such as deletion, blocking, demarcation, etc.

1.F Komponenten

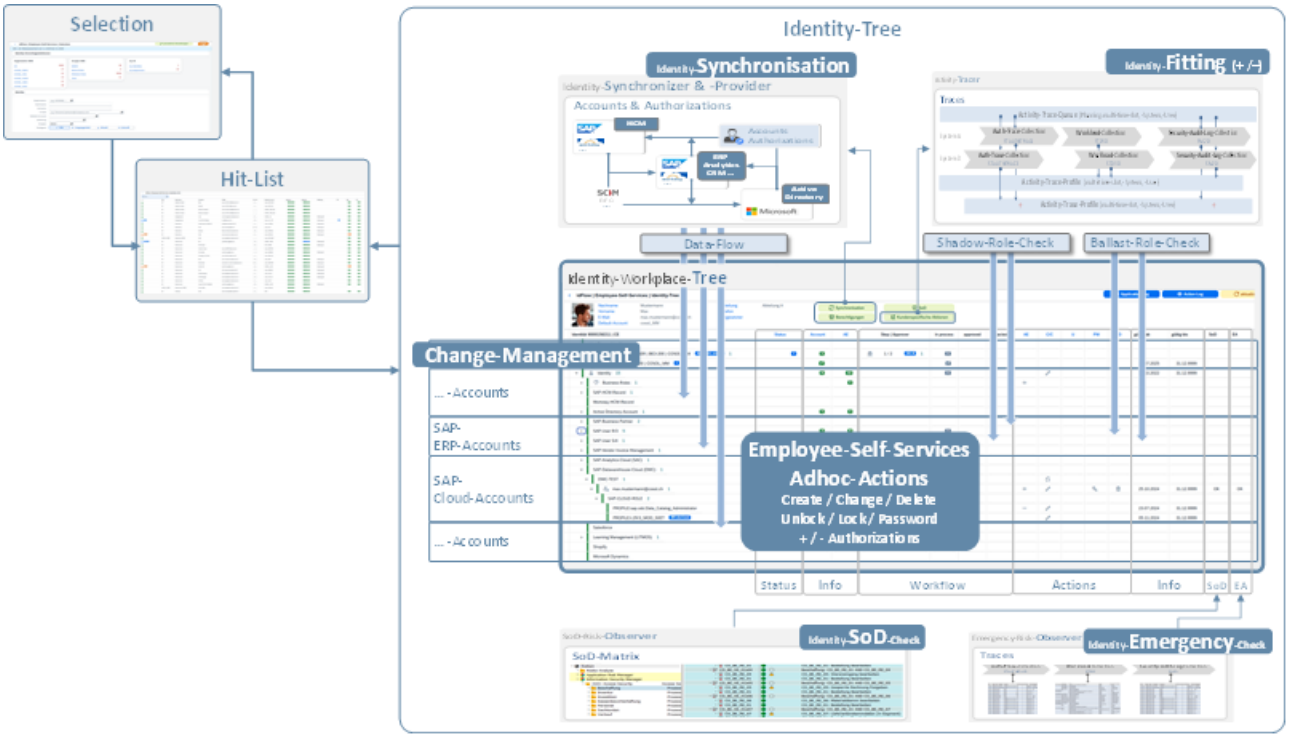
identity & access Manager	
Catalog	Management of all Identities & Accounts
Workplaces	Customer-, Employee-, Administrator-Services
Synchronizer	Account-Data-Flow (auto-create, -change)
Provider	Authorization-Provisioning
Identity-Assigner	Analysis (duplicates, errors) and assignment of accounts to identities
SoD-Risk-Observer	Too many permissions? (-> Audit, etc.)
Authorization-Observer	Too few / to many permissions?
Identity-Creator	Multi-/Mass-Creation of Identities, Accounts und Authorizations
RBJITA	Rule-Based-Just-In-Time-Access
RBAMP	Rule-Based-Account-Mass-Processing
authorizationManager	
Catalog	Management of all authorization elements
Workplaces	Customer-, Employee-, Administrator-Services
Business-Roles	Combination of different authorization elements & destinations
SoD-Risk-Observer	too many permissions? (-> revision, etc.)
Optimizer	+ / - : Transactions/applications (used/unused)
Deriver	+ / - / change: Org.-Level of customer organizational units
Distributor	Distribution of Authorization-Elements in the System-Landscape
emergency access Manager	
Emergency-Role-Provider	Emergeny-Authorization-Provisioning
Activity-Risk-Observer	Analysis of critical actvities
licenseManager	
Calculator	Calculation and optimisation of licenses
coreFunctions	
Requests & Workflow	Request, E-Mail, Process-Steps, Responsabilty
Risk-Observer	Access-, System-, Operations-Security
Activity-Tracer	Authorization-Trace, Workload, Security-Audit-Log, etc.
Data-Collector	Data collection and central storage in all systems

2. identity & accessManager [IAM]

2.A Big-Picture

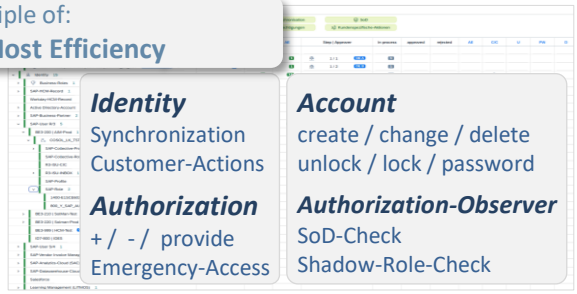


2.B Identity-Workplace (web browser / Fiori)



Principle of:

- **Most Efficiency**



Identity
Synchronization
Customer-Actions

Authorization
+ / - / provide
Emergency-Access

Account
create / change / delete
unlock / lock / password

Authorization-Observer
SoD-Check
Shadow-Role-Check

2.C Synchronizers & Providers

Event Recognition

Event recognition is integrated into the core function **Data Collection** and makes it possible to **detect** state changes **in all integrated systems** and trigger **defined** actions

For example, a name change in the HCM system or an e-mail change in the Active Directory can be automatically detected and distributed to all relevant systems.

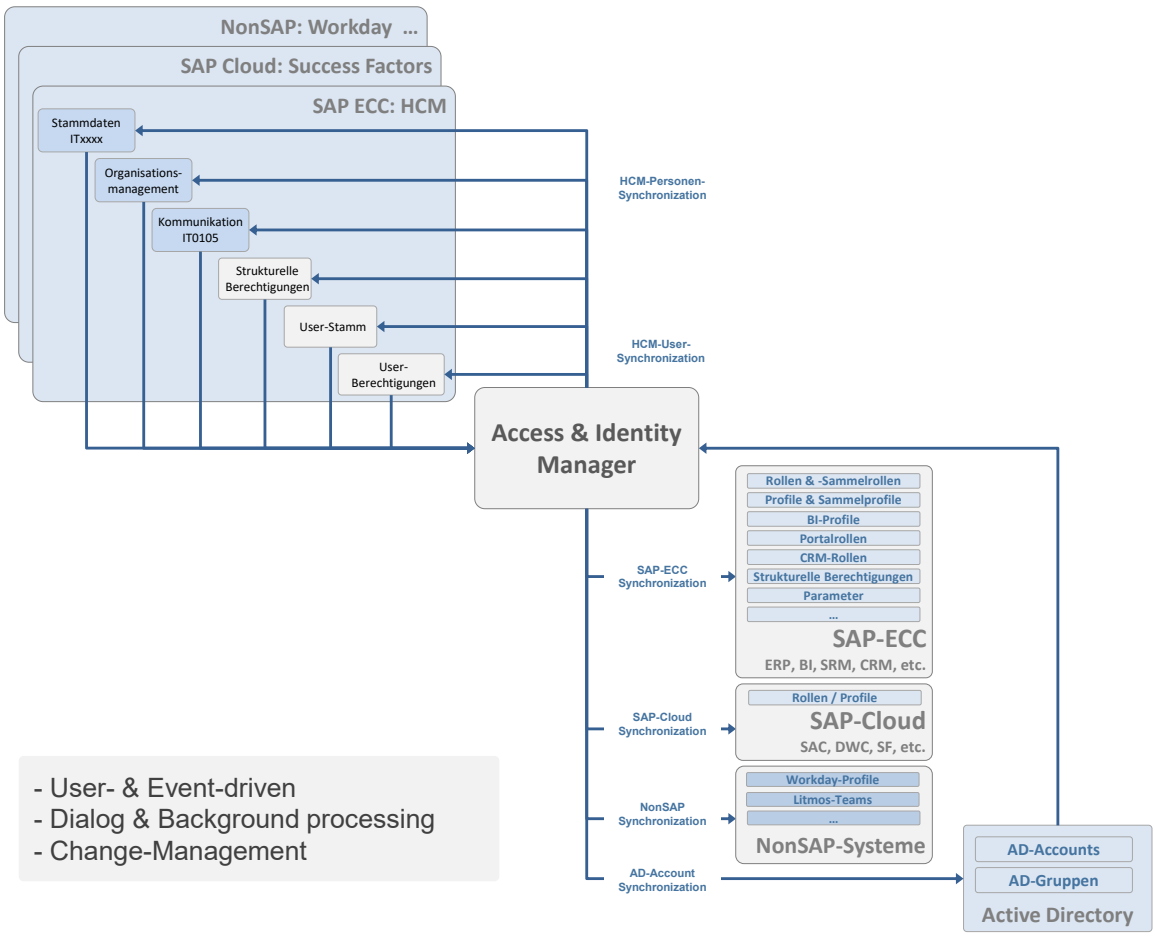
Data Flow

The **synchronizer** ensures that the **master data** of the accounts belonging to each other are synchronized.

The **provider** ensures that the necessary authorizations (defaults) and the requested authorizations (requests) are assigned to the relevant accounts.

Both the synchronizer and the provider are based on **extensive sets of rules** that are defined in **customizing** and can be adapted by the customer at any time.

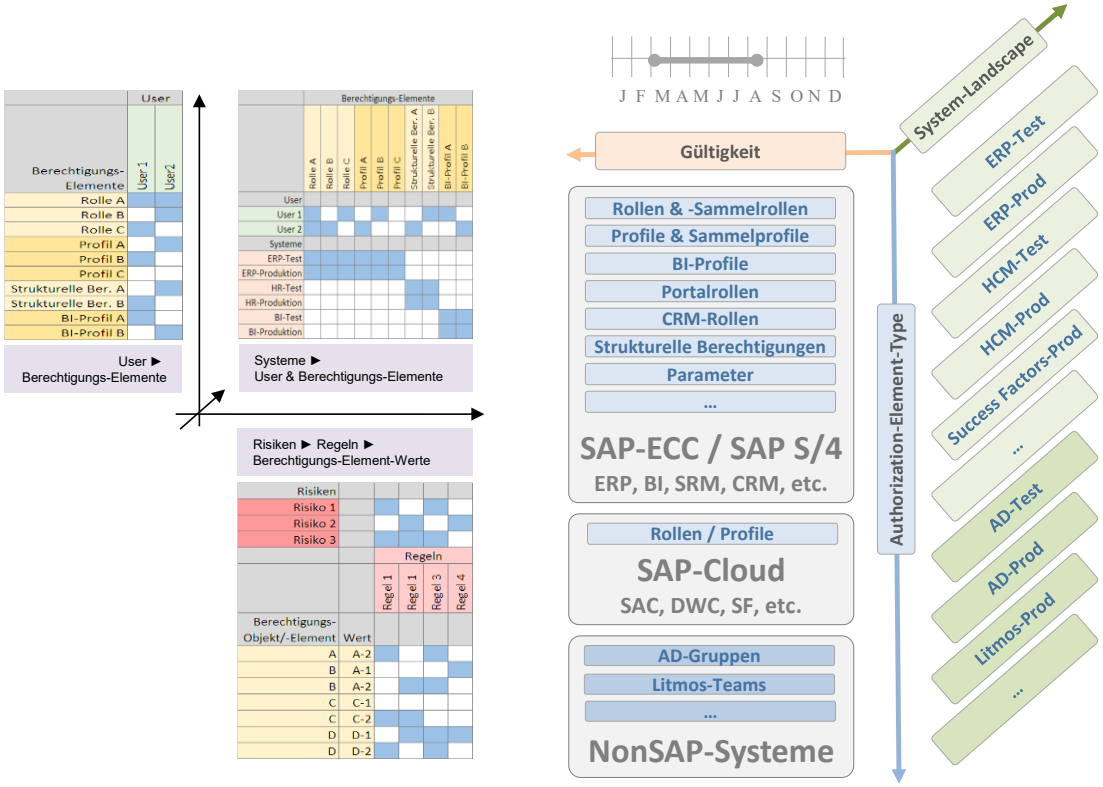
- The identity serves as a "container" of accounts that belong together.
  (e.g. R/3 user, S/4HANA user, SAP cloud user, AD account, person, nonSAP accounts, ...)
- Any system and attribute can be both input and output.
- Rules are mapped as decision tables.
- Customer-specific exits are planned.
- Accounts and permissions can be defined as default. (Derivation from e.g. - position, - personal data, existing accounts, etc.)
- Scenarios define the data flow and can be flexibly mapped for different needs. (e.g. internal employees, external employees, technical accounts, ...)



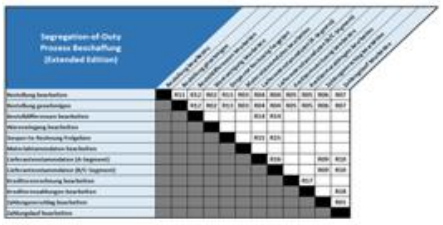
2.D SoD Risk Observer

The SoD Risk Observer **ensures that the policies are permanently adhered to by automated monitoring of the defined risks or that they** are **assessed**, **documented** and **dealt** with in the event of a violation.

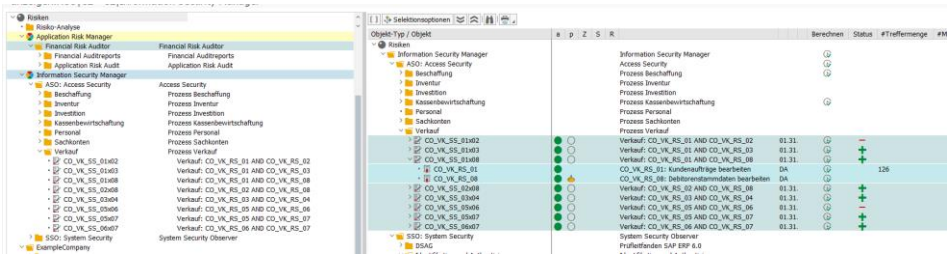
- Test item → **1 Identity**
- Basics → DSAG, SAP-GRC, auditing houses
- Concept & Documentation → Excel
- Customizing → Risk Organizer
  → Rule Organizer
- Execution → Dialogue & Background
- Protocol → SoD Analysis
- Mitigation → Form & Workflow



The rules and risks are documented and can also be used to prove the applied set of rules.



The rule and risks are transparently implemented in the system. They can be extended to suit the customers' needs as well as deactivated in a targeted manner.



2.E Authorization-Observer (Identity-Authorizations)

The Authorization Observer has the task of recognizing the **risks** that arise from the design / redesign of authorizations (and can **occur in productive operation**) and to support their elimination.

A distinction must be made between two types of risk:

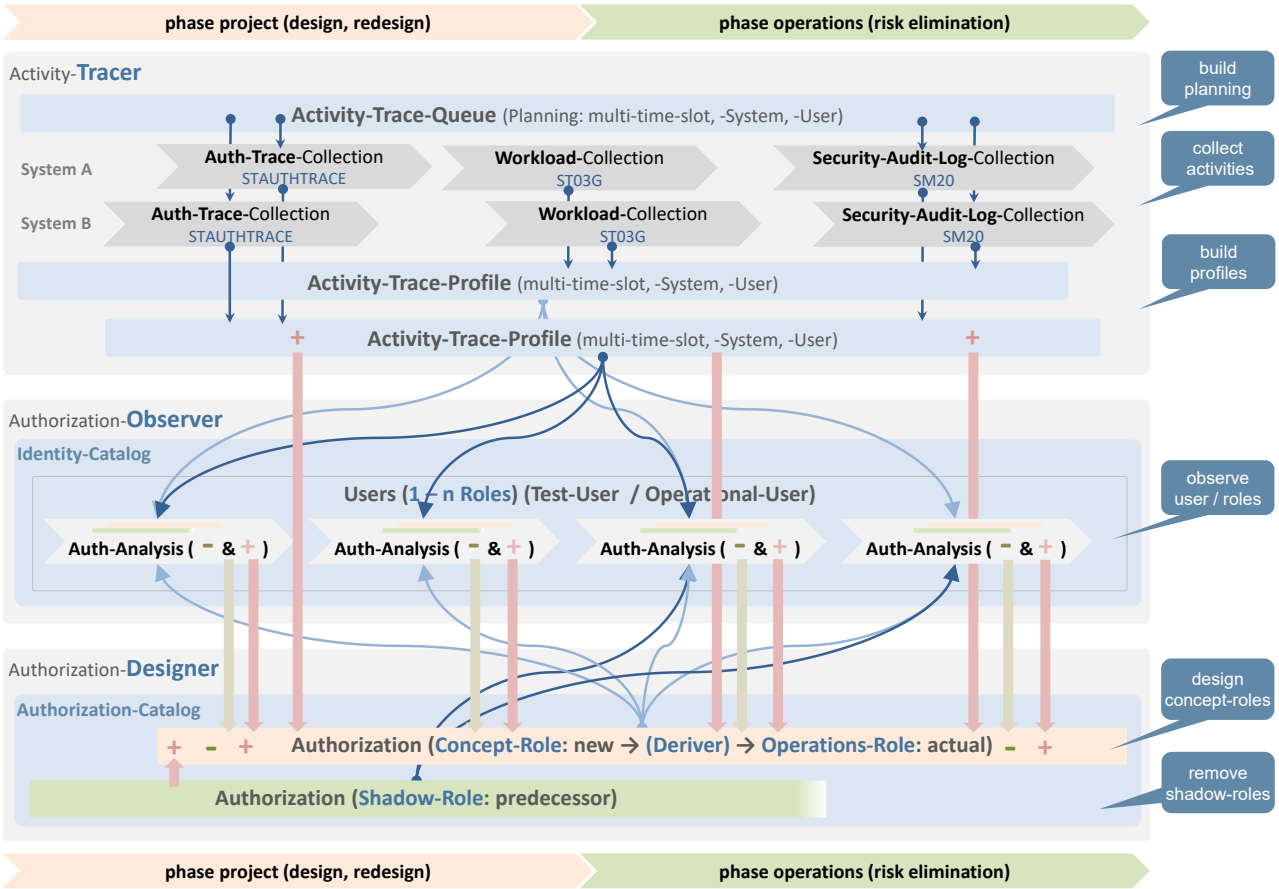
- "**too few** permissions" -> **Operations-Risk-Eliminator**
  -> user can't work due to lack of permissions!
- "**too many** permissions" -> **Authorization-Optimizer**
  -> SoD risks etc. arise due to non-necessary elements in the permissions

For both risk types, the analysis principle is to check the permissions assigned to an account (e.g. R/3 user) against the collected traces.

- -> **Necessity** (Use) of the **Shadow Roles** (previous roles) → **too few permissions**
- -> **Needlessness** (non-use) of **Ballast Roles** → **too many permissions**

These **analyses** are carried out iteratively, both in the **project phase** (design / redesign) and in the **production phase**. Each analysis cycle leads to an **optimization** of authorizations.

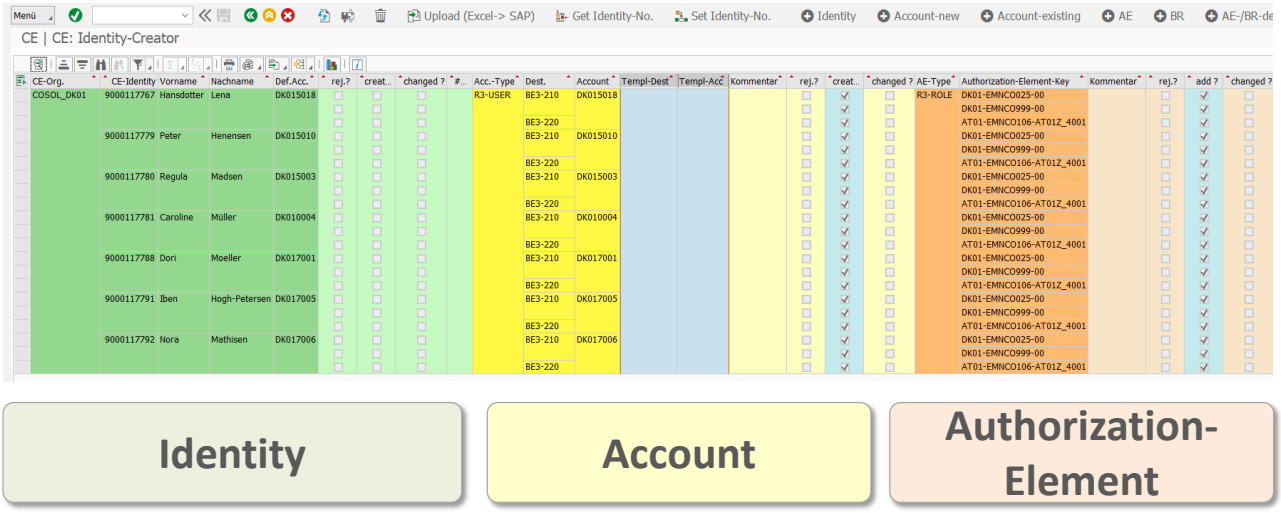
In order to eliminate the operational risks in the productive phase, **the user retains his previous roles** until **these "shadow roles" are no longer necessary**.



2.F Identity-Creator

The Identity Creator:

- is an easy-to-use user interface for requesting/performing the following actions:
  - create Identities
  - create Accounts
  - add Authorization-Elements
- Supports both:
  - Mass upload via Excel template
  - Mass processing dialog for:
    - n Identities
    - n Accounts
    - n Authorization element



2.G RBJITA

Rule-based just-in-time access enables the automatic provisioning/deprovisioning of authorizations that the user only needs at certain times / time windows.

- Concept & Documentation → Excel
- Customizing → Decission table (E96, E97, E98)
- Execution → Dialogue & Background
- Protocol → Application log, action log, e-mail to administrator

Examples:

Role	Access / Task	Jan	Feb	Mar	Apr	Mai	Jun	Jul	Aug	Sep	Oct	Nov	Dez
Accountants and finance staff													
Access	Access to financial systems, sensitive financial data, or advanced reporting capabilities												
Task	e.g. annual financial statements, quarterly reports, tax returns and budget planning												
HR staff													
Access	Temporary access to sensitive employee data or advanced HR functions												
Task	e.g. implementation of salary adjustments, year-end bonuses, performance reviews and reporting on annual financial statements												
IT administrator													
Access	Increased admin rights for critical systems												
Task	e.g. performing system updates, security patches, database cleanups or infrastructure maintenance												
Controlling and Compliance													
Access	Access confidential reports and data analysis												
Task	e.g. creating reports for management, performing risk analyses and compliance checks												
Warehouse and logistics employees													
Access	Temporary access to inventory and analysis tools												
Task	e.g. carrying out inventories or annual audits in stock												

2.H RBAMP

Rule-based account mass processing is the counterpart to additive functions such as identity creators etc.

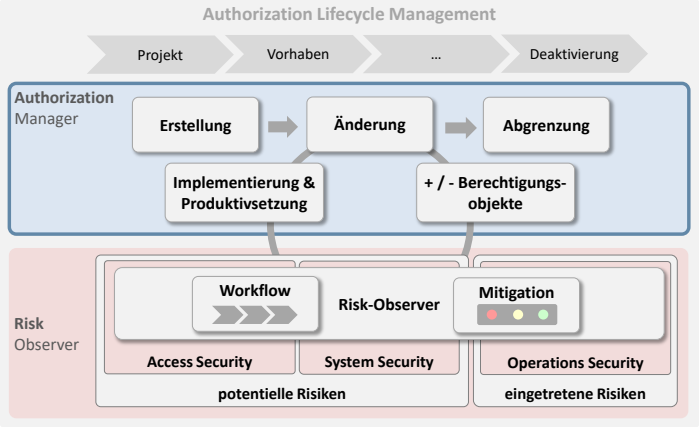
The typical tasks are the **subtractive measures** such as **deletion**, **blocking**, **demarcation**, etc.

- Concept & Documentation → Excel
- Customizing → Decission table (E96, E97, E98)
- Execution → Dialogue & Background
- Protocol → Application log, action log, e-mail to administrator

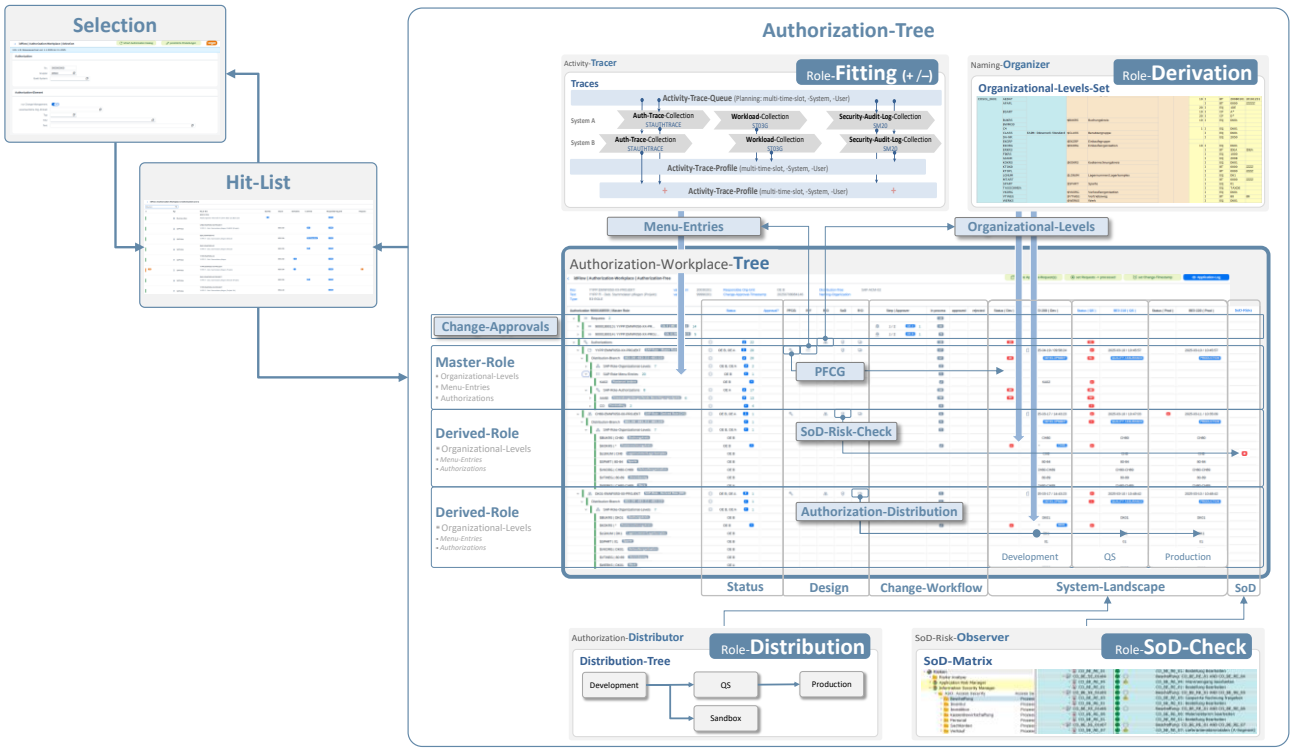
		Blacklist	Int.C-O	Int.C-O-ATZ	ext.C.O	Int.GPH	Int.GP0	Int.F.1	Int.F.2	Int.F.3	Int.F.4	Int.F.5	Int.F.6	Int.A.2	Int.A.3	Int.B.2	Int.B.3	Int.Norm	ext.A.3	ext.A.4	ext.B	ext.Norm	A	B	VIM.A	VIM.B	VIM.C	VIM.0	BUPA.A	BUPA.B	BUPA.0
Priorität		5	10	11	12	13	14	21A	21B	21C	21D	21E	21F	24	25	26	27	29	31	32	35	39	91	92	211	212	213	214	221	222	223
Bemerkung								Forst	Forst	Forst	Forst	Forst	Forst																		
Conditions																															
Processing-Step		1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2
Blacklist		Ja	--	--	--	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
Account-Type		R3-User	R3-User	R3-User	R3-User	R3-User	R3-User	R3-User	R3-User	R3-User	R3-User	R3-User	R3-User	R3-User	R3-User	R3-User	R3-User	R3-User	R3-User	R3-User	R3-User	R3-User	R3-User	R3-User	R3-VIM	R3-VIM	R3-VIM	R3-VIM	R3-BUPA	R3-BUPA	R3-BUPA
Destination		--	--	--	--	GPH-200	GP0-010	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
R3-User	auf Destination vorhanden	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	Nein	Ja	Ja	Ja	Nein	Ja	Ja
R3-User	in Processing-Step-1 zum delete vorgemerkt	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	Ja	Nein	Nein	--	Ja	Nein
last login, (create date)	180>	--		--		--	Ja	Nein	Nein	Nein	Nein	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Nein	--	--	--	--	--	--	--
last login, (create date)	100 - 179	--	Ja	--	Ja	--		Nein	Nein	Ja	Ja	Nein	Nein	Nein	Ja	Nein	Nein	Nein	Nein	Nein	Nein	Nein	--	Ja	--	--	--	--	--	--	--
last login, (create date)	30 - 99 (oder empty + create-date 30 - 99)	--		--		--	Nein	Ja	Ja	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Nein	Ja	Ja	Nein	Nein	--	--	--	--	--	--	--	--	--
CE-Organisation	interne, externe, weitere	--	interne	Interne	externe	interne	interne	interne	interne	interne	interne	interne	interne	interne	interne	interne	interne	interne	externe	externe	externe	externe	--	--	--	--	--	--	--	--	--
Identity-gültig	ja, nein	--	--	--	Nein	--	--	Ja	Nein	Ja	Nein	Ja	Nein	Nein	Nein	--	--	--	Nein	Ja	Nein	Ja	--	--	--	--	--	--	--	--	--
Account-gültig	ja, nein	--	--	Ja	--	--	--	--	--	Ja	--	--	--	--	--	Ja	--	--	--	--	Ja	--	Ja	--	--	--	--	--	--	--	--
Unit C-O		--	Ja	Ja	--	--	Nein	--	--	--	--	--	--	--	--	Nein	Nein	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Personalstamm	ja, nein	--	Ja	Ja	--	--	--	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Ja	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Identity-Status	1=aktiv, 0=inaktiv	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Employment-Status	0=ausgetreten, 1=ruhend, 2=Rentner, 3=aktiv	--	--	--	--	3	3	--	--	--	--	--	--	0, 2	0, 2	1	3	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Wiedereintritt	HCM-Wiedereintritt in Zukunft	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Authorization	R3-COL-ROLE CP *BANFFREIGABE*	--	--	--	--	--	oder	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Authorization	R3-Role CP *FREIGABE_BANF*	--	--	--	--	--		--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Authorization	R3-Role *VIM*	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	Nein	--	--	--	--
Actions																															
R/3-User	abgrenzen (Account-ENDDA & E40-ENDDA & E40-fix)			X						X						X					X		X								
R/3-User	sperren																														
R/3-User	löschen		X		X				X		X	X	X	X	X				X				X								
R/3-User	nichts zu tun !	X				X	X	X									X	X		X		X						X			X
VIM-User	Delete-Flag (Löschvormerkung)																								X	X	X				
R/3-BUPA	Delete-Flag (Löschvormerkung)																											X	X		

3. authorizationManager [AM]

3.A Big-Picture



3.B Authorization-Workplace (Web Browser / Fiori)



Principle of:

- **Most Efficiency**

Role-Observer
Analysis
Visualization
SoD-Check

Role-Designer
Maintenance (z.B. PFCG)
Fitting
Derivation
Distribution
Approval-Process

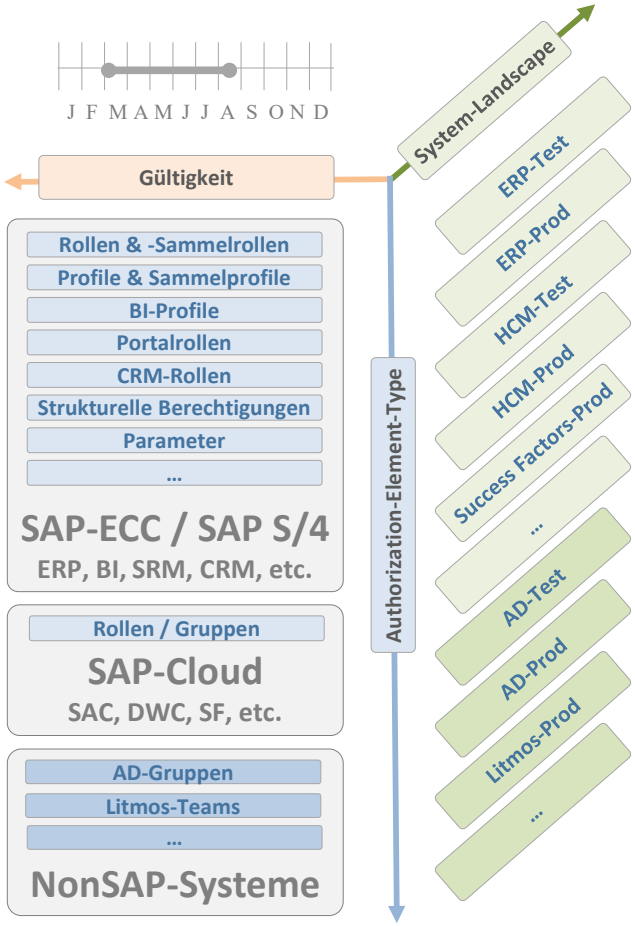
3.C Business Roles

The business role is used to link and process application authorizations that belong together from the entire system landscape (SAP and NonSAP).

For example, one (1) business role can be defined for the position "Controller", which includes all necessary authorizations on all necessary target systems.
→ By assigning one (1) business role to an identity, all necessary application roles are provisioned simultaneously and in one step.

The business role enables:

- the combination of different authorization elements
- the definition of different destination destinations
- the determination of the temporal validity

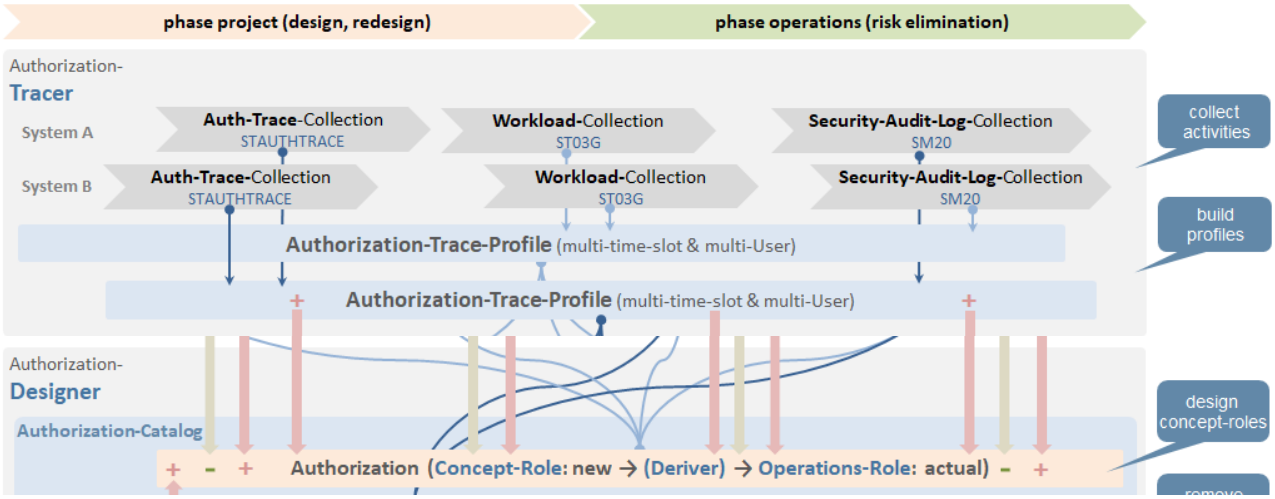


3.D Authorization Optimizer

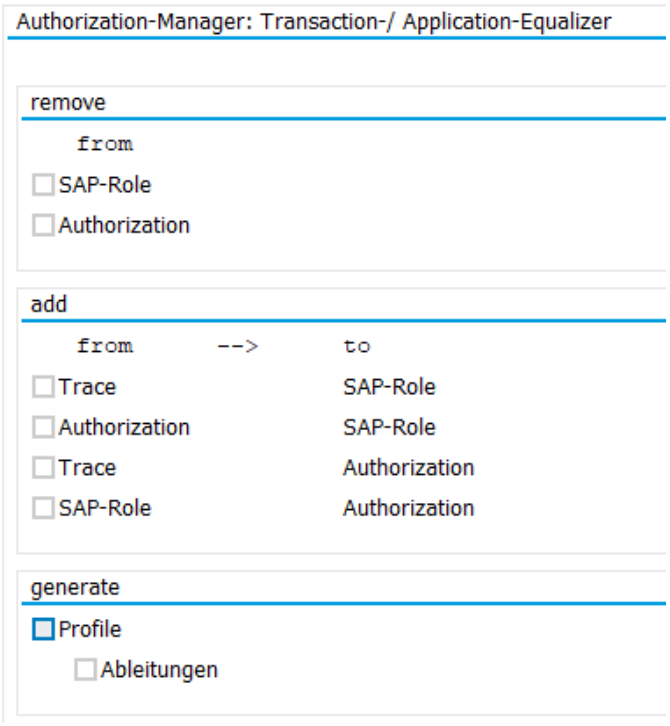
During the design/redesign of an authorization, the optimizer ensures that the **necessary transactions/applications are recognized and integrated into the authorization**.

The target state (quantity of transactions/applications) is defined by:

- the TR/App collected in the traces
- the manual specifications/definition in the master data of the authorization



The equalizer enables the specific comparison between the traces, the authorization in the catalog, and the SAP role.

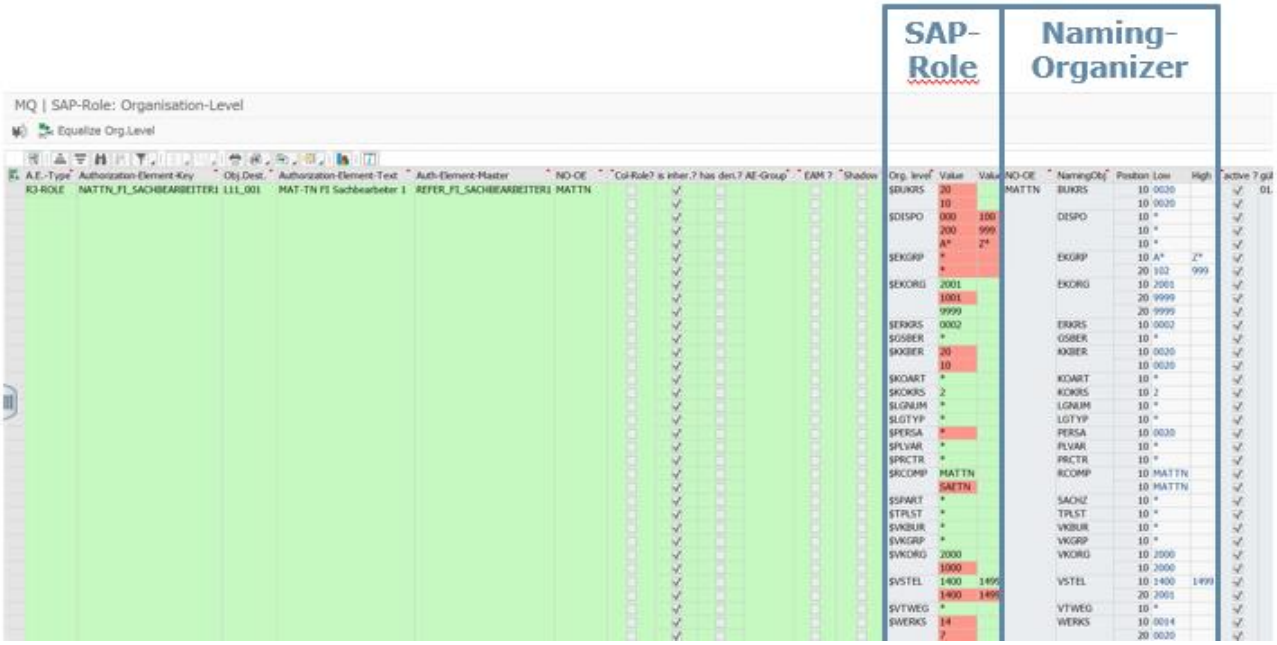


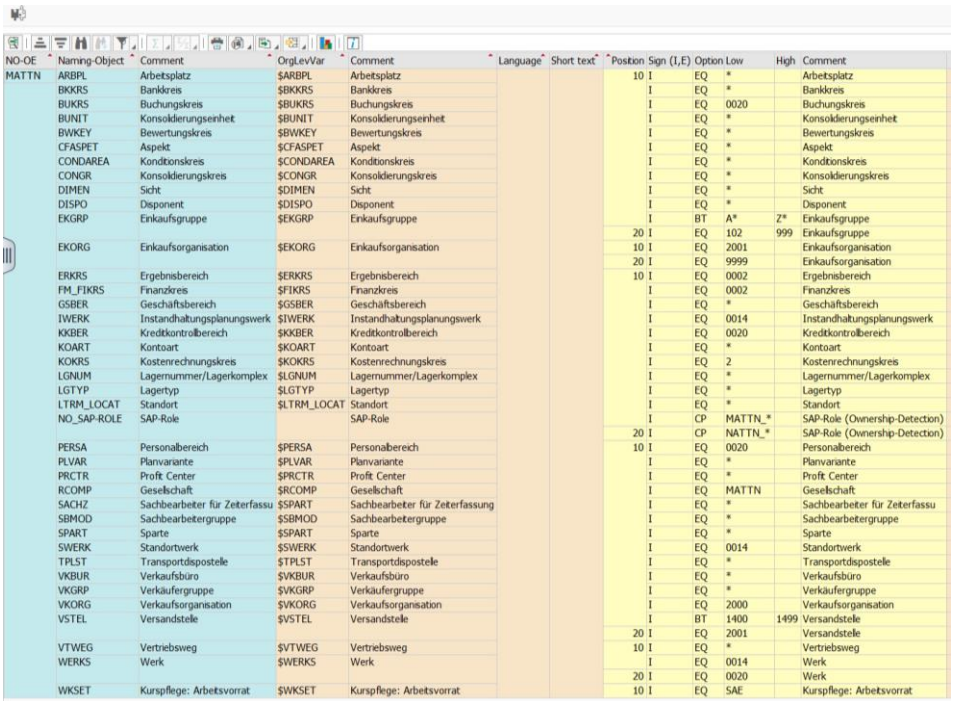
3.E Authorization-Deriver

The deriver ensures that the **Org.Level** defined in the authorizations (derivatives from master roles) meet the specifications.

The specifications are defined for each customer organizational unit in Customizing (**Naming Organizer**).

- The target state (values of the Org.Level) is defined in the Naming Organizer.
- The comparison in the source systems can be carried out partially or completely.
- Generation in the source systems can be initiated directly.



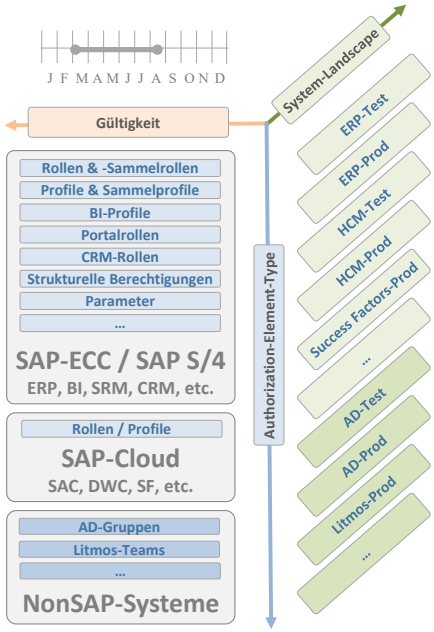


NO-OE	Naming-Object	Comment	OrgLevVar	Comment	Language	Short text	Position	Sign (I,E)	Option	Low	High	Comment
MATTN	ARBPL	Arbeitsplatz	$ARBPL	Arbeitsplatz			10	I	EQ	*		Arbeitsplatz
	BKKRS	Bankkreis	$BKKRS	Bankkreis				I	EQ	*		Bankkreis
	BUKRS	Buchungskreis	$BUKRS	Buchungskreis				I	EQ	0020		Buchungskreis
	BUNIT	Konsolidierungseinheit	$BUNIT	Konsolidierungseinheit				I	EQ	*		Konsolidierungseinheit
	BWKEY	Bewertungskreis	$BWKEY	Bewertungskreis				I	EQ	*		Bewertungskreis
	CFASPET	Aspekt	$CFASPET	Aspekt				I	EQ	*		Aspekt
	CONDAREA	Konditionskreis	$CONDAREA	Konditionskreis				I	EQ	*		Konditionskreis
	CONGR	Konsolidierungskreis	$CONGR	Konsolidierungskreis				I	EQ	*		Konsolidierungskreis
	DIMEN	Sicht	$DIMEN	Sicht				I	EQ	*		Sicht
	DISPO	Disponent	$DISPO	Disponent				I	EQ	*		Disponent
	EKGRP	Einkaufsgruppe	$EKGRP	Einkaufsgruppe				I	BT	A*	Z*	Einkaufsgruppe
							20	I	EQ	102	999	Einkaufsgruppe
	EKORG	Einkaufsorganisation	$EKORG	Einkaufsorganisation			10	I	EQ	2001		Einkaufsorganisation
							20	I	EQ	9999		Einkaufsorganisation
	ERKRS	Ergebnisbereich	$ERKRS	Ergebnisbereich			10	I	EQ	0002		Ergebnisbereich
	FM_FIKRS	Finanzkreis	$FIKRS	Finanzkreis				I	EQ	0002		Finanzkreis
	GSBER	Geschäftsbereich	$GSBER	Geschäftsbereich				I	EQ	*		Geschäftsbereich
	IWERK	Instandhaltungsplanungswerk	$IWERK	Instandhaltungsplanungswerk				I	EQ	0014		Instandhaltungsplanungswerk
	KKBER	Kreditkontrollbereich	$KKBER	Kreditkontrollbereich				I	EQ	0020		Kreditkontrollbereich
	KOART	Kontoart	$KOART	Kontoart				I	EQ	*		Kontoart
	KOKRS	Kostenrechnungskreis	$KOKRS	Kostenrechnungskreis				I	EQ	2		Kostenrechnungskreis
	LGNUM	Lagernummer/Lagerkomplex	$LGNUM	Lagernummer/Lagerkomplex				I	EQ	*		Lagernummer/Lagerkomplex
	LGTYP	Lagertyp	$LGTYP	Lagertyp				I	EQ	*		Lagertyp
	LTRM_LOCAT	Standort	$LTRM_LOCAT	Standort				I	EQ	*		Standort
	NO_SAP-ROLE	SAP-Role		SAP-Role				I	CP	MATTN_*		SAP-Role (Ownership-Detection)
							20	I	CP	NATTN_*		SAP-Role (Ownership-Detection)
	PERSA	Personalbereich	$PERSA	Personalbereich			10	I	EQ	0020		Personalbereich
	PLVAR	Planvariante	$PLVAR	Planvariante				I	EQ	*		Planvariante
	PRCTR	Profit Center	$PRCTR	Profit Center				I	EQ	*		Profit Center
	RCOMP	Gesellschaft	$RCOMP	Gesellschaft				I	EQ	MATTN		Gesellschaft
	SACHZ	Sachbearbeiter für Zeiterfassu	$SPART	Sachbearbeiter für Zeiterfassung				I	EQ	*		Sachbearbeiter für Zeiterfassu
	SBMOD	Sachbearbeitergruppe	$SBMOD	Sachbearbeitergruppe				I	EQ	*		Sachbearbeitergruppe
	SPART	Sparte	$SPART	Sparte				I	EQ	*		Sparte
	SWERK	Standortwerk	$SWERK	Standortwerk				I	EQ	0014		Standortwerk
	TPLST	Transportdispostelle	$TPLST	Transportdispostelle				I	EQ	*		Transportdispostelle
	VKBUR	Verkaufsbüro	$VKBUR	Verkaufsbüro				I	EQ	*		Verkaufsbüro
	VKGRP	Verkäufergruppe	$VKGRP	Verkäufergruppe				I	EQ	*		Verkäufergruppe
	VKORG	Verkaufsorganisation	$VKORG	Verkaufsorganisation				I	EQ	2000		Verkaufsorganisation
	VSTEL	Versandstelle	$VSTEL	Versandstelle				I	BT	1400	1499	Versandstelle
							20	I	EQ	2001		Versandstelle
	VTWEG	Vertriebsweg	$VTWEG	Vertriebsweg			10	I	EQ	*		Vertriebsweg
	WERKS	Werk	$WERKS	Werk				I	EQ	0014		Werk
							20	I	EQ	0020		Werk
	WKSET	Kurspflege: Arbeitsvorrat	$WKSET	Kurspflege: Arbeitsvorrat			10	I	EQ	SAE		Kurspflege: Arbeitsvorrat

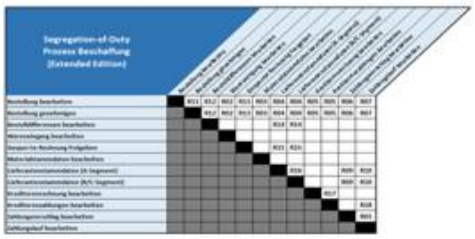
3.F SoD-Risk-Observer (Authorization)

The SoD Risk Observer **ensures that the policies are permanently adhered to by automated monitoring of the defined risks or that they** are **assessed**, **documented** and **dealt** with in the event of a violation.

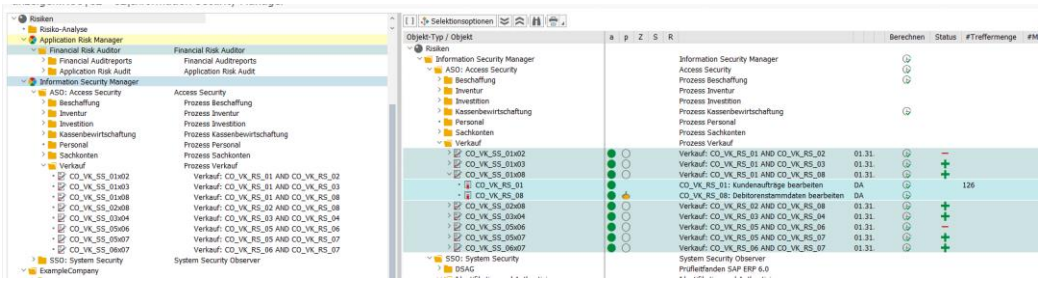
- Test item → **1 Authorization**
- Basics → DSAG, SAP-GRC, auditing houses
- Concept & Documentation → Excel
- Customizing → Risk Organizer
  → Rule Organizer
- Execution → Dialogue & Background
- Protocol → SoD Analysis
- Mitigation → Form & Workflow



The rules and risks are documented and can also be used to prove the applied set of rules.



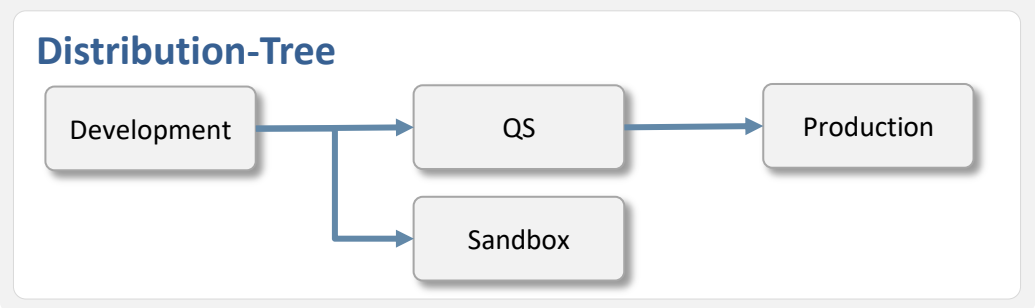
The rules and risks are transparently implemented in the system. They can be extended to suit the customer's needs as well as deactivated in a targeted manner.



3.G Authorization Distributor

The Authorization Distributor enables the distribution of authorizations (SAP roles) in the system landscape. The distribution path is defined in the distribution tree.

Example:



The actual distribution can be carried out either via the SAP transport system or directly via RFC distribution

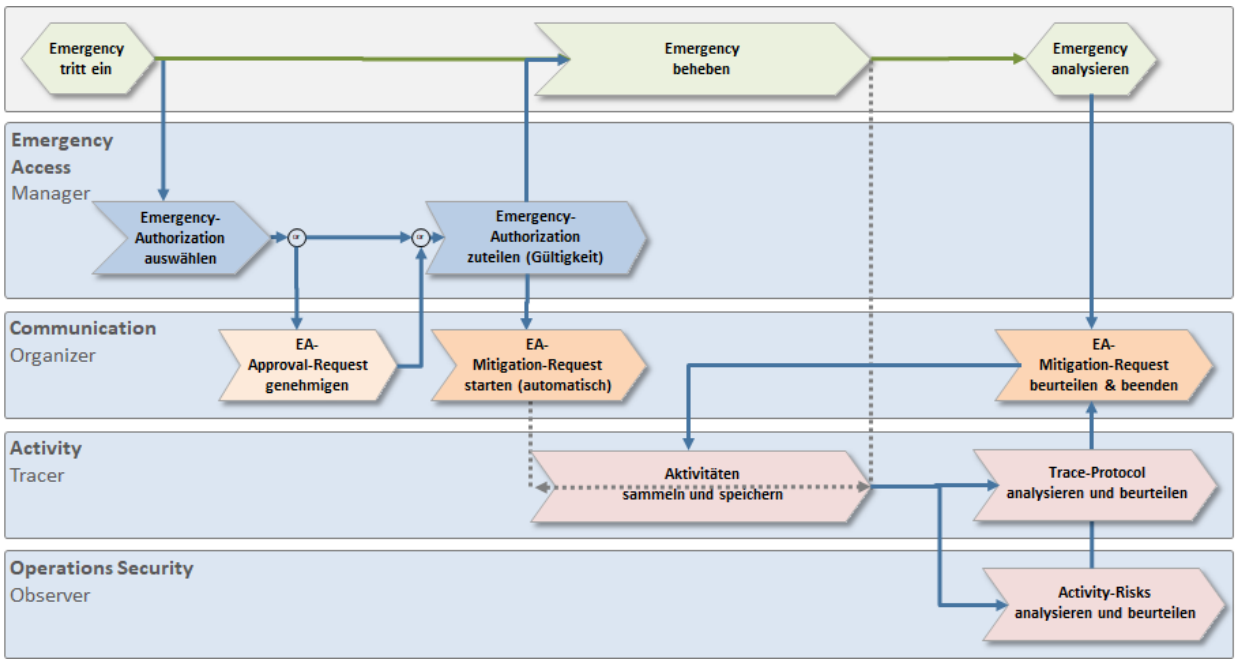
The distribution can also trigger a request with a corresponding workflow.

4. emergency accessManager [EAM]

The emergency accessManager (EAM) allows the **assignment** of "emergency permissions" and the **monitoring** of the activities carried out during the "emergency period".

The EAM is fully integrated into the various idFlow components.

4.A Process

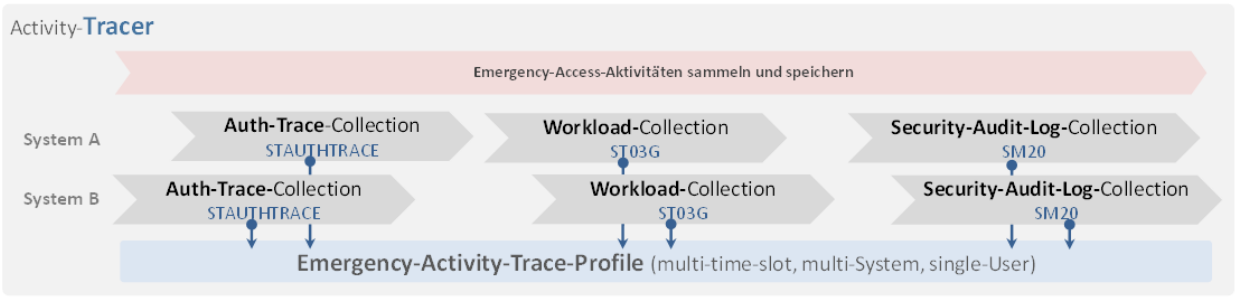


4.B Request-Workplace

Request with / without approval workflow

- Self-service (Web browser / Fiori)
- Admin Services (Web browser / Fiori or SAP GUI)

4.C Activity-Risk-Observer



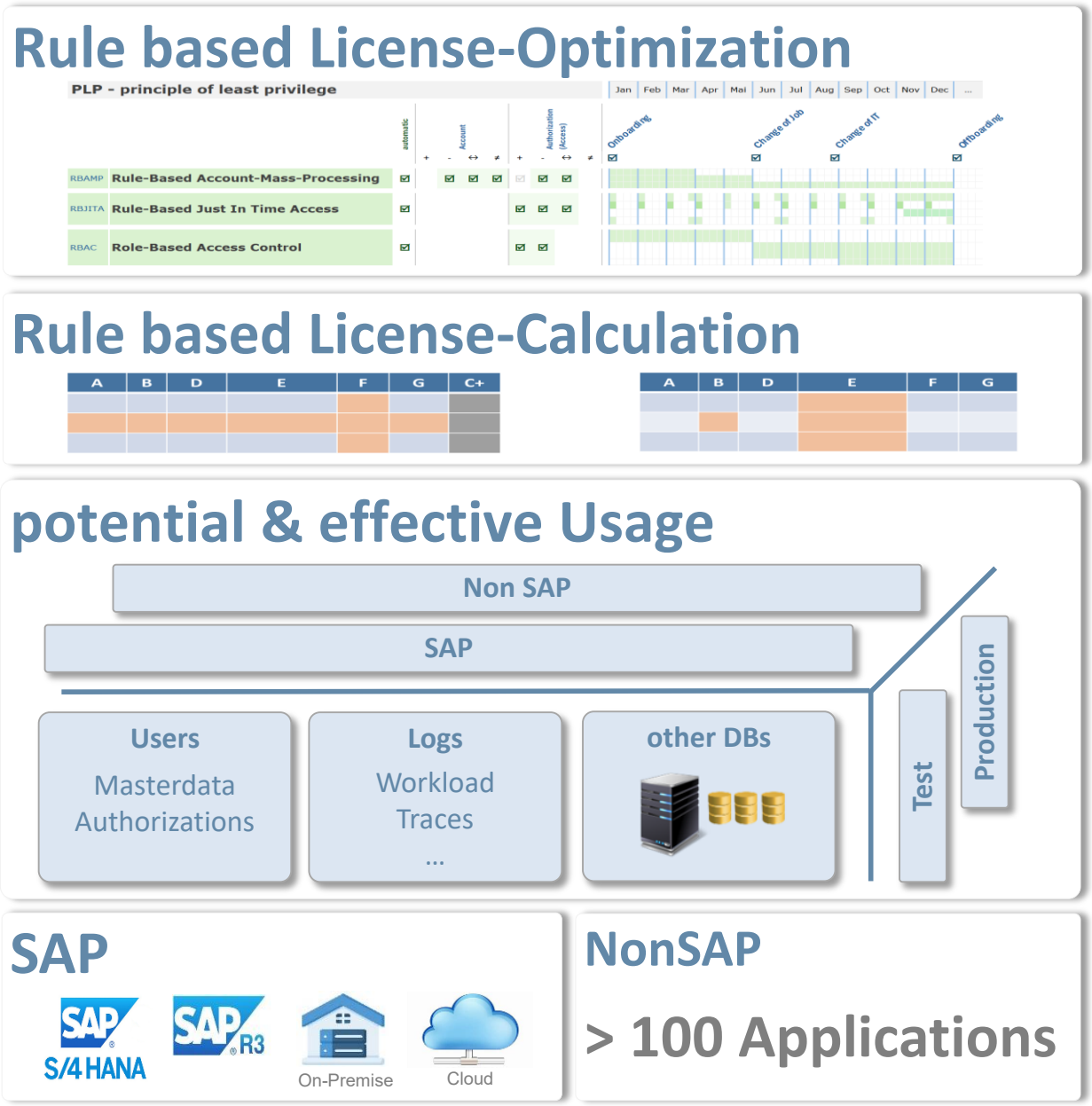
- manuelle Überwachung der Activities

- definierte Risiken
- automatisierte Überwachung der Activities

5. licenseManager [LM]

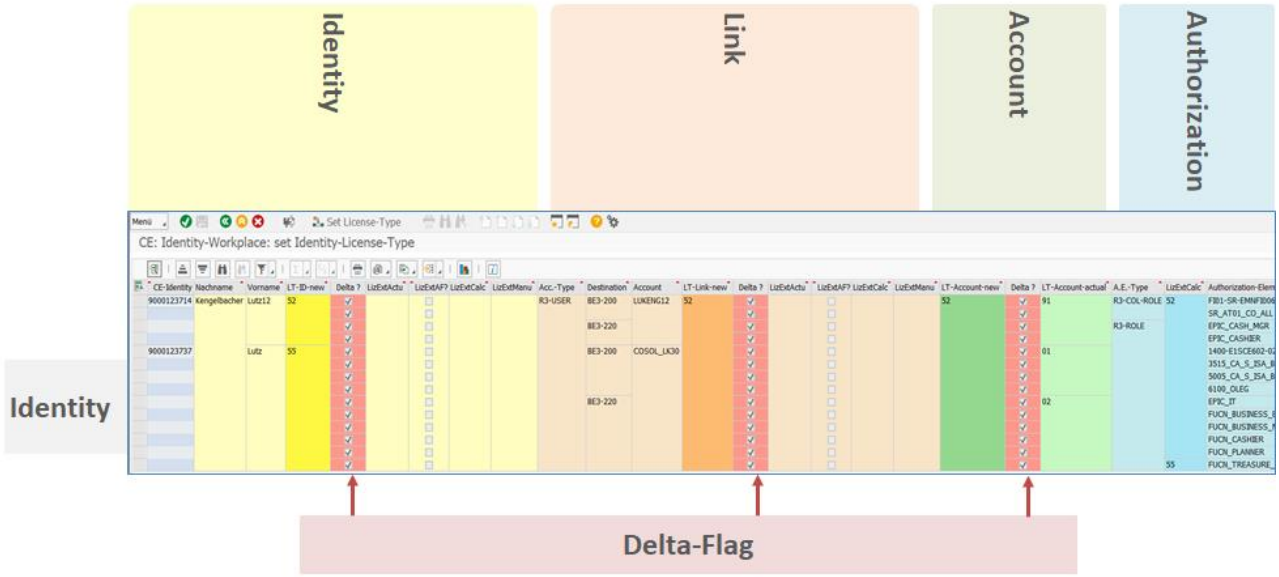
The licenseManager **calculates the** license type to be applied **per Identity & Account**.

5.A Big-Picture



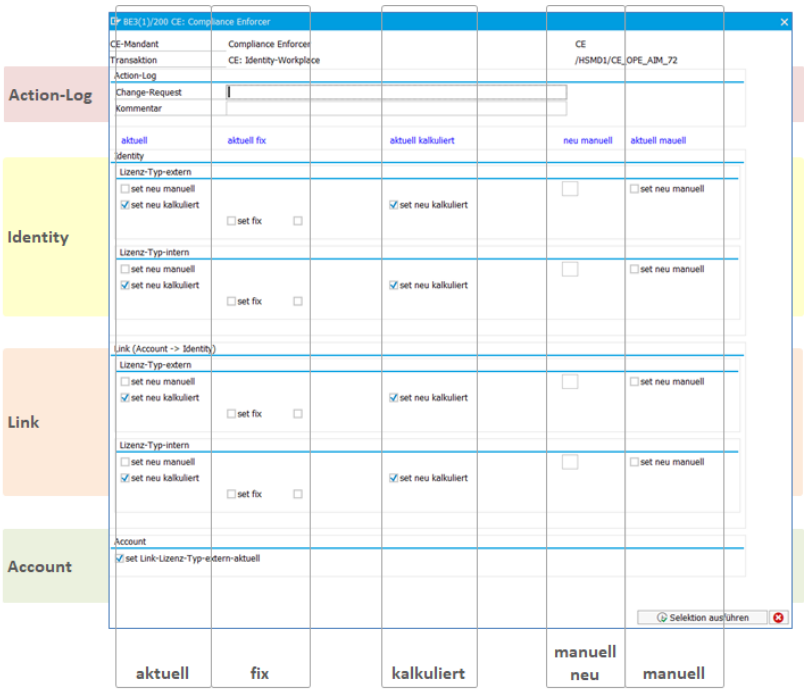
5.B License Calculator

- A distinction is made between an "internal license type" (e.g., for internal service allocation) and an "external license type" (e.g., for license measurement by SAP).
- The license type is determined based on the permissions assigned to the respective account or other measurable criteria or set manually.
- Inheritance to the Identity level takes place on the basis of the customer-specific defined set of rules.



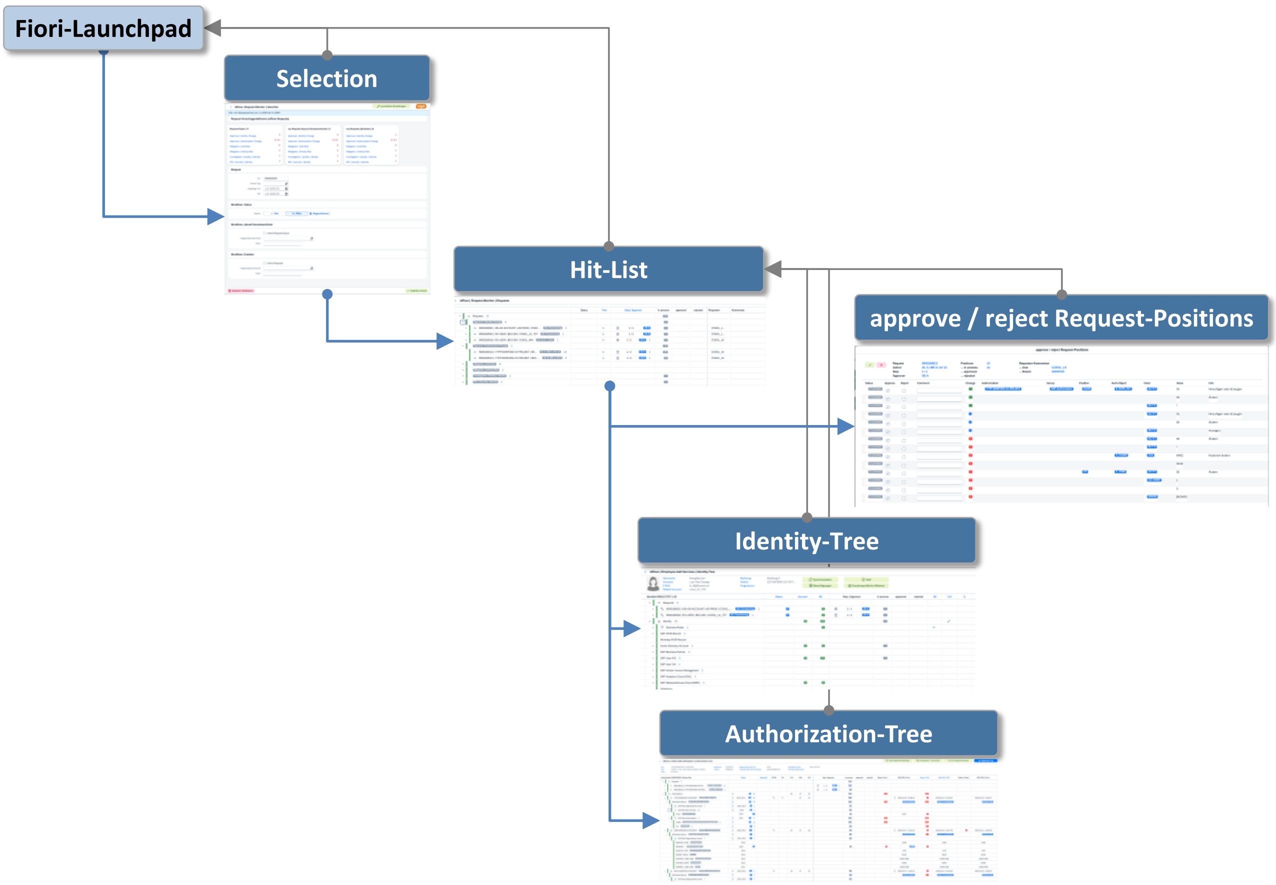
5.C License Update

- Both the calculated license type and a manually determined license type can be saved in the billing-relevant attributes.

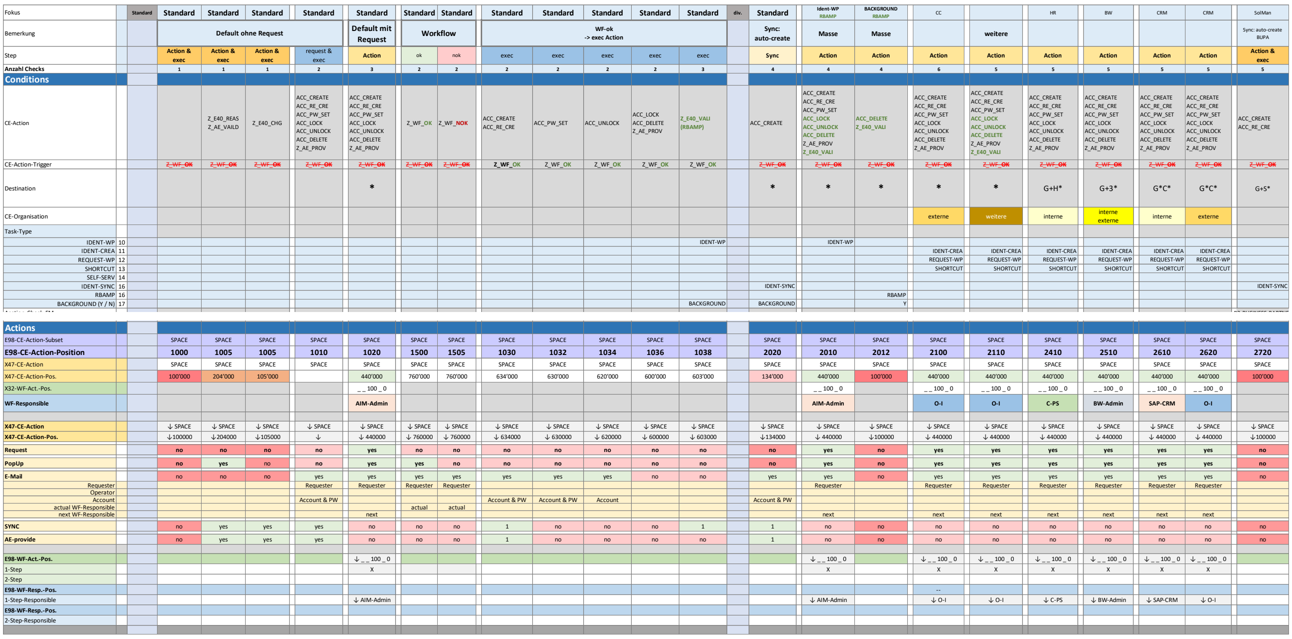


6. Requests & Workflow

6.A Request Monitor (Web Browser / Fiori)



6.B Workflow Customizing (Decision Table)



6.C Request Email

Email as Request for Approval / Denial

Attachment

APPROVE_request.SAP 392 Bytes

REJECT_request.SAP 390 Bytes

Message

Message to WF-Responsible (new activity - ready to execute)

Request-Subject	AIM-APPROVAL: Account create
Request-Object	Account-Type: R3-USER Destination: BE3-200 Account: COSOL_LK30 - Lutz Kengelbacher
Request-Status	ready
Contact	zusätzlicher Kontakt Lutz Kengelbacher
Notice	zusätzliche Notiz
Info	zusätzliche Information
Message-from	COSOL_LK - Lutz Kengelbacher

Text

Text

Beispieltext

/HSMD1/000000_XXXX: Mail-Type für Request mit approve/reject

Task

Task of Responsible

Action	ACC_CREATE		
Workflow-Task	APPROVAL		
Workflow-Step	1 / 1		
Workflow-Step-Responsible-OE	CE/CE_Organisationseinheit B 9000117197		
Workflow-Step-Responsible-1	COSOL_LK24	Lutz24 Kengelbacher	kengelbacher24@bluewin.ch
Workflow-Step-Responsible-2	COSOL_LK	Lutz Kengelbacher	lutz.kengelbacher@cosol.ch
Account-Type	R3-USER		
Destination	BE3-200		
Account	COSOL_LK30		
Firstname	Lutz		
Lastname	Kengelbacher		
E-Mail	lutz30.keng@test.ch		

Workflow-Information

Workflow-Information

Action	WF-Step	Entry-Type	Change-Request	User-Input	User-Input	User-Input	User	Date/Time
ACC_CREATE		REQUEST_CREATED					COSOL_LK	2020.12.09-03:48:49

Request-Details

Request-Details

Feldtext	Feldwert	Kommentar	Feldname
Mandant	200		MANDT
CE: CE-Objekt	9000156523		OBJECT
CE: Request-Event	AP-AC-ANAC		REQ_EVENT

E-mail as info

Message

Message to ACCOUNT

Subject	AIM-Info: Account COSOL_LK30 was created
Contact	info@cosol.ch
Notice	FAQ: www.cosol.ch/downloads/FAQ
Info	weitere Informationen .....
Message-from	COSOL_LK - Lutz Kengelbacher

Text

Text

Beispieltext

/HSMD1/000000_0000: E-mail ohne Request

Task

Information on Account

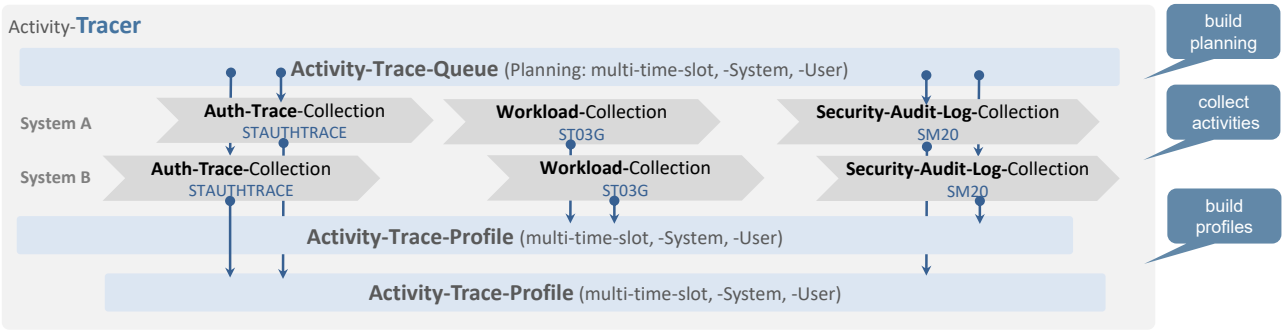
Action	ACC_CREATE
Account-Type	R3-USER
Destination	BE3-220
Account	COSOL_LK30
Password	Oa311469483!
Firstname	Lutz
Lastname	Kengelbacher
E-Mail	lutz30.keng@test.ch

7. Activity Tracer

The activity tracer **collects the activities** that were carried out by an account (e.g. SAP user) in a certain time window. The **three different trace types** achieve very good trace accuracy and display transactions such as "Display BOM" can also be recorded.

The traces are the basis for further analysis and design work.

7.A Trace -> Profile



7.B Structure

- adhoc traces
  - Emergency access (critical activities?)
- Planned Traces
  - Authorization Designer
  - Authorization-Observer
  - Concept: Excel
  - Customizing: Trace Queue
- 1 Trace includes:
  - 1 Trace Type (Authorization Trace, Workload, Security Audit Log)
  - 1 Account (SAP User)
  - 1 Destination (SAP system)
  - 1 day
- n Traces -> 1 Trace Profile (e.g. Trace Profile Buyer)
  - Multi-Time Slot
  - multi-user
  - Multi-System

BCB GmbH
Landhausstrasse 1
9053 Teufen
info@bcb-gmbh.ch
www.bcb-gmbh.ch