compliance solutions

idFlow

Booklet

Version	25.04.2024
Status	freigegeben
Sprache	deutsch

Inhaltsverzeichnis

1. idFlow:

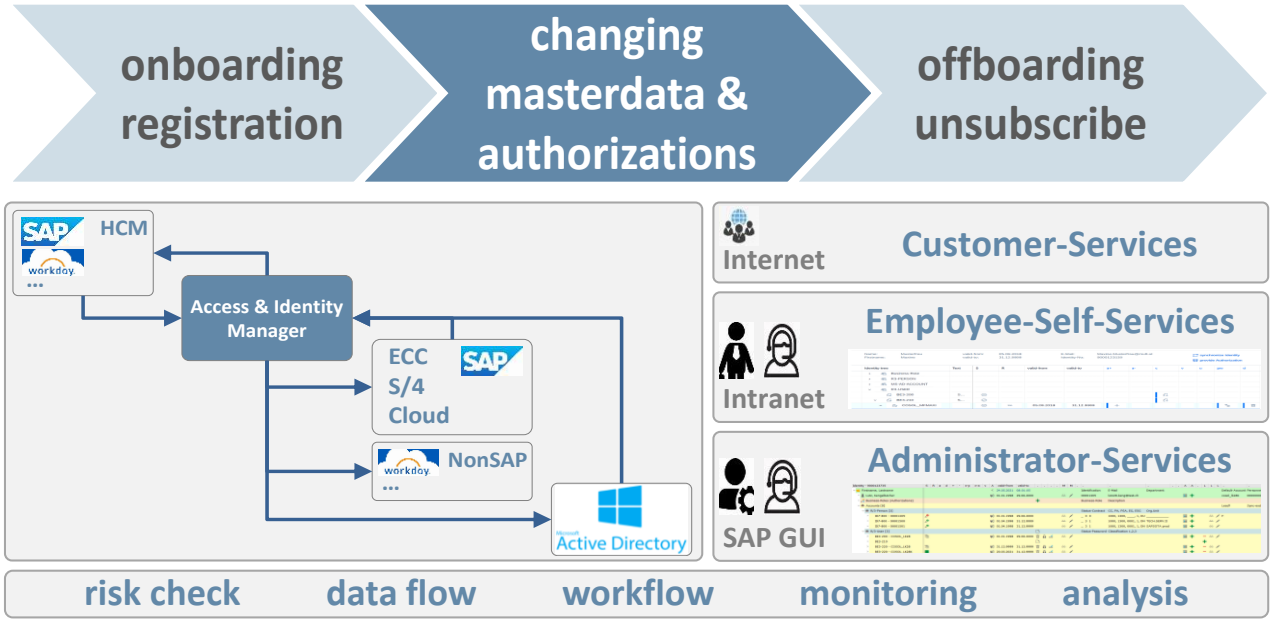
1.A Hauptfunktionen

- **id**Flow dient der Automatisierung und Optimierung der **User-/** und **Berechtigungs-Prozesse.**
- **id**Flow umfasst alle notwendigen Funktionen für **Synchronisation**, **Provisionierung**, **Workflow, Onboarding, Change, Offboarding** und **Risiko-Prüfung.**

1.B Alleinstellungsmerkmale

- **id**Flow ist ein hochintegriertes „All-in-One"-Produkt. Der gesamte Lebenszyklus aller Accounts und Berechtigungen der SAP- und NonSAP-Systeme wird unterstützt.
- **id**Flow ist ein in ABAP entwickeltes **SAP-AddOn** und benötigt **keine zusätzlichen Hardwareinvestitionen.**
- **id**Flow ermöglicht ein **konkurrenzloses Kosten <-> Nutzenverhältnis.**

1.C Big-Picture



Kontext	Integration der gesamten SAP-Systemlandschaft (SAP R/3, ECC, S/4, Cloud) und auch der NonSAP-Systeme)
Event-Recognition (create, change, delete)	Event-Recognition (create, change, delete) für alle angeschlossenen Systeme/Accounts z.B. ■ realtime-Verarbeitung eines Mitarbeiter-Eintritts ■ SAP-User-Löschung aufgrund eines «unsubscribe» in einem Webshop ■ Änderung der Organisationszuordnung eines Personalstammes ■ etc., etc. etc. ……
Interface-Level	Abhängig von Funktion und Aufgabe werden unterschiedliche User-Interfaces angeboten: ■ UI5/FIORI via Internet für z.B. Customer ■ UI5/FIORI via Intranet für Mitarbeiter-Self-Services ■ SAP-GUI für Administratoren
risk check	regelbasierte Analyse und Überwachung der SoD-Risiken und der Emergency-Access-Risiken
data flow	regelbasierte Synchronisation von Masterdata und Authorizations
workflow	■ regelbasierte und kontextabhängige Findung der Workflow-Steps und -Responsibles ■ E-Mail als Trigger und Workflow-Eingang für approve/reject durch die Responsibles
monitoring	Request-Monitor als Workflow-Inbox und -Überwachung
analysis	■ Inplace-Analysen (ALV-Grid) für alle relevanten Daten ■ InfoCockpit (MS-Excel) für diverse periodische- und adhoc-Analysen

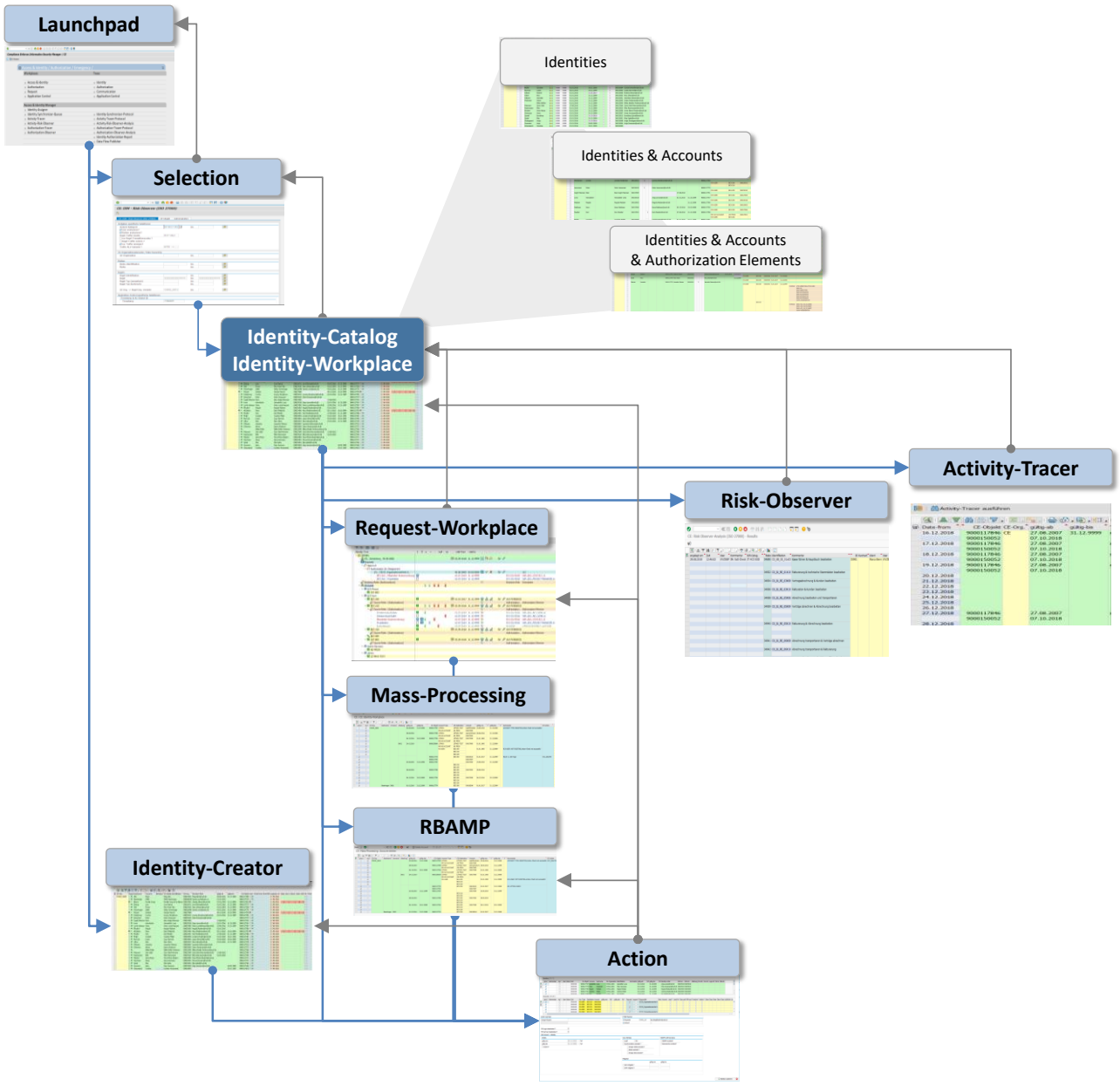
1.D Komponenten

access & identity Manager	
Catalog	Verwaltung aller Identities & Accounts
Request-Workplaces	Customer-, Employee-, Administrator-Services
Synchronizer	Account-Data-Flow (auto-create, -change)
Provider	Authorization-Provisioning (Defaults, Requests)
RBAMP	Rule-Based-Account-Mass-Processing
SoD-Risk-Observer	zu viele Berechtigungen? (-> Revision, etc.)
Activity-Tracer	welche Activities wurden durchgeführt?
Authorization-Observer	zu wenige Berechtigungen?
authorizationManager	
Catalog	Verwaltung aller Authorization-Elements
SoD-Risk-Observer	zu viele Berechtigungen? (-> Revision, etc.)
Optimizer	+ / - : Transaktionen/Applikationen (genutzte / ungenutzte)
Deriver	+ / - / change : Org.-Level der Kunden-Organisationseinheiten
emergency access Manager	
Request-Workplace	Provisionierung Notfallberechtigungen
Activity-Risk-Observer	Analyse von kritischen Actvities
riskObserver	
ASO, SSO, OSO	access-, system-, operations-security
licenseManager	
Calculator	Kalkulation & Optimierung der Lizenzen

2. access & identityManager

2.A Identity-Workplace (Catalog)

- Die Identity dient dazu, **zusammengehörende Accounts** der ganzen Systemlandschaft (SAP und NonSAP) zu **verknüpfen** und gemeinsam zu verarbeiten. So kann z.B. ein Softwareentwicklungs-User und ein Test-User (genutzt durch die gleiche Person auf dem gleichen SAP-QS-System) in der gleichen Identity zusammengefasst werden.
- Der Identity-Workplace (Catalog) ist die „**zentrale Schaltstelle»** für alle Identity-Tasks.
  - Masterdata
  - Request-Workplace (Administrator-Level)
  - Synchronizer
  - Mass-Processing (Dialog)
  - Rule-Based-Account-Mass-Prossessing (Background und Dialog)
  - SoD-Risk-Observer
  - Activity-Tracer
  - Emergency-Access



2.B Request-Workplaces

Die Request-Workplaces dienen den **verschiedenen Anwendergruppen** dazu, deren Anforderungen (Requests) zu erstellen. Die entstehenden Requests können **sowohl mit als auch ohne Workflow** verarbeitet werden.

Customer-Services

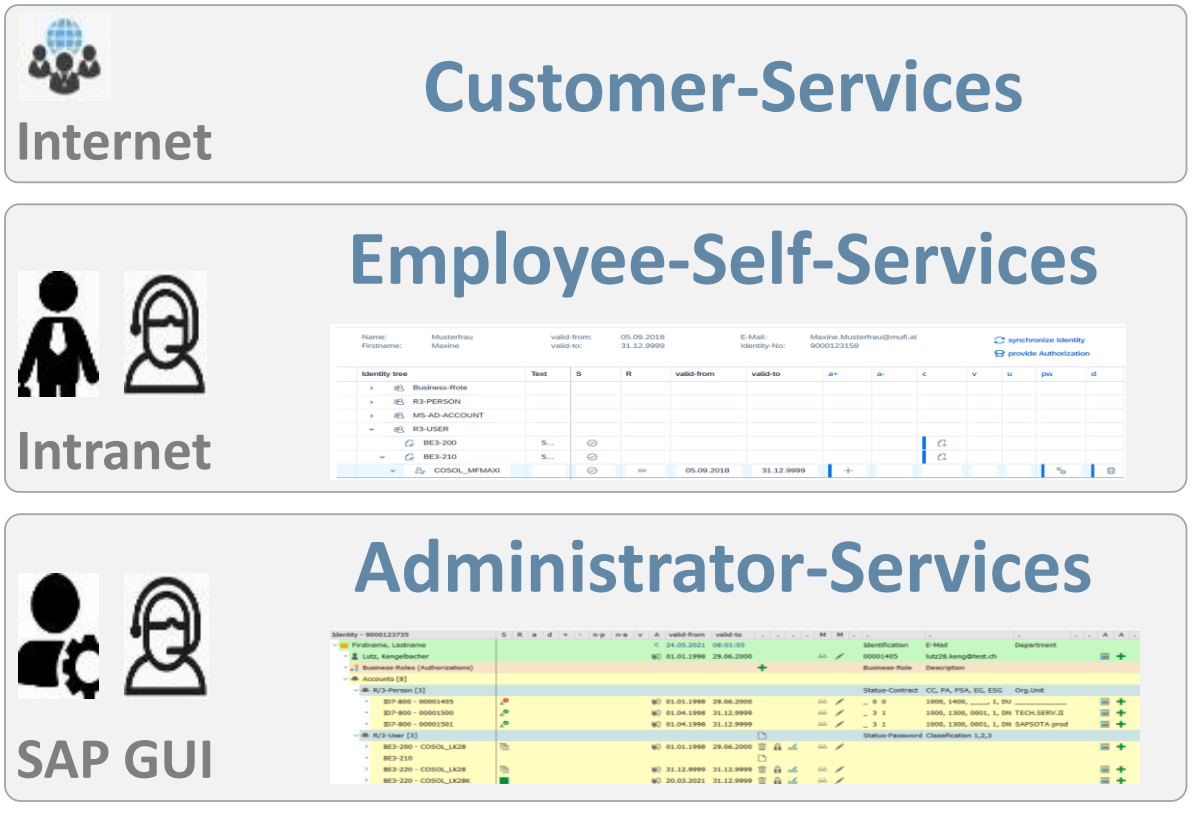
- B2C (z.B. Customer-Webshop) -> create/change Account
- B2B (z.B. Reseller-Webshop) -> create/change Account

Employee-Self-Services (UI5 / Fiori)

- Reset Password
- Request User
- Unlock User & set User vaild
- + / - Authorizations
- Change Masterdata
- Customer-Specifics

Administrator-Services (SAP-GUI)

- z.B. Mass-Processing, Request-Workplace, Identity-Creator, Identity-Assigner
- Create, Change, Delete
- Lock, Unlock
- + / - Berechtigungen
- …



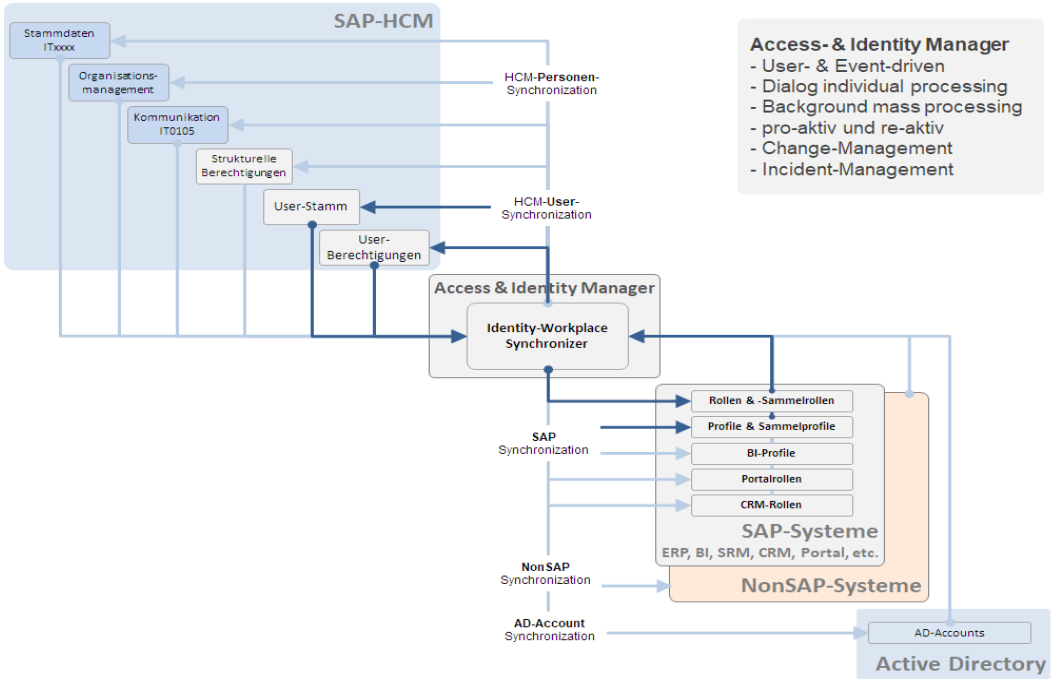
2.C Synchronizer & Provider

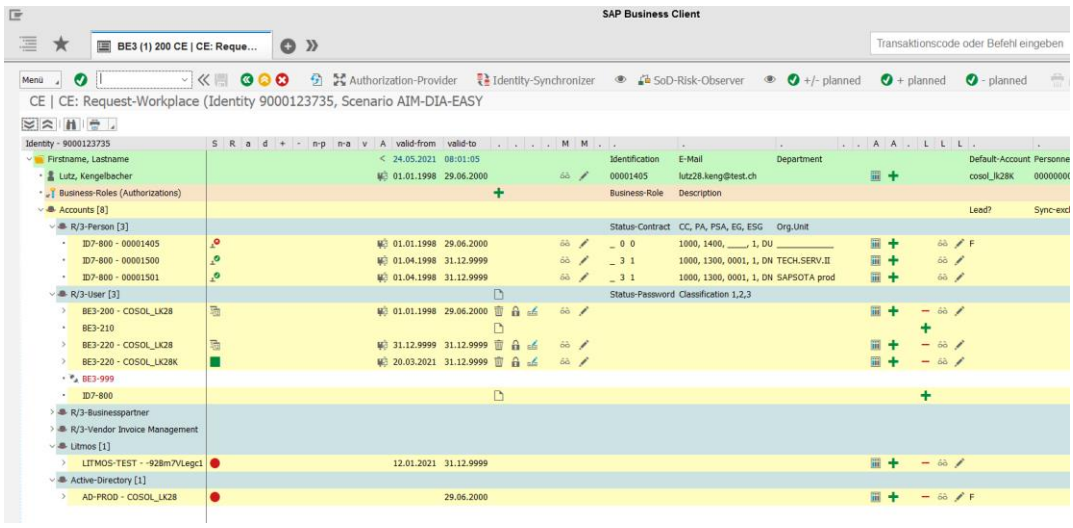
Der **Synchronizer** stellt sicher, dass die **Master-Data** der zusammengehörenden Accounts abgeglichen werden.

Der **Provider** stellt sicher, dass die notwendigen **Berechtigungen** (Defaults) und die angeforderten Berechtigungen (Requests) den relevanten Accounts zugeteilt werden.

Sowohl der Synchronizer wie auch der Provider basieren auf **umfangreichen Regelwerken**, die im **Customizing** definiert und jederzeit durch den Customer angepasst werden können.

- Die Identity dient als «Container» zusammengehörender Accounts.
  (z.B. R/3-User, S/4HANA-User, SAP-Cloud-user, AD-Account, Person, NonSAP-Accounts, …)
- Jedes System und jedes Attribut können sowohl Input als auch Output sein.
- Regeln werden als Entscheidungstabellen abgebildet.
- Kundenspezifische Exits sind vorgesehen.
- Accounts und Berechtigungen können als Default definiert werden.
  (Ableitung aus z.B. - Planstelle, - Personendaten, vorhanden Accounts, etc.)
- Szenarien definieren den Datenfluss und können für unterschiedliche Bedürfnisse flexibel abgebildet werden.
  (z.B. interne MA, externe MA, technische Accounts, ….)





2.D Mass-Processing (Dialog)

Die Massenverarbeitung ermöglicht die **gleichzeitige**, **kontrollierte** und **protokollierte Änderung** an n Datenobjekten.

Dabei können die Änderungen auf 5 Level vorgenommen werden:

- Identity
- Link Identity < -> Account
- Account
- Link Account <-> Authorization-Element
- Authorization-Element

		pro	Dialog/Batch
Identity			
	Change Identity-Data	Identity	Dialog
	Change Identity-CE-Organisation	Identity	Dialog
Link Identity -> Account			
	Change Link-Data	Link	Dialog
	Delimit Link-Validity	Link	Dialog
	Unassign	Link	Dialog
	Reassign	Link	Dialog
Account			
	Rule-based account-mass-processing	Account	Dialog & Batch
	Unlock	Account	Dialog
	Lock	Account	Dialog
	Create	Account	Dialog
	Re-create	Account	Dialog
	Delete	Account	Dialog
	Set password	Account	Dialog
Link Account -> Authorization-Element			
	Change Link-Data	AE	Dialog
	+ planned-AE	Account	Dialog
	- planned AE	Account	Dialog
	+/- planned AE (Default & BR-derivativ	Account	Dialog
	+ planned-AE (accept not planned)	AE	Dialog
	- planned-AE (accept not actual)	AE	Dialog
Authorization-Element			
	Provide AE (set planned -> actual)	AE	Dialog

2.E RBAMP (Background & Dialog)

Rule-Based-Account-Mass-Processing ist das Gegenstück zu den additiven Funktionen wie Identity-Creator etc.
Die typischen Aufgaben sind die **subtraktiven Massnahmen** wie **Löschung**, **Sperrung**, **Abgrenzung**, etc.

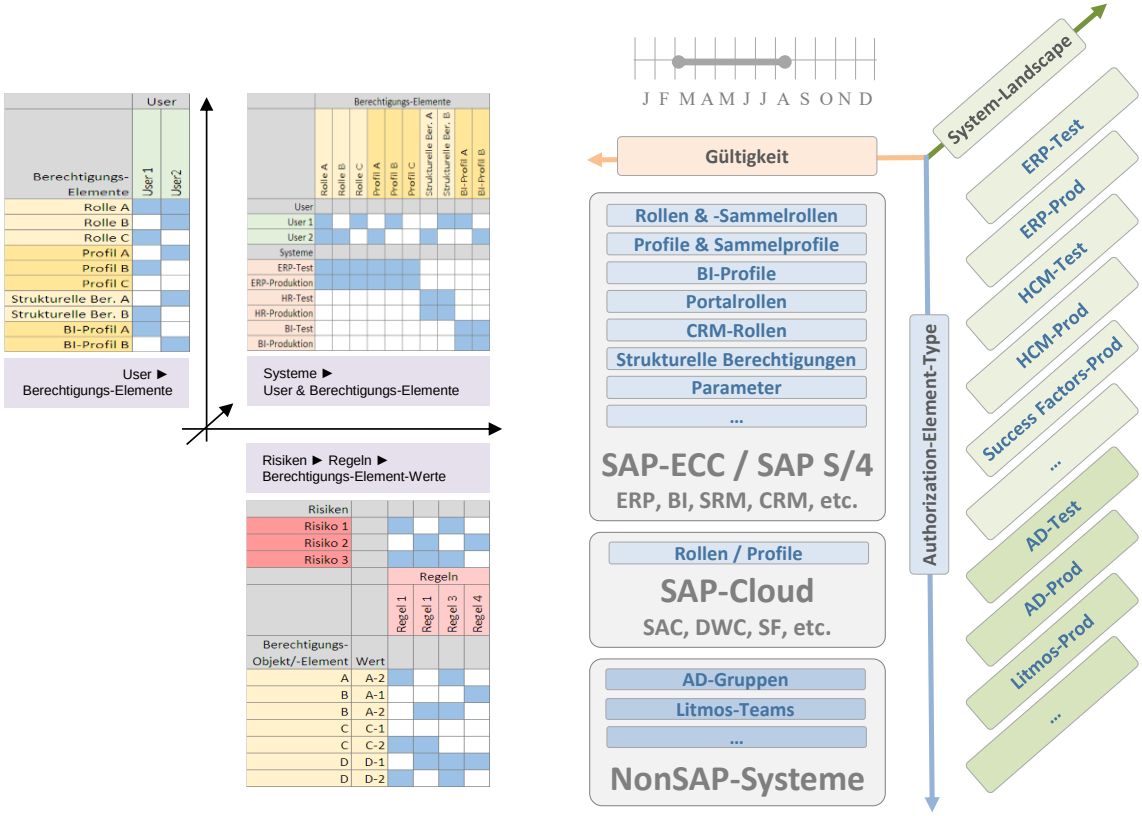
- Konzept & Doku → Excel
- Customizing → Decission table (E96, E97, E98)
- Execution → Dialog & Background
- Protokoll → Application-Log, Action-Log, E-Mail an Administrator

		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	

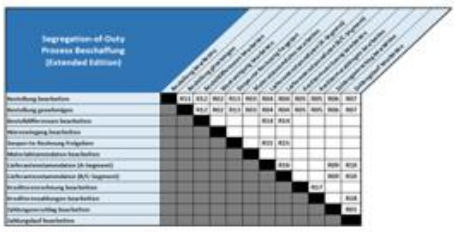
2.F SoD-Risk-Observer (Identity)

Der SoD-Risk-Observer stellt durch **automatisierte Überwachung** der definierten Risiken sicher, dass die Policies permanent eingehalten werden oder bei einem **Verstoss beurteilt**, **dokumentiert** und **behandelt** werden.

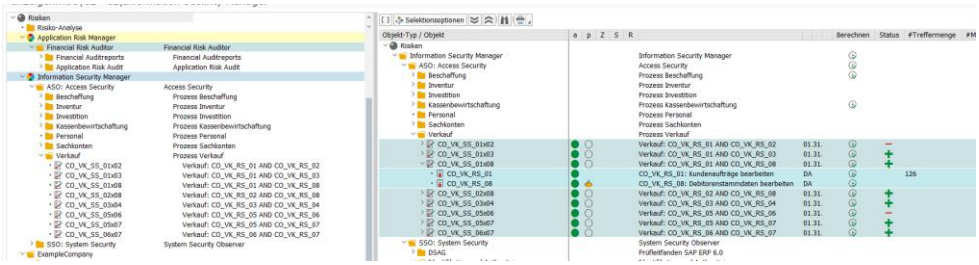
- Prüfgegenstand → **1 Identity**
- Grundlagen → DSAG, SAP-GRC, Revisionshäuser
- Konzept & Doku → Excel
- Customizing → Risk-Organizer
  → Rule-Organizer
- Execution → Dialog & Background
- Protokoll → SoD-Analysis
- Mitigation → Formular & Workflow



Die Regeln und Risiken sind dokumentiert und können auch für den Nachweis des angewendeten Regelwerks verwendet werden.



Die Regel und Risiken sind transparent im System implementiert. Sie können ebenso kundenspezifisch erweitert wie auch gezielt deaktiviert werden.

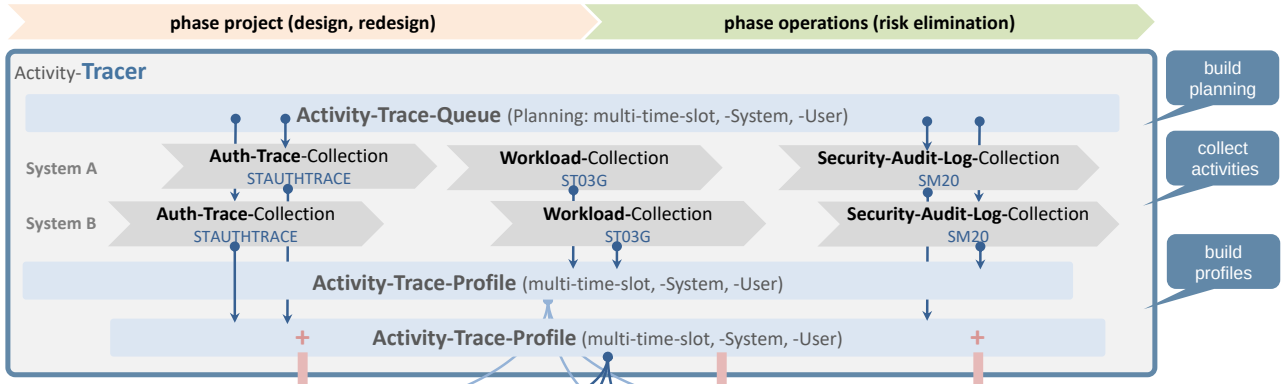


2.G Activity-Tracer

Der Activity-Tracer **sammelt die Aktivitäten,** die von einem Account (z.B. SAP-User) in einem bestimmten Zeitfenster durchgeführt wurden. Durch die **drei verschiedenen Trace-Typen** wird eine sehr gute Trace-Genauigkeit erreicht und es können z.B. auch Anzeigetransaktionen wie „Anzeigen Stückliste“ erfasst werden.

Die Traces sind Grundlage für weiterführende Analysen und Design-Arbeiten.

- adhoc Traces
  - Emergency-Access (kritische Aktivitäten?)
- geplante Traces
  - Authorization-Designer
  - Authorization-Observer
  - Konzept: Excel
  - Customizing: Trace-Queue
- 1 Trace umfasst:
  - 1 Trace-Typ (Authorization-Trace, Workload, Security-Audit-Log)
  - 1 Account (SAP-User)
  - 1 Destination (SAP-System)
  - 1 Tag
- n Traces -> 1 Trace-Profile
  (z.B. Trace-Profil Einkäufer)
  - multi-time-slot
  - multi-user
  - multi-system



2.H Authorization-Observer

Der Authorization-Observer hat die Aufgabe die **Risiken** zu erkennen, welche durch Design / Redesign von Berechtigungen entstehen (und im **Produktivbetrieb eintreten** können) und deren Eliminierung zu unterstützen.

Dabei ist zwischen zwei Risiko-Typen zu unterscheiden:

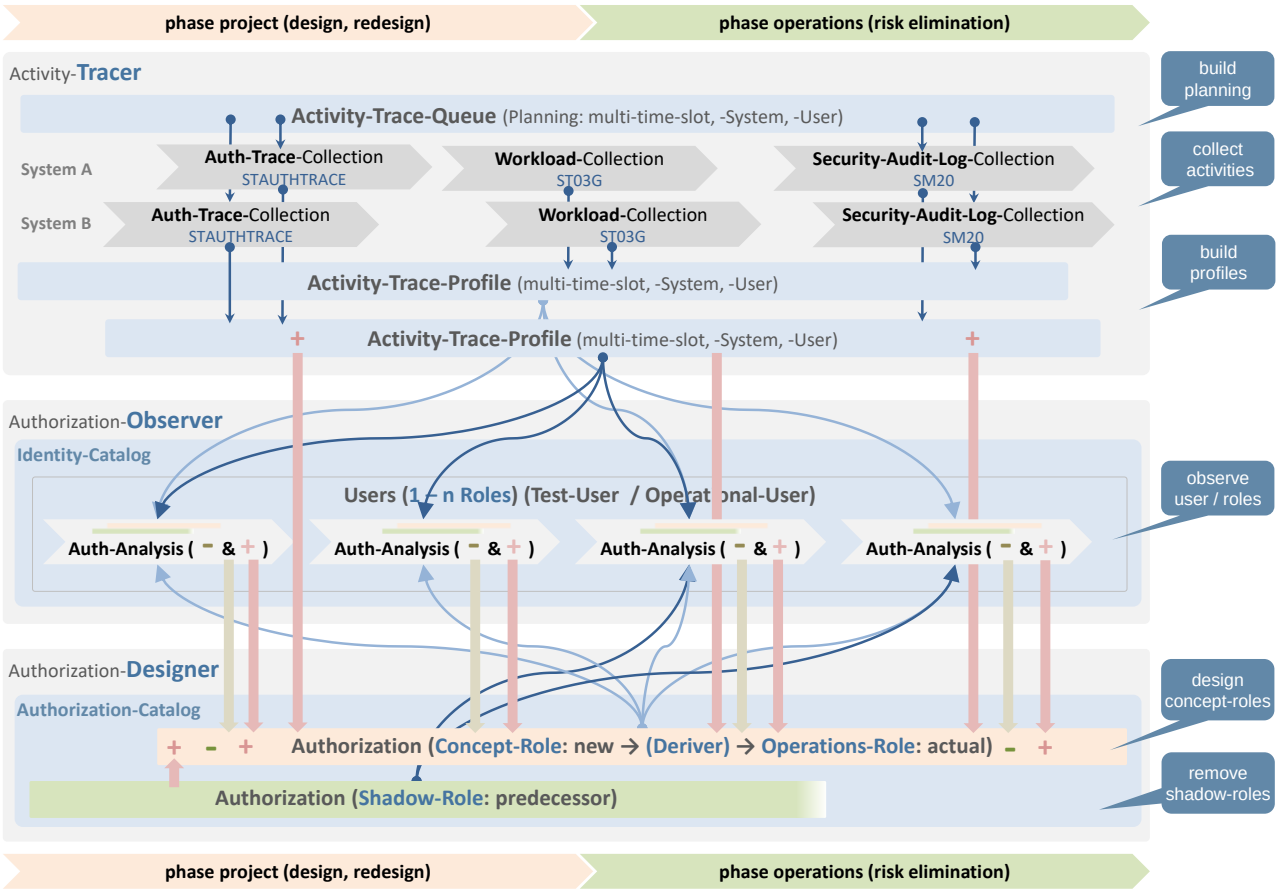
- „**zu wenig** Berechtigungen“ -> **Operations-Risk-Eliminator**
  -> Anwender kann aufgrund fehlender Berechtigungen nicht arbeiten!
- „**zu viele** Berechtigungen“ -> **SoD-Risk-Optimizer**
  -> SoD-Risiken etc. entstehen aufgrund nicht notwendiger Elemente in den Berechtigungen

Bei beiden Risiko-Typen besteht das Analyse-Prinzip darin, die einem Account (z.B. R/3-User) zugewiesenen Berechtigungen, gegen die gesammelten Traces zu prüfen.

- -> **Notwendigkeit** (Nutzung) der **Shadow-Roles** (bisherige Rollen) -> **zu wenig Berechtigungen**
- -> **Überflüssigkeit** (Nicht-Nutzung) von **Berechtigungselementen** -> **zu viele Berechtigungen**

Diese **Analysen** werden iterativ, sowohl in der **Projektphase** (Design / Redesign) als auch in der **Produktivphase**, durchgeführt. Jeder Analysezyklus führt dabei zu einer **Optimierung** der Berechtigungen.

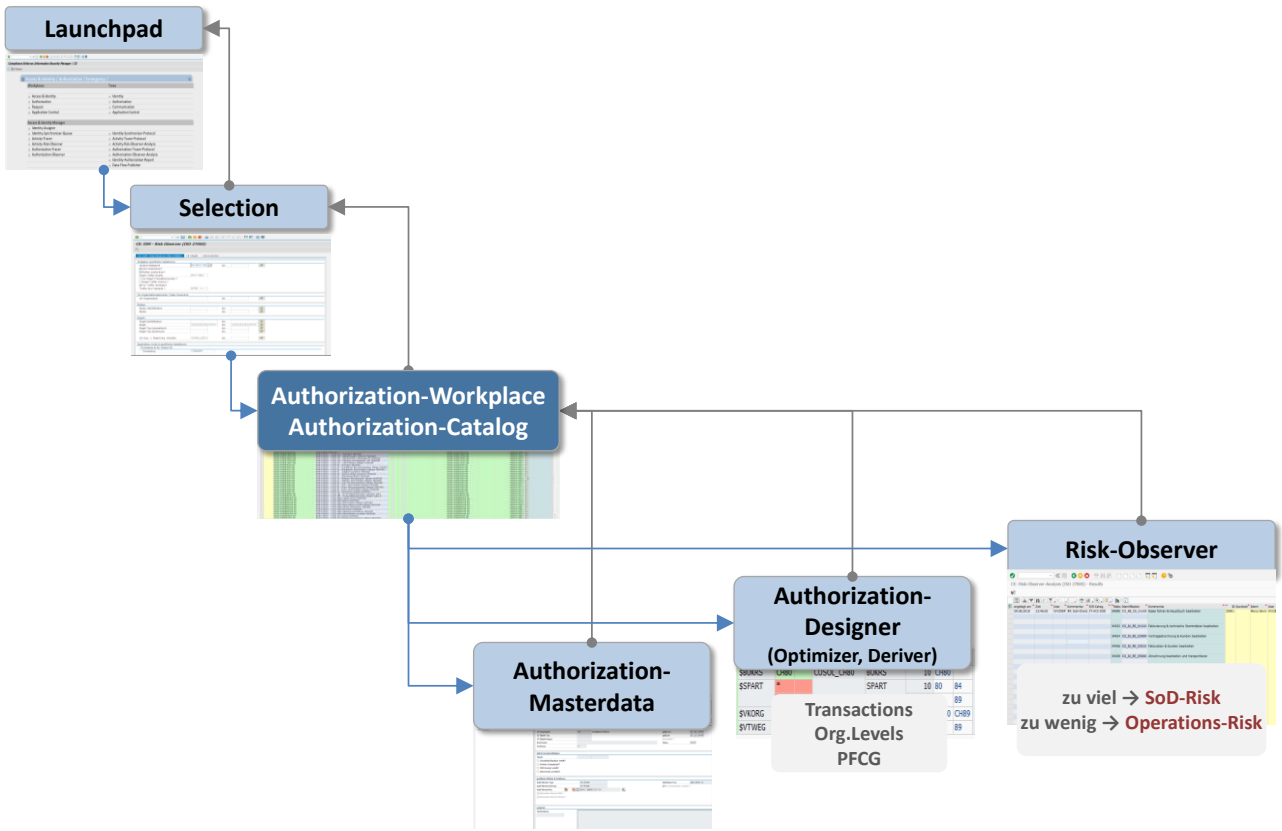
Um die Operation-Risks in der Produktivphase zu eliminieren, **behält der Anwender seine bisherigen Rollen,** solange **bis diese „Shadow-Roles“ nicht mehr notwendig** sind.



3. authorizationManager

3.A Authorization-Workplace (Catalog)

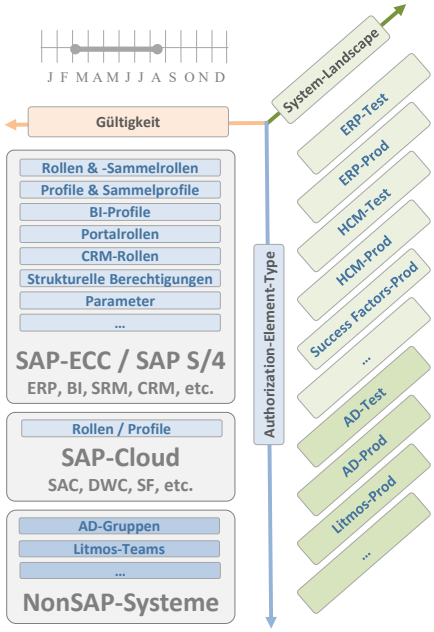
- Eine Authorization dient dazu, allen relevanten Applikationsberechtigungen (z.B. R/3-Sammelrolle) eine Hülle zur Verfügung zu stellen, um damit den kompletten Lebenszyklus der Authorization effizient und effektiv zu unterstützen.
- Der Authorization-Workplace (Catalog) ist die zentrale «Schaltstelle» für alle Authorization-Tasks.
    - Masterdata
    - SoD-Risk-Observer
    - Optimizer
    - Deriver



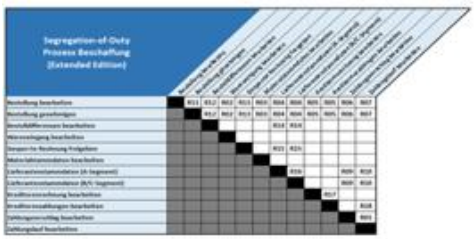
3.B SoD-Risk-Observer (Authorization)

Der SoD-Risk-Observer stellt durch **automatisierte Überwachung** der definierten Risiken sicher, dass die Policies permanent eingehalten werden oder bei einem **Verstoss beurteilt**, **dokumentiert** und **behandelt** werden.

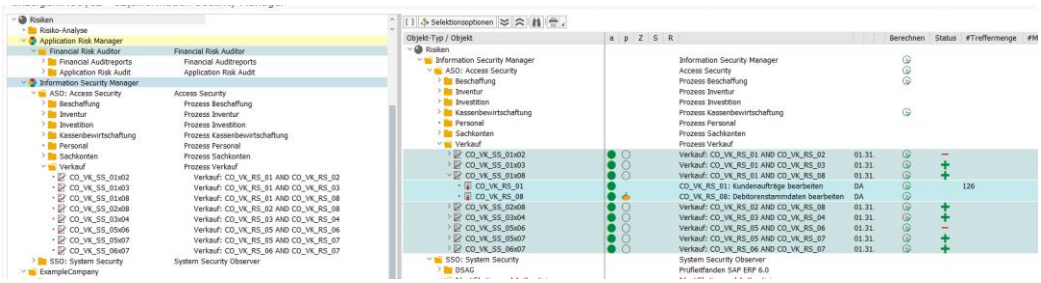
- Prüfgegenstand → **1 Authorization**
- Grundlagen → DSAG, SAP-GRC, Revisionshäuser
- Konzept & Doku → Excel
- Customizing → Risk-Organizer
  → Rule-Organizer
- Execution → Dialog & Background
- Protokoll → SoD-Analysis
- Mitigation → Formular & Workflow



Die Regeln und Risiken sind dokumentiert und können auch für den Nachweis des angewendeten Regelwerks verwendet werden.



Die Regel und Risiken sind transparent im System implementiert. Sie können ebenso kundenspezifisch erweitert wie auch gezielt deaktiviert werden.

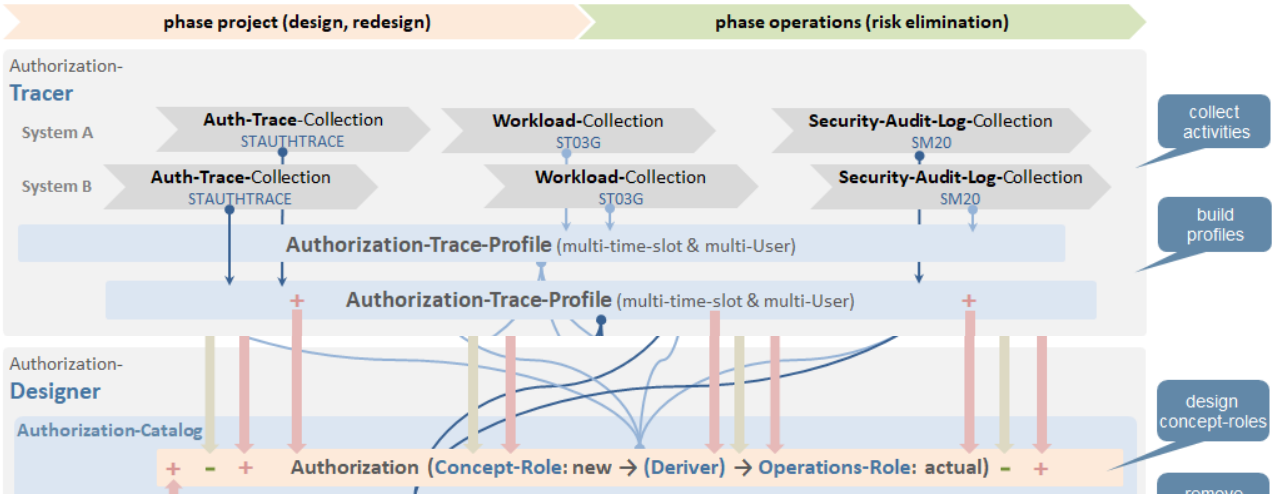


3.C Optimizer

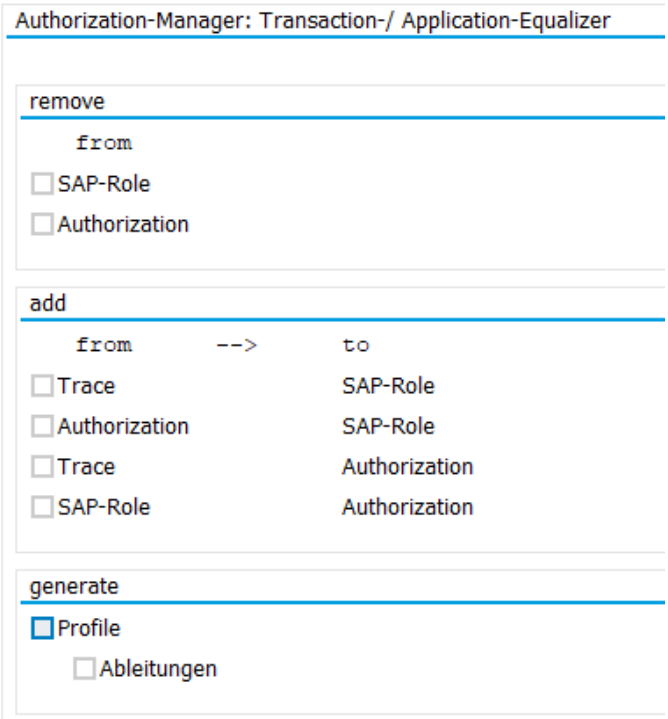
Der Optimizer stellt während des Designs / Redesigns einer Berechtigung sicher, dass die **notwendigen Transaktionen/Applikationen erkannt und in die Berechtigung integriert** werden.

Der Soll-Zustand (Menge der Transaktionen/Applikationen) wird definiert durch:

- die in den Traces gesammelten TR/App
- die manuellen Vorgaben/Definition in den Masterdata der Authorization



Der Equalizer ermöglich den spezifischen Abgleich zwischen den Traces, der Authorization im Katalog und der SAP-Role.

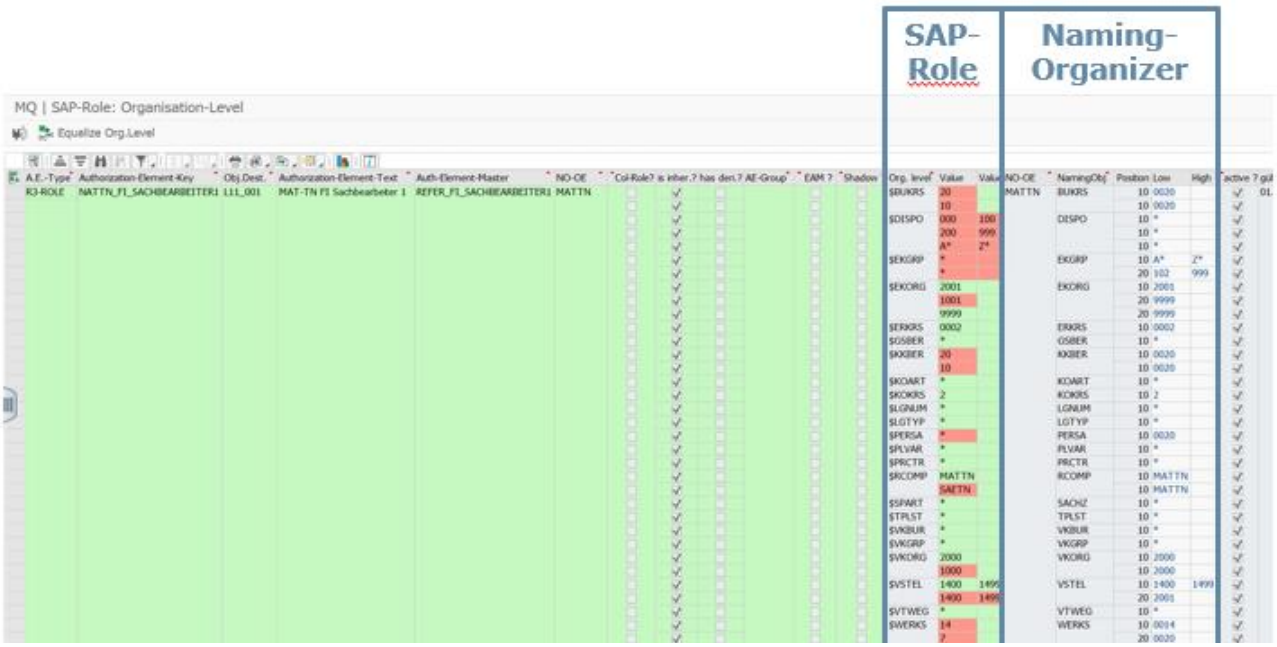


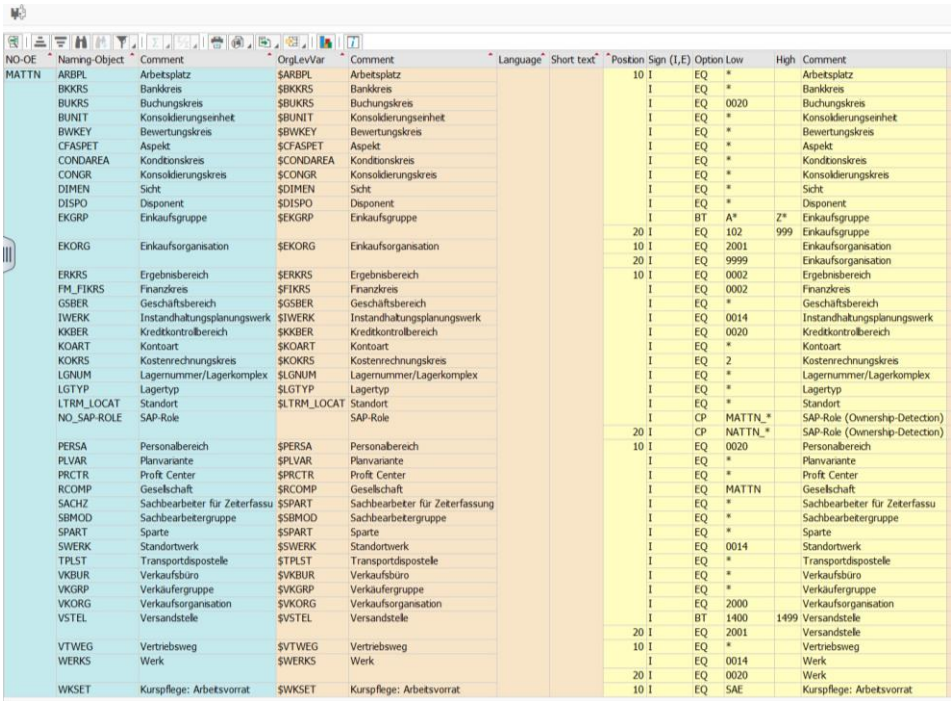
3.D Deriver

Der Deriver stellt sicher, dass die in den Berechtigungen (**Ableitungen aus Master-Rollen**) definierten **Org.Level** den Vorgaben entsprechen.

Die Vorgaben werden pro Customer-Organisationseinheit im Customizing (**Naming-Organizer**) definiert.

- Der Sollzustand (Werte der Org.Level) wird im Naming-Organizer definiert.
- Der Abgleich in den Quellsystemen kann partiell oder komplett erfolgen.
- Die Generierung in den Quellsystemen kann direkt angestossen werden.





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

4. emergency accessManager

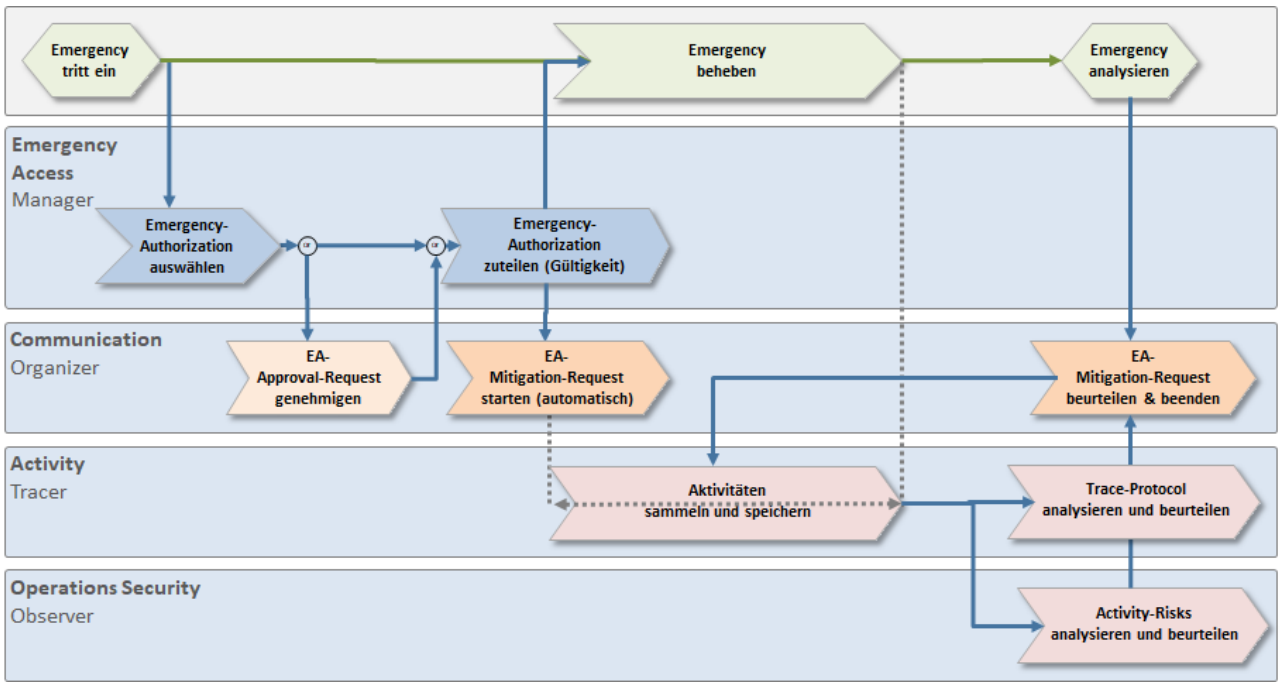
Der emergency accessManager (EAM) ermöglicht die **Zuteilung** von "Notfall-Berechtigungen" und die **Überwachung** der Aktivitäten, welche im "Notfall-Zeitraum" durchgeführt wurden.

Der EAM ist vollumfänglich in die verschiedenen idFlow-Komponenten integriert.

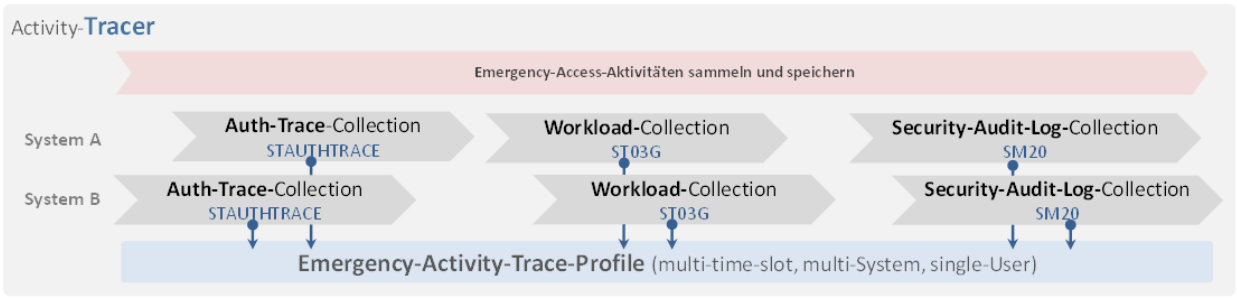
4.A Request-Workplace

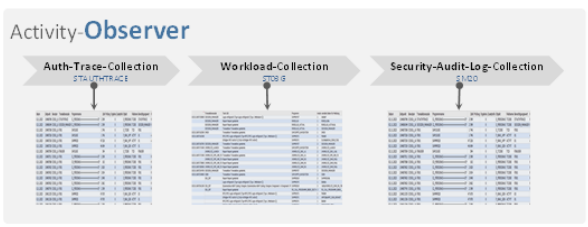
Request mit / ohne Freigabeworkflow

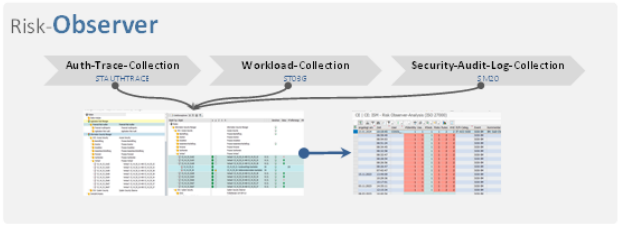
- Self-Service (Intranet)
- Admin-Services (SAP GUI)



4.B Activity-Risk-Observer







- manuelle Überwachung der Activities

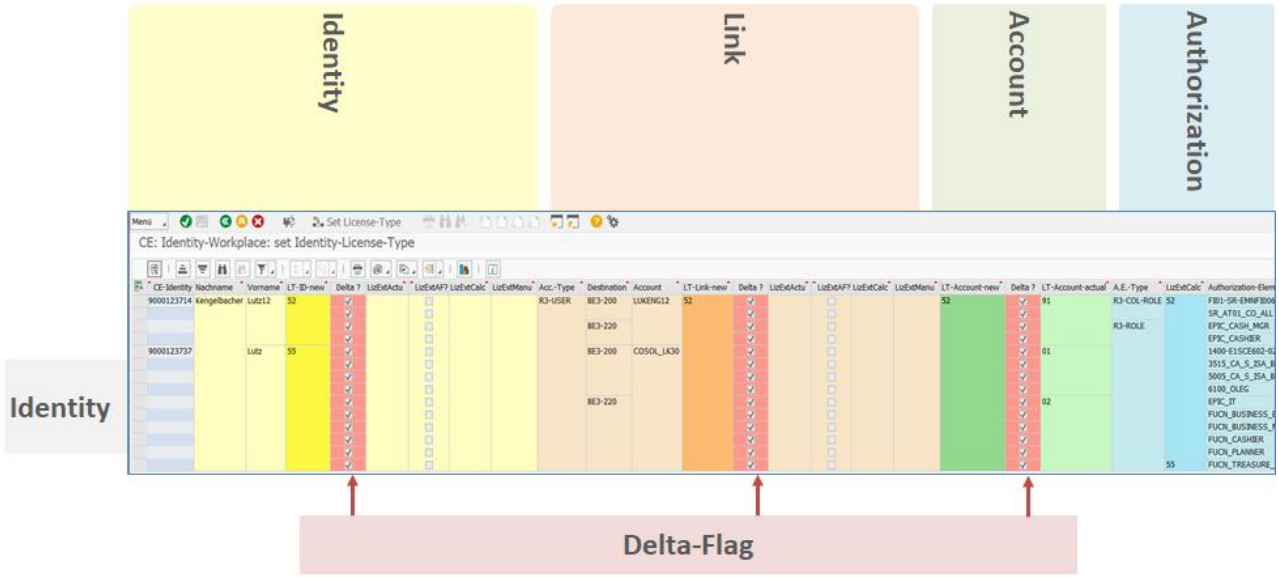
- definierte Risiken
- automatisierte Überwachung der Activities

5. licenseManager

Der licenseManger **kalkuliert** pro Identity & Account den **anzuwendenden Lizenztyp**.

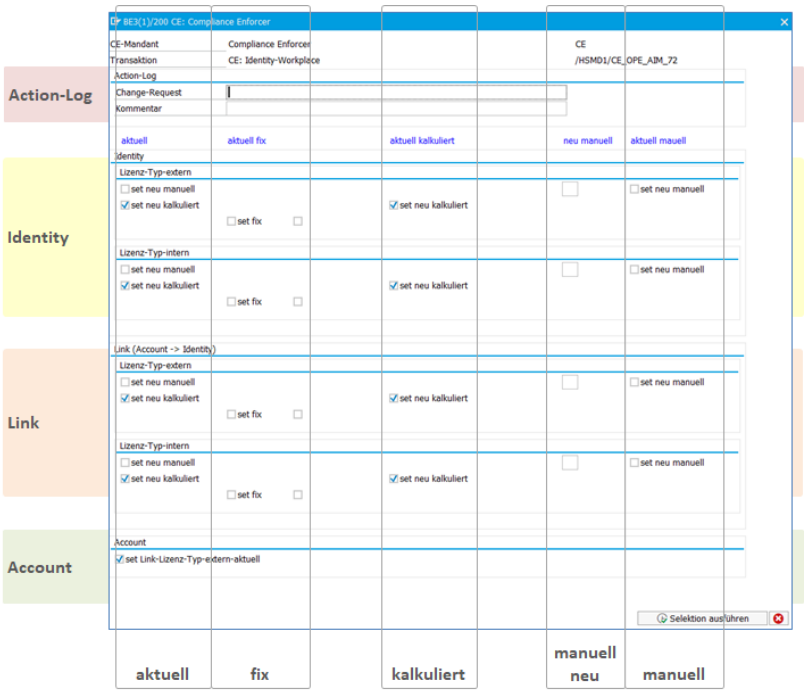
5.A Calculator

- Es wird zwischen einem „internen Lizenztyp“ (z.B. für die interne Leistungsverrechnung) und einem „externen Lizenztyp“ (z.B. für die Lizenzvermessung durch SAP) unterschieden.
- Der Lizenztyp wird aufgrund der dem jeweiligen Account zugeteilten Berechtigungen oder anderer messbarer Kriterien ermittelt oder manuell gesetzt.
- Die Vererbung auf den Level Identity erfolgt aufgrund des kundenspezifisch definierten Regelwerks.



5.B DB-Update

- Es kann sowohl der kalkulierte Lizenztyp wie auch ein manuell bestimmter Lizenztyp in die verrechnungsrelevanten Attribute gespeichert werden.



cosol GmbH
Vogelherdstrasse 21
CH-9016 St.Gallen
info@cosol.ch
www.cosol.ch