idFlow

Booklet

Version	04.08.2025
Sprache	Deutsch

Inhaltsverzeichnis

1. idFlow

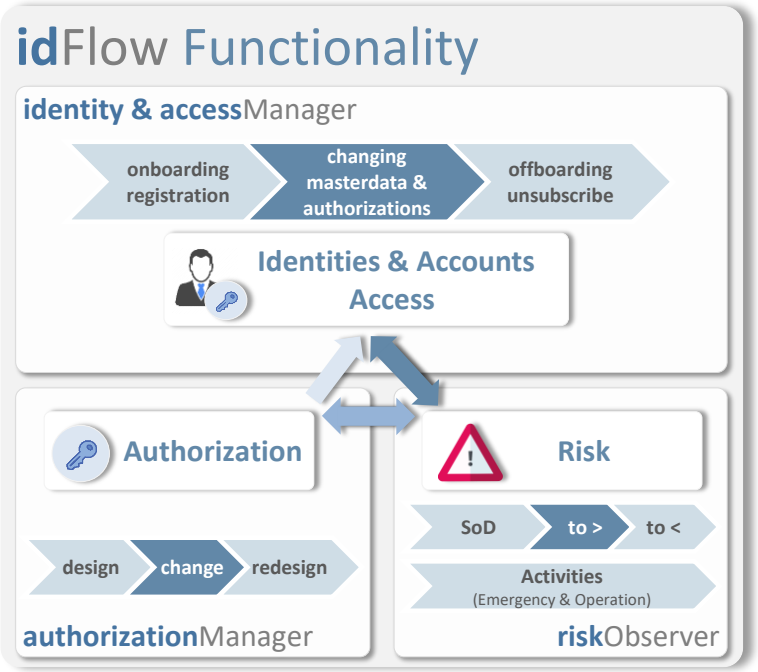
1.A Hauptaufgaben

- **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.**

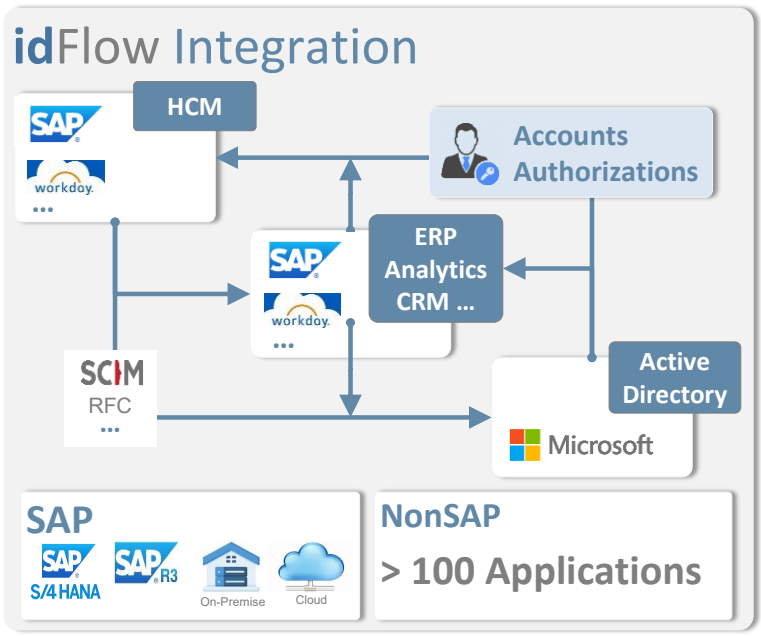
1.B Alleinstellungsmerkmale

- **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.**

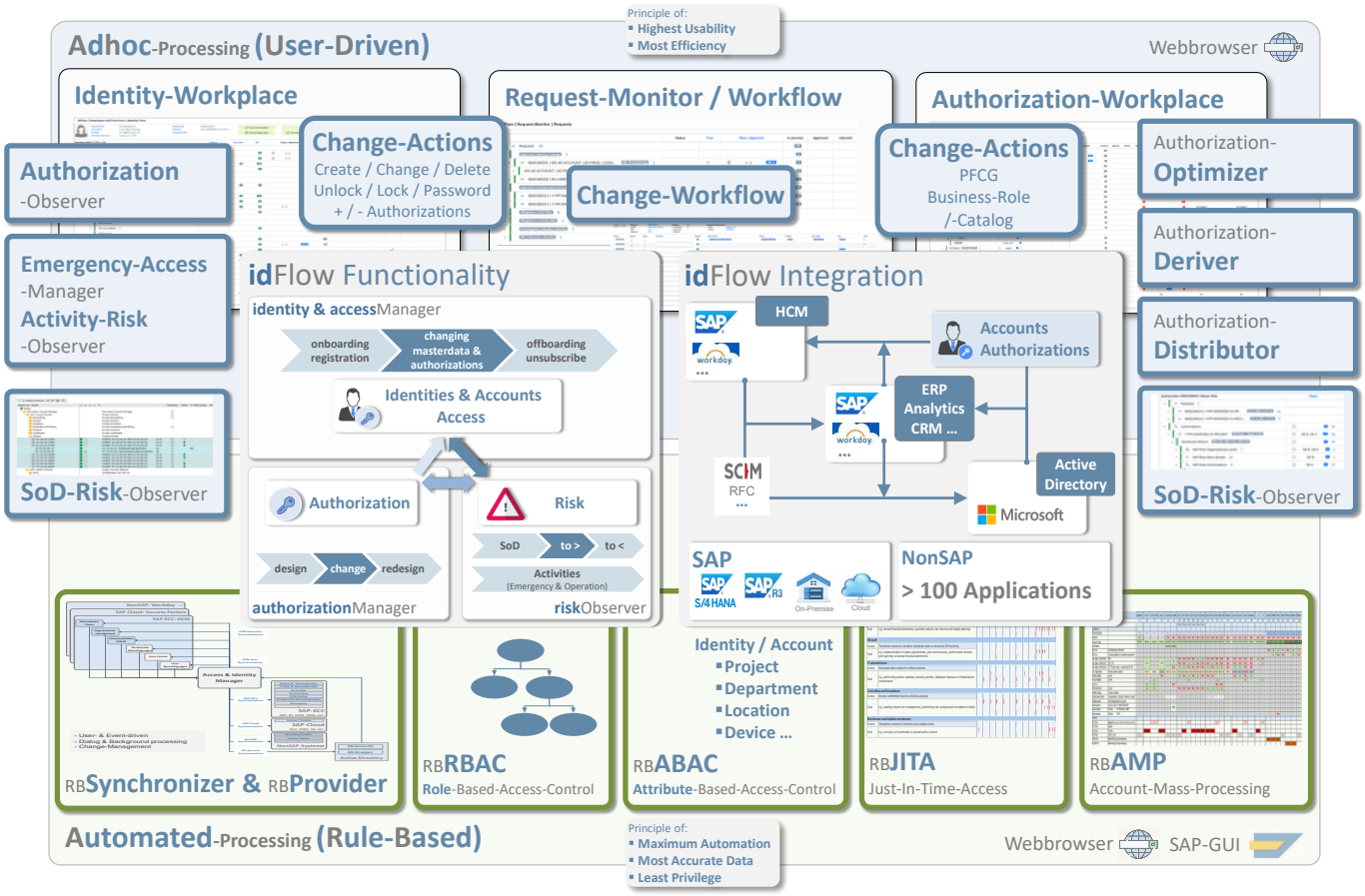
1.C Hauptfunktionen



1.D Integration SAP & NonSAP



1.E Business-Functions / Applications



Adhoc-Processing (User-Driven)

Identity-Workplace	
Authorization-Observer	zu wenige / zu viele Berechtigungen?
emergency access Manager	Emergency-Authorization-Provisionierung
Activity-Risk-Observer	Analyse von kritischen Aktivitäten
SoD-Risk-Observer	zu viele Berechtigungen? (→ Revision, etc.)
Authorization-Workplace	
Authorization-**Optimizer**	+ / - Transaktionen/Applikationen (genutzt / ungenutzt)
Authorization-**Deriver**	+ / - / **change**: Org.-Level der Kunden-Organisationseinheiten
Authorization-**Distributor**	'Verteilung der Authorization-Elemente in der Systemlandschaft
SoD-Risk-Observer	zu viele Berechtigungen? (→ Revision, etc.)

Automated Processing (Rule-Based)

Synchronizer & Provider	Account-/ & Authorization-Data-Flow (create, change, delete, provide)
Role-Based-Access-Control	Berechtigungen basierend auf vordefinierten Rollen
Attribute-Based-Access-Control	Berechtigungen basierend auf einer Kombination von Attributen
Just-In-Time-Access	Berechtigungen die nur in einem bestimmten Zeitfenster nötig sind
Account-Mass-Processing	Subtraktive Massnahmen wie Löschung, Sperrung, Abgrenzung, etc.

Principle of Highest-Usability

- Die Applikationen stehen den verschiedenen Anwendergruppen via **Webbrowser** zur Verfügung.
- Die Funktionalitäten verfolgen den „All-in-one"-Ansatz und reagieren **dynamisch** auf die jeweilige Anwendergruppen (Berechtigungen & Customizing).

Principle of Most Efficiency

- Die User-Interaktionen lösen „Actions" aus. Diese sind sehr flexibel konfigurierbar und können selbst automatisch passende Folgeaktivitäten auslösen. Daraus resultiert eine erhebliche Reduktion der Arbeitsschritte und des Aufwands.

Principle of Maximum Automation

- Prozesse, die einer beschreibbaren **Regel** folgen, können auch **automatisiert** werden!
- Customizing-Entscheidungstabellen bilden das entsprechende **Regelwerk** ab.

Principle of Most Accurate Data

- Die notwendigen **Datenflüsse** werden in Customizing-**Entscheidungstabellen** abgebildet.
- Event-Recognition sorgt für proaktive und reaktive **Datensynchronisierung**.

Principle of Least Privilege

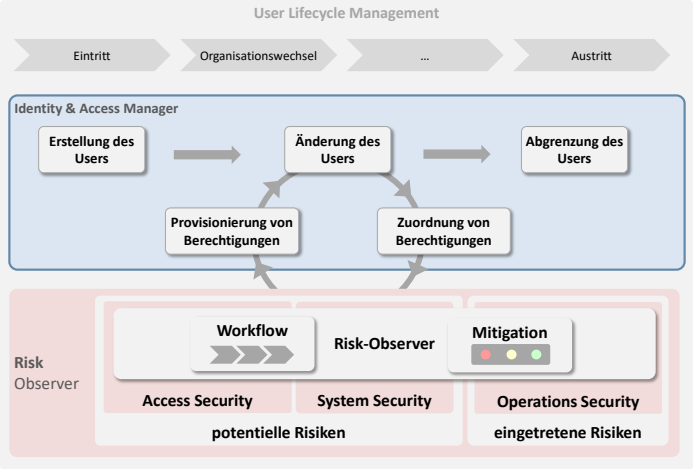
- Rule-Based-**Just-In-Time-Access** ermöglicht die automatische Provisionierung/Deprovisionierung von Berechtigungen die der Anwender nur zu bestimmten Zeitpunkten / Zeitfenstern benötigt.
- Rule-Based-**Account-Mass-Processing** ist das Gegenstück zu den additiven Funktionen wie Identity-Creator etc. Die typischen Aufgaben sind die subtraktiven Massnahmen wie Löschung, Sperrung, Abgrenzung, etc.

1.F Komponenten

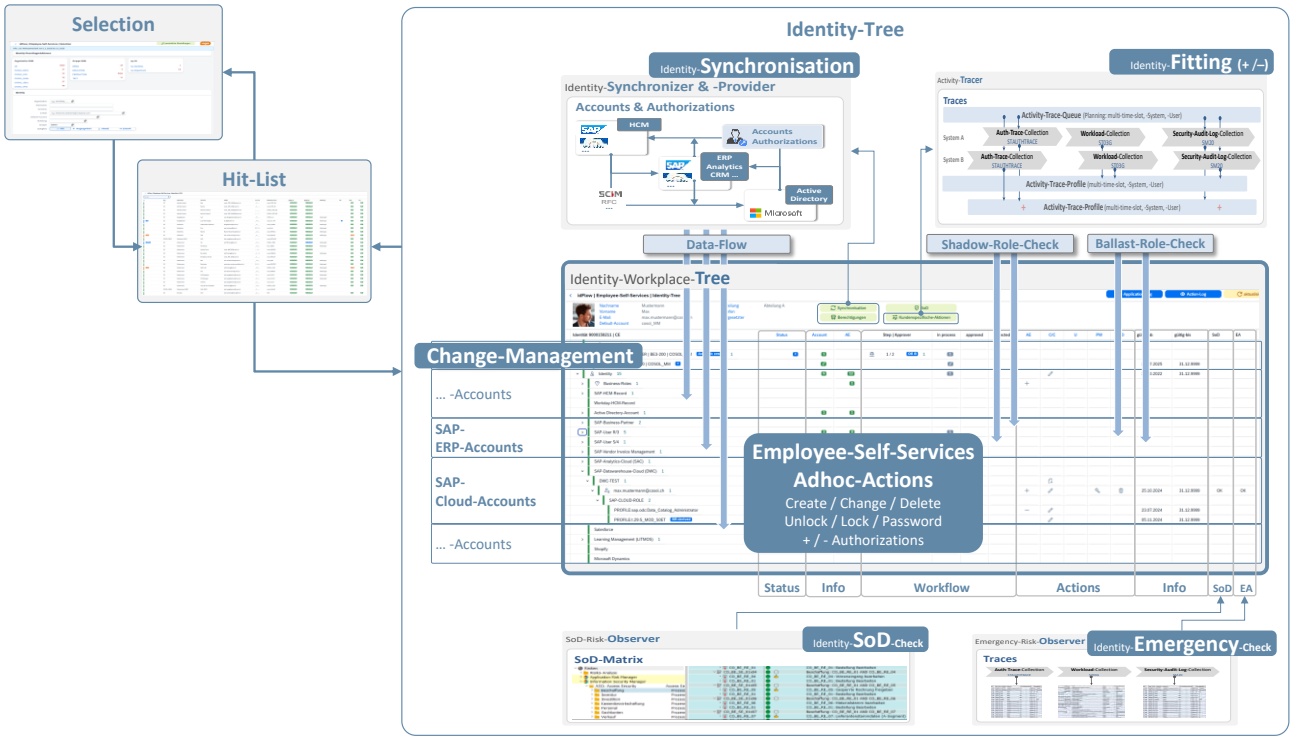
identity & access Manager	
Catalog	Verwaltung aller Identities & Accounts
Workplaces	Adhoc-Processing & Mass-Processing
Synchronizer	Account-Data-Flow (auto-create, -change)
Provider	Authorization-Provisioning
Identity-Assigner	Analyse (Duplikate, Fehler) und Zuweisung von Accounts zu Identities
SoD-Risk-Observer	zu viele Berechtigungen? (-> Revision, etc.)
Authorization-Observer	zu wenige / zu viele Berechtigungen?
Identity-Creator	Multi-/Massen-Erzeugung von Identitäten, Accounts und Berechtigungen
RBJITA	Rule-Based-Just-In-Time-Access
RBAMP	Rule-Based-Account-Mass-Processing
authorizationManager	
Catalog	Verwaltung aller Authorization-Elements
Workplaces	Customer-, Employee-, Administrator-Services
Business-Roles	Kombination verschiedener Authorization-Elements & Destinationen
SoD-Risk-Observer	zu viele Berechtigungen? (-> Revision, etc.)
Optimizer	+ / - : Transaktionen/Applikationen (genutzte / ungenutzte)
Deriver	+ / - / change: Org.-Level der Kunden-Organisationseinheiten
Distributor	Verteilung der Authorization-Elements in der Systemlandschaft
emergency access Manager	
Emergency-Role-Provider	Emergeny-Authorization-Provisionierung
Activity-Risk-Observer	Analyse von kritischen Actvities
licenseManager	
Calculator	Kalkulation & Optimierung der Lizenzen
coreFunctions	
Requests & Workflow	Request, E-Mail, Prozess-Schritte, Verantwortlichkeiten
Risk-Observer	Access-, System-, Operations-Security
Activity-Tracer	Authorization-Trace, Workload, Security-Audit-Log, etc.
Data-Collector	Daten-Sammlung und zentrale Speicherung in allen Systemen

2. identity & accessManager [IAM]

2.A Big-Picture

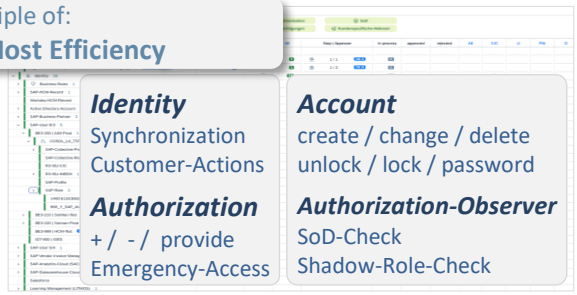


2.B Identity-Workplace (Webbrowser / Fiori)



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 Synchronizer & Provider

Event-Recognition

Die **Event-Recognition** ist in die Core-Funktion **Data-Collection** integriert und ermöglicht es **Zustandsänderungen** in allen integrierten Systemen zu **erkennen** und definierte **Aktionen** auszulösen

So kann z.B. eine Namensänderung im HCM-System oder eine E-Mail-Änderung im Active-Directory automatisch erkannt und in alle relevanten Systeme verteilt werden.

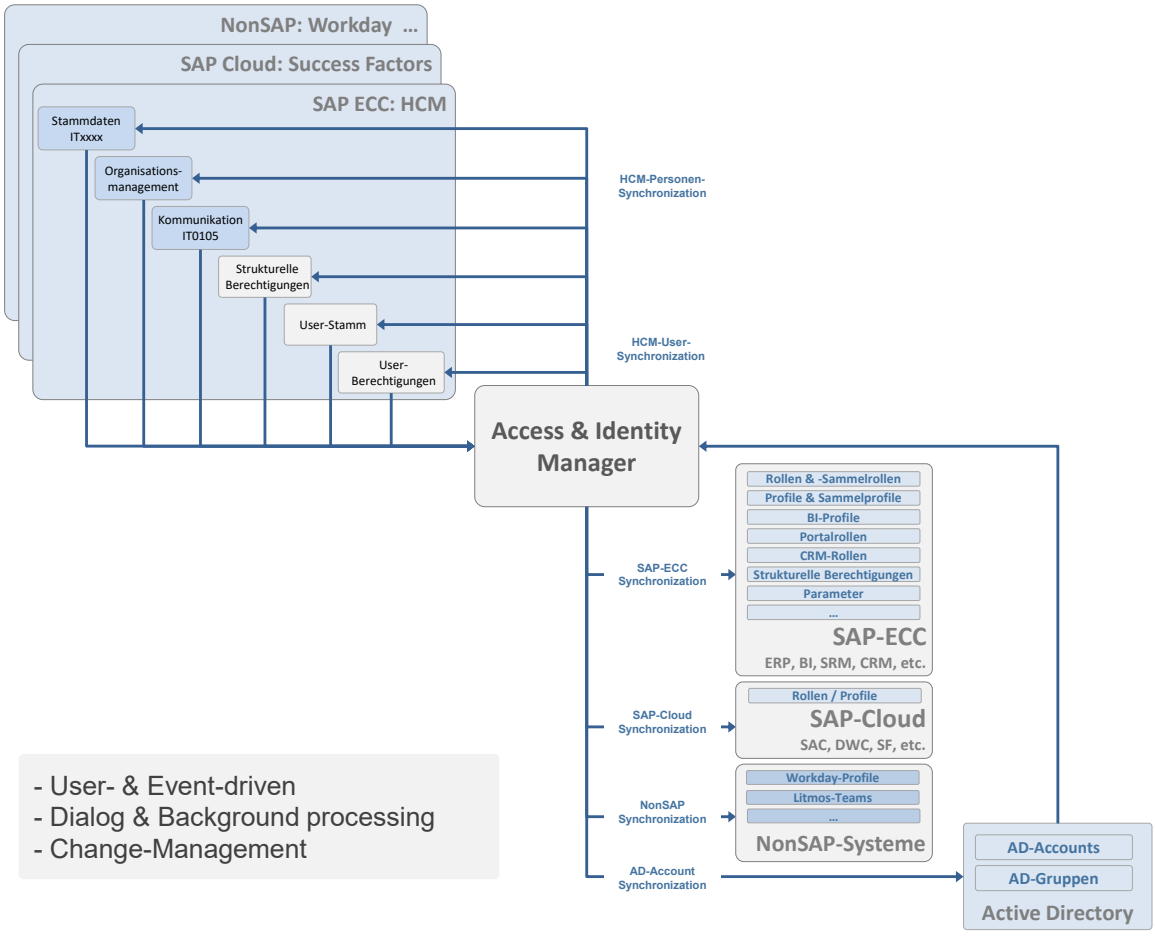
Data-Flow

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.

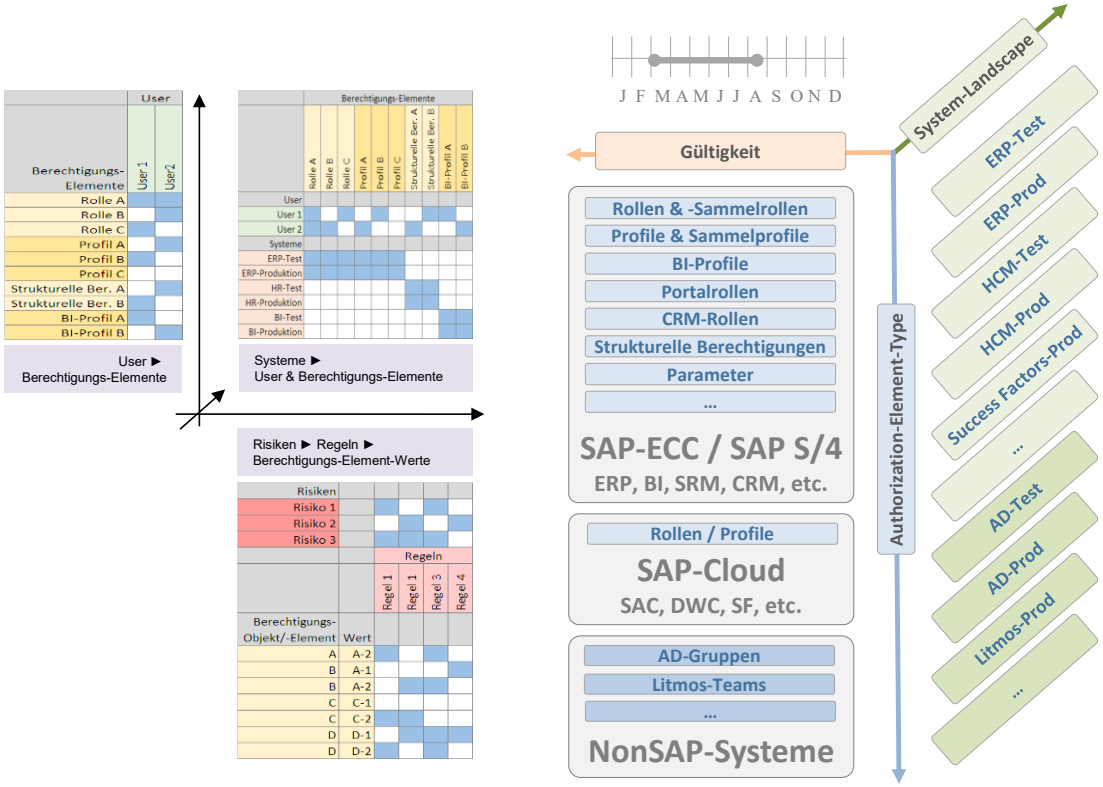
- Die Identity dient als «Container» zusammengehörender Accounts.
  (z.B. R/3-User, S/4HANA-User, SAP-Cloud-user, AD-Account, Person, NonSAP-Accounts, …)
- Jedes System und jedes Attribut können sowohl Input als auch Output sein.
- Regeln werden als Entscheidungstabellen abgebildet.
- Kundenspezifische 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 Mitarbeiter externe Mitarbeiter, technische Accounts, …)



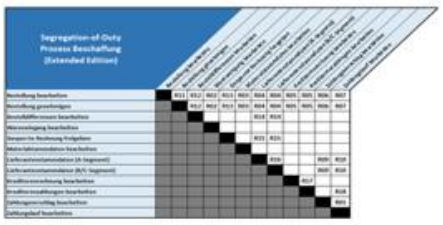
2.D SoD-Risk-Observer

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.

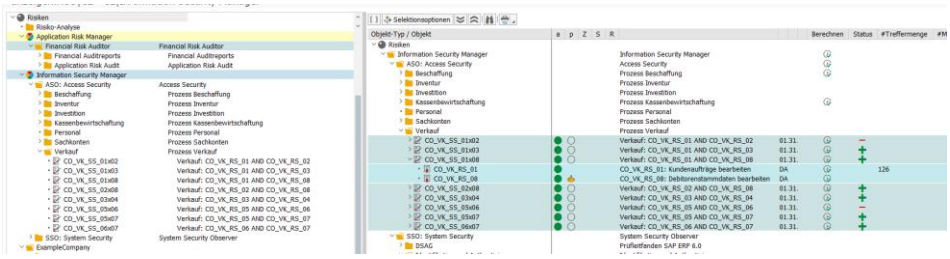
- Prüfgegenstand → **1 Identity**
- Grundlagen → DSAG, SAP-GRC, Revisionshäuser
- Konzept & Doku → Excel
- Customizing → Risk-Organizer
  → Rule-Organizer
- Execution → Dialog & Background
- Protokoll → SoD-Analysis
- Mitigation → Formular & Workflow



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.E Authorization-Observer (Identity-Authorizations)

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:

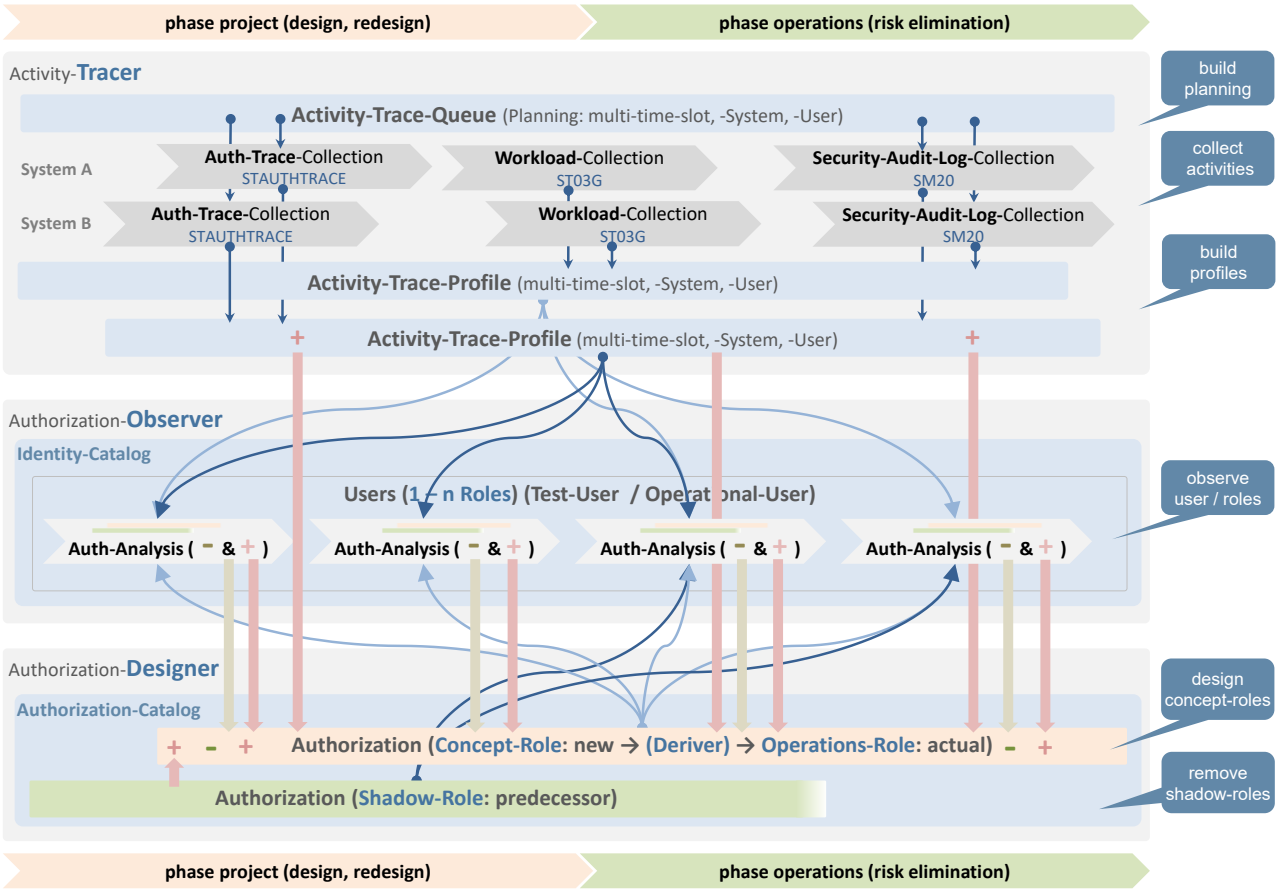
- „**zu wenig** Berechtigungen“ -> **Operations-Risk-Eliminator**
  -> Anwender kann aufgrund fehlender Berechtigungen nicht arbeiten!
- „**zu viele** Berechtigungen“ -> **Authorization-Optimizer**
  -> SoD-Risiken etc. entstehen aufgrund nicht notwendiger Elemente in den Berechtigungen

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 **Ballast-Roles** -> **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.

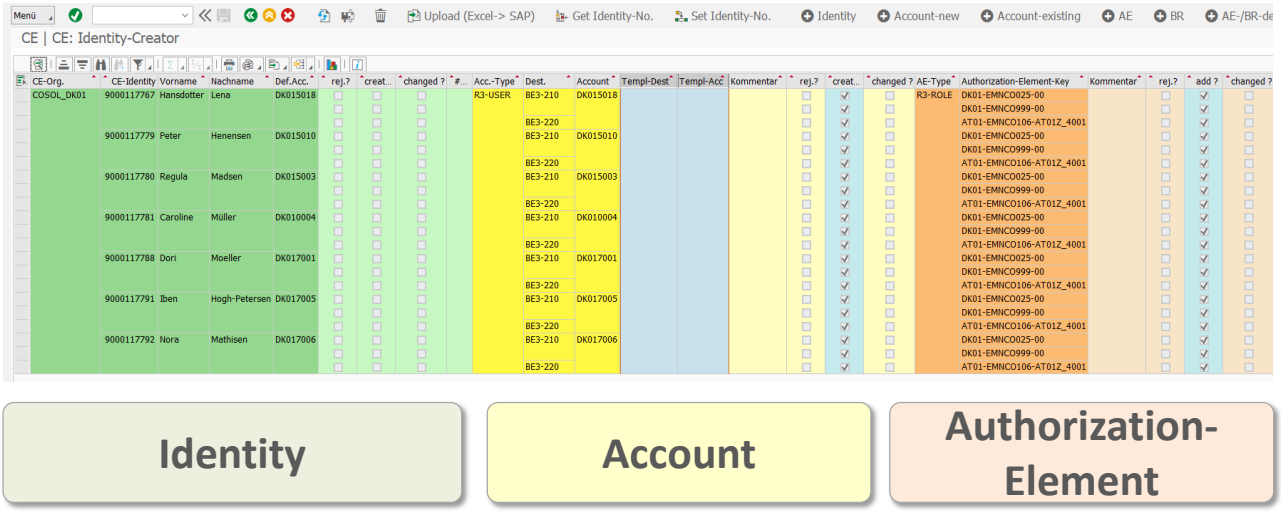
Um die Operation-Risks in der Produktivphase zu eliminieren, **behält der Anwender seine bisherigen Rollen,** solange **bis diese „Shadow-Roles“ nicht mehr notwendig** sind.



2.F Identity-Creator

Der Identity-Creator:

- ist ein einfach zu bedienendes User-Interface für die Beantragung/Durchführung folgender Actions:
  - create Identities
  - create Accounts
  - add Authorization-Elements
- unterstützt sowohl:
  - Massenupload via Excel-Template
  - Massenverarbeitung im Dialog für:
    - n Identities
    - n Accounts
    - n Authorization-Elements



2.G RBJITA

Rule-Based-Just-In-Time-Access ermöglicht die automatische Provisionierung/Deprovisionierung von Berechtigungen die der Anwender nur zu bestimmten Zeitpunkten / Zeitfenstern benötigt.

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

Beispiele:

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

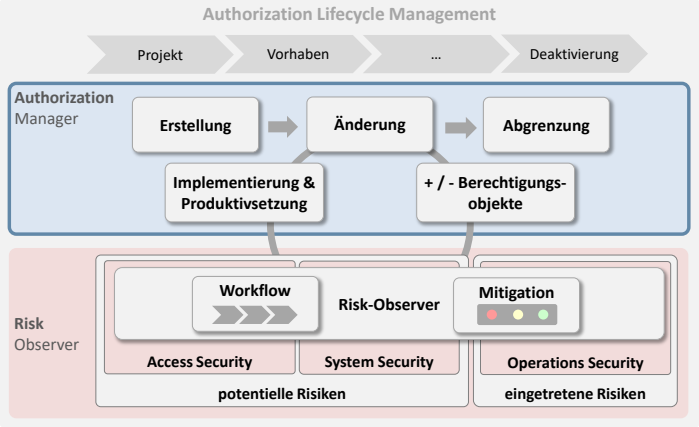
Rule-Based-Account-Mass-Processing ist das Gegenstück zu den additiven Funktionen wie Identity-Creator etc.
Die typischen Aufgaben sind die **subtraktiven Massnahmen** wie **Löschung**, **Sperrung**, **Abgrenzung**, etc.

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

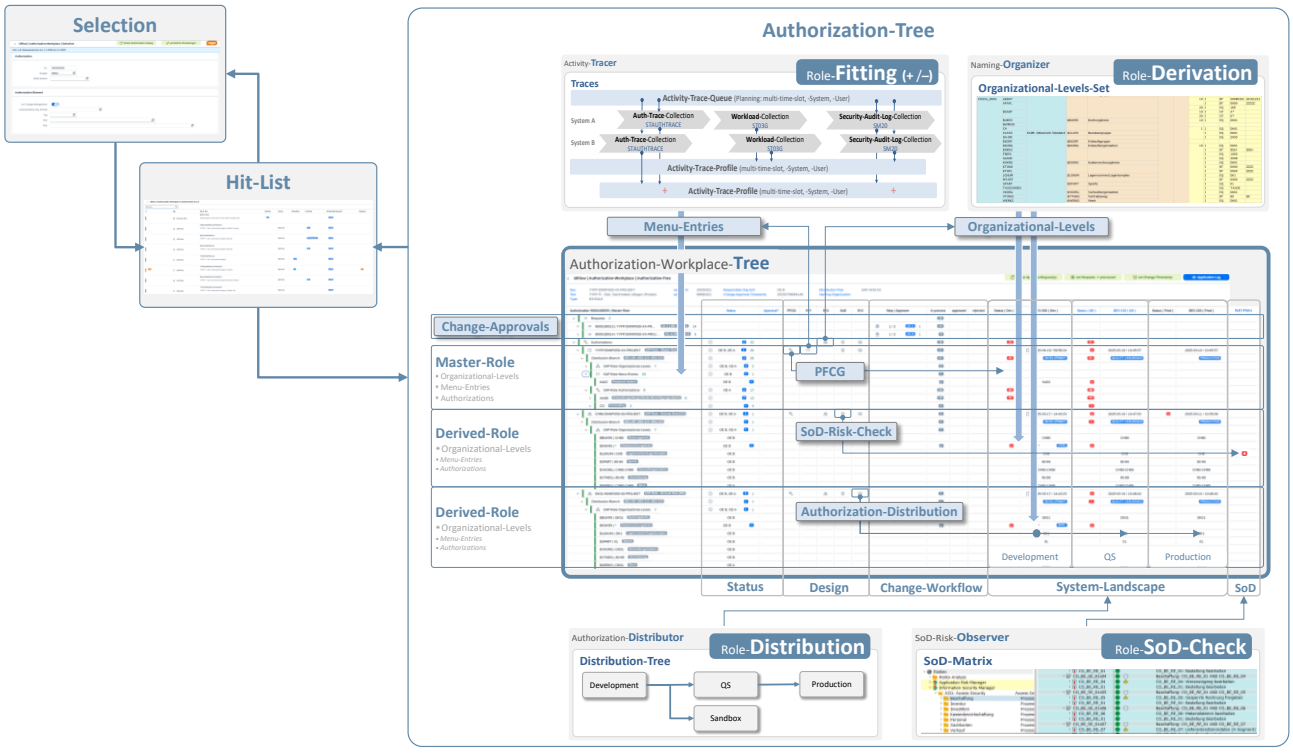
		Blacklist	Int.C-O	Int.C-O-ATZ	ext.C.O	Int.GPH	Int.GP0	Int.F.1	Int.F.2	Int.F.3	Int.F.4	Int.F.5	Int.F.6	Int.A.2	Int.A.3	Int.B.2	Int.B.3	Int.Norm	ext.A.3	ext.A.4	ext.B	ext.Norm	A	B	VIM.A	VIM.B	VIM.C	VIM.0	BUPA.A	BUPA.B	BUPA.0
Priorität		5	10	11	12	13	14	21A	21B	21C	21D	21E	21F	24	25	26	27	29	31	32	35	39	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		

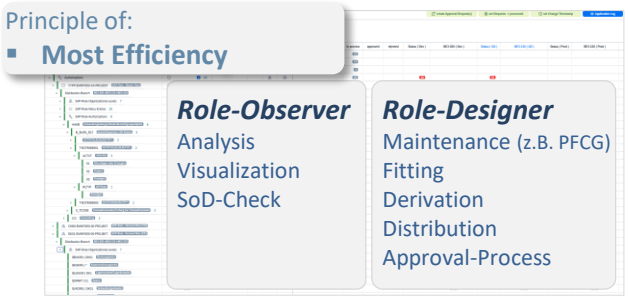
3. authorizationManager [AM]

3.A Big-Picture



3.B Authorization-Workplace (Webbrowser / Fiori)





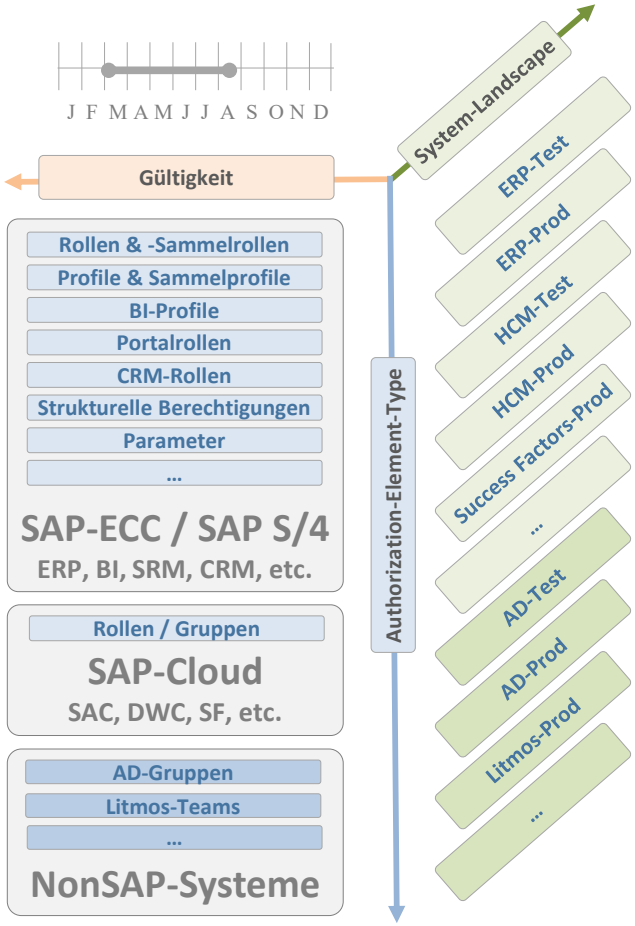
3.C Business-Roles

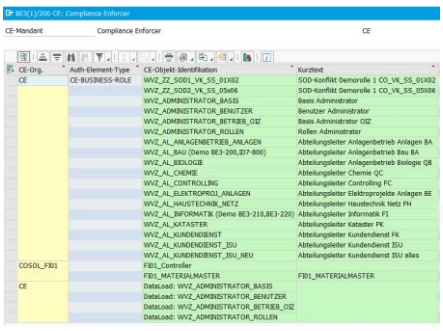
Die Business-Role dient dazu, zusammengehörende Applikations-Berechtigungen der ganzen Systemlandschaft (SAP und NonSAP) zu verknüpfen und gemeinsam zu verarbeiten.

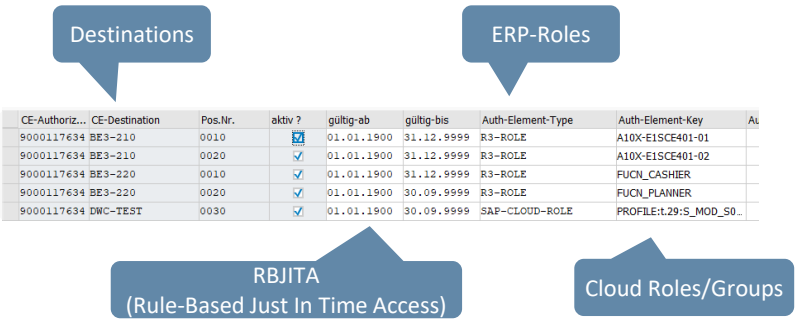
So kann z.B. für die Planstelle „Controller“ eine(1) Business-Role definiert werden, welche alle notwendigen Berechtigungen auf allen notwendigen Zielsysteme umfasst.
→ Durch die Zuweisung einer(1) Business-Role zu einer Identity werden alle notwendigen Application-Roles gleichzeitig und in einem Arbeitsschritt provisioniert.

Die Business-Rolle ermöglicht:

- die Kombination verschiedener Authorization-Elemente
- die Definition verschiedener Ziel-Destinationen
- die Festlegung der zeitlichen Gültigkeit





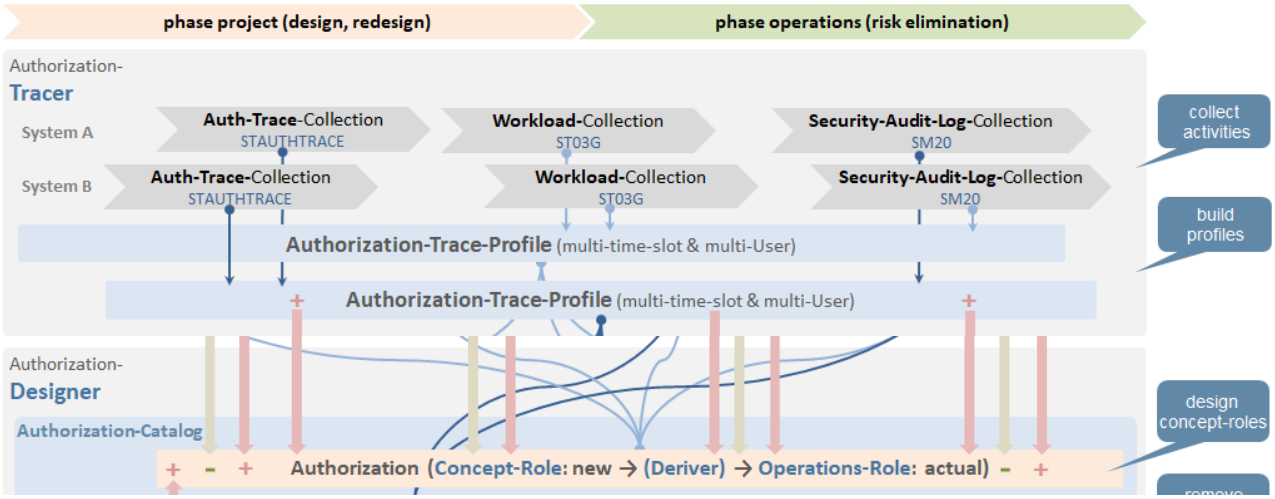


3.D Authorization-Optimizer

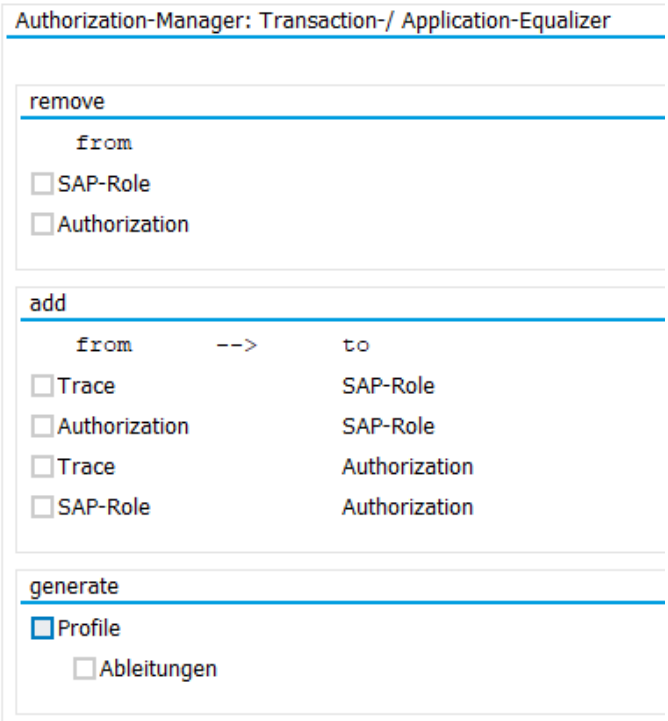
Der Optimizer stellt während des Designs / Redesigns einer Berechtigung sicher, dass die **notwendigen Transaktionen/Applikationen erkannt und in die Berechtigung integriert** werden.

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.

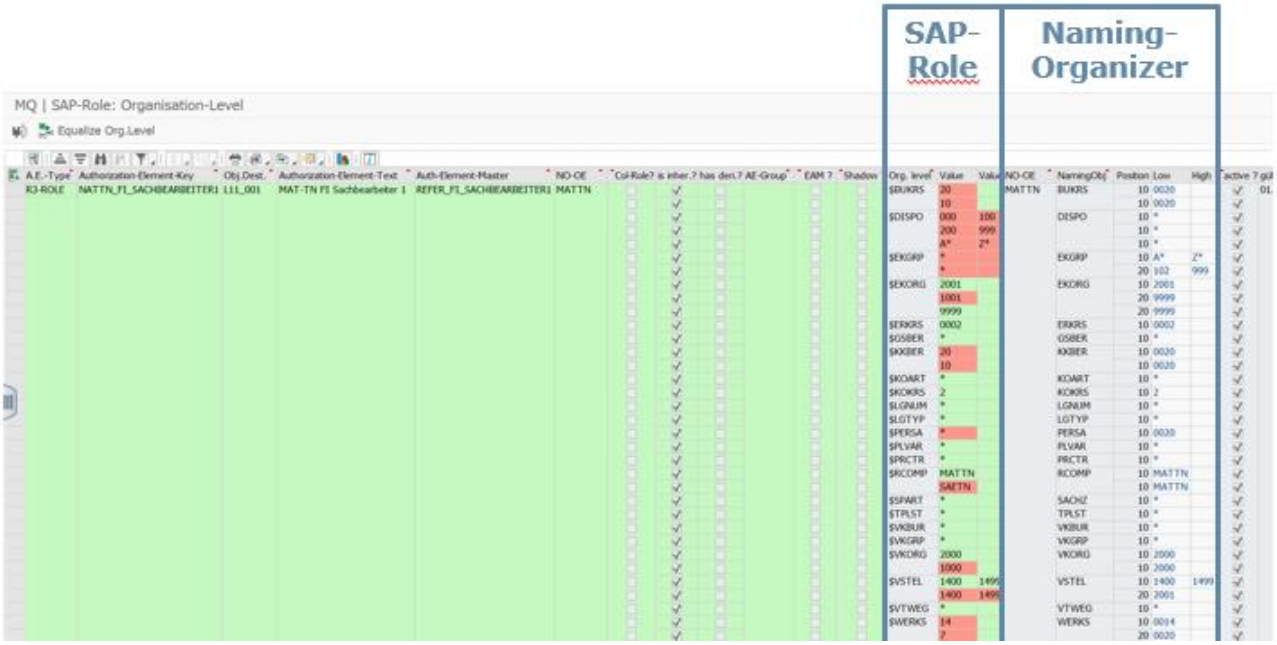


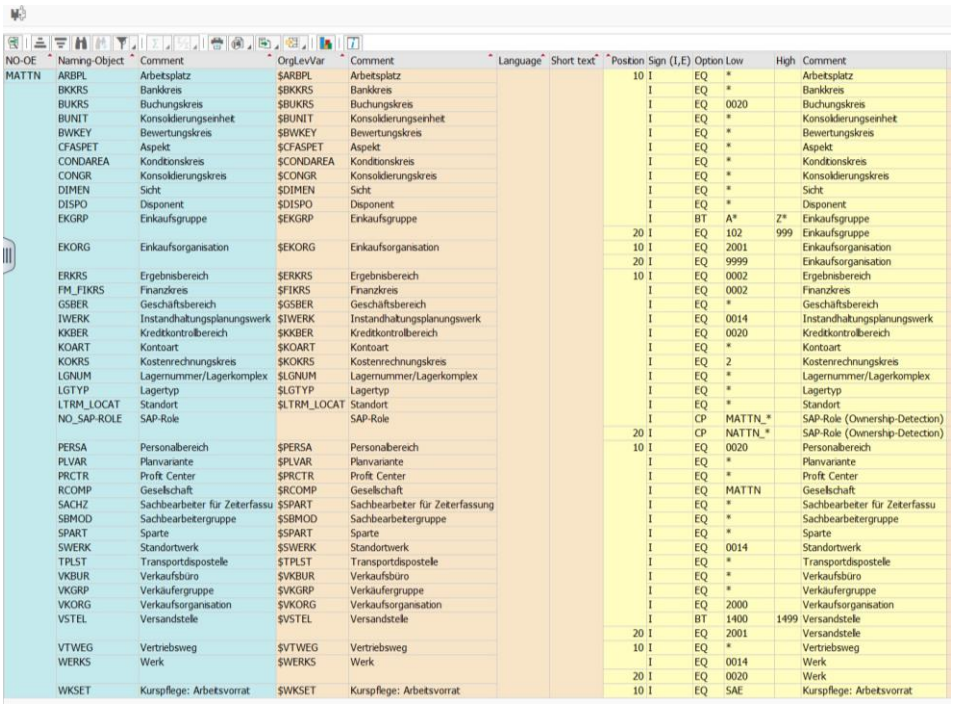
3.E Authorization-Deriver

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.



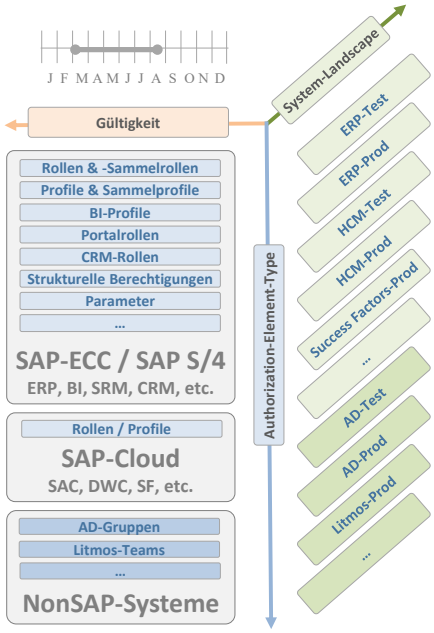


NO-OE	Naming-Object	Comment	OrgLevVar	Comment	Language	Short text	Position	Sign (I,E)	Option	Low	High	Comment
MATTN	ARBPL	Arbeitsplatz	$ARBPL	Arbeitsplatz			10	I	EQ	*		Arbeitsplatz
	BKKRS	Bankkreis	$BKKRS	Bankkreis				I	EQ	*		Bankkreis
	BUKRS	Buchungskreis	$BUKRS	Buchungskreis				I	EQ	0020		Buchungskreis
	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

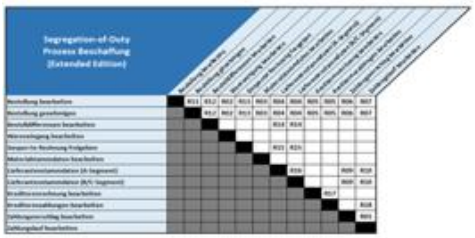
3.F SoD-Risk-Observer (Authorization)

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.

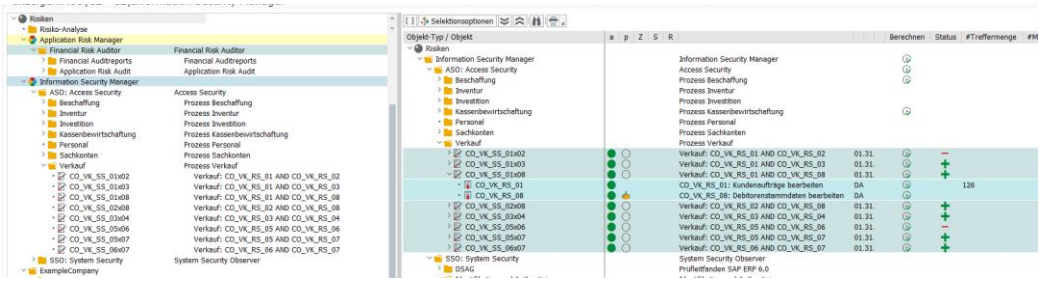
- Prüfgegenstand → **1 Authorization**
- Grundlagen → DSAG, SAP-GRC, Revisionshäuser
- Konzept & Doku → Excel
- Customizing → Risk-Organizer
  → Rule-Organizer
- Execution → Dialog & Background
- Protokoll → SoD-Analysis
- Mitigation → Formular & Workflow



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



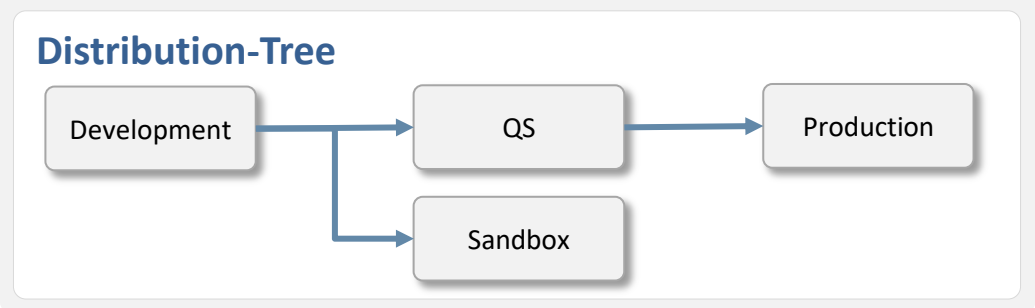
Die Regeln und Risiken sind transparent im System implementiert. Sie können ebenso kundenspezifisch erweitert wie auch gezielt deaktiviert werden.



3.G Authorization-Distributor

Der Authorization-Distributor ermöglicht die Verteilung der Authorizations (SAP-Rollen) in der Systemlandschaft. Der Verteilungspfad wird im Distribution-Tree festgelegt.

Beispiel:



Die eigentliche Verteilung kann sowohl via SAP-Transportsystem oder direkt via RFC-Verteilung erfolgen

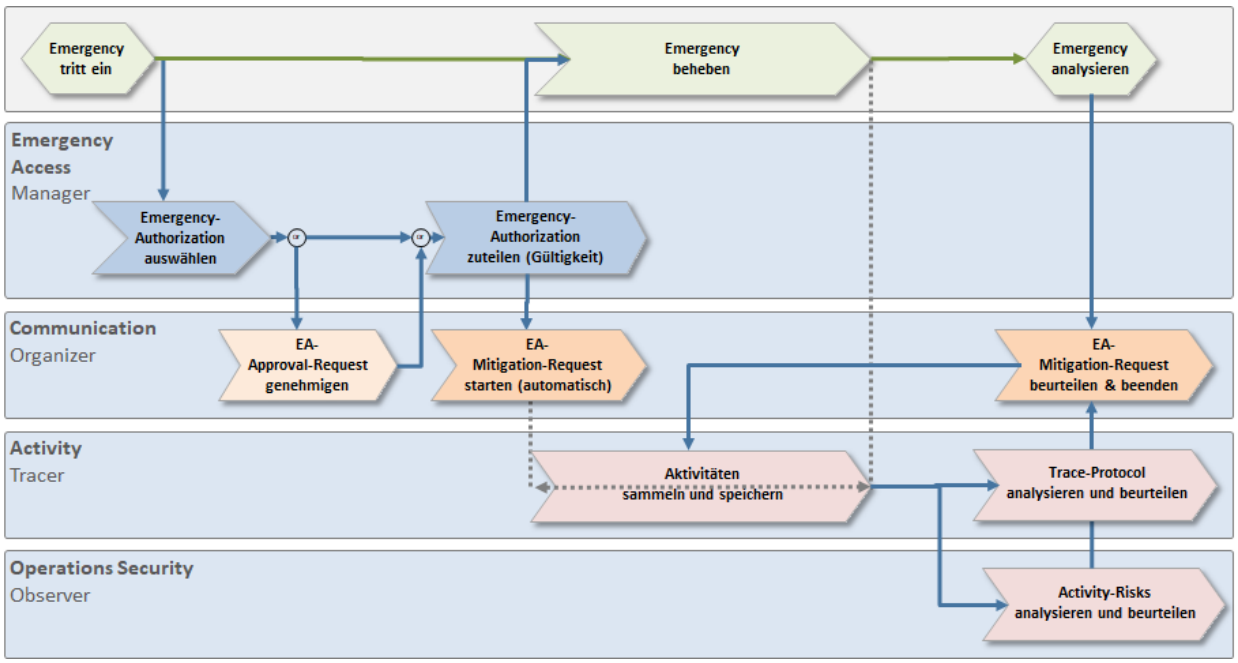
Die Verteilung kann auch einen Request mit entsprechendem Workflow auslösen.

4. emergency accessManager [EAM]

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 Prozess

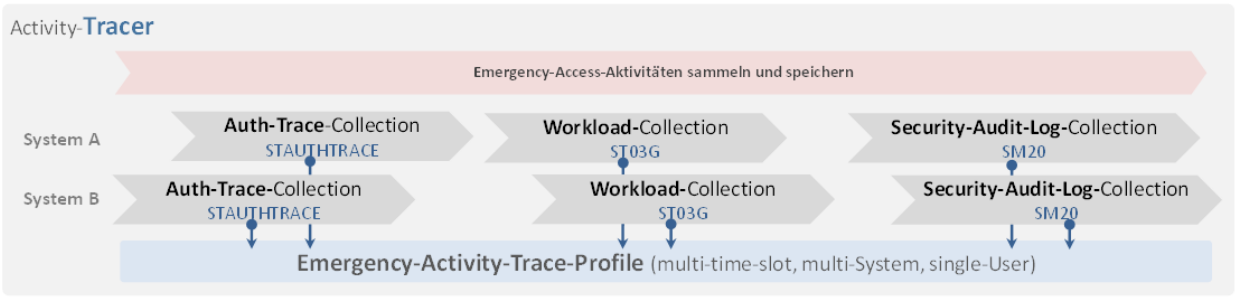


4.B Request-Workplace

Request mit / ohne Freigabeworkflow

- Self-Service (Webbrowser / Fiori)
- Admin-Services (Webbrowser / Fiori oder SAP GUI)

4.C Activity-Risk-Observer



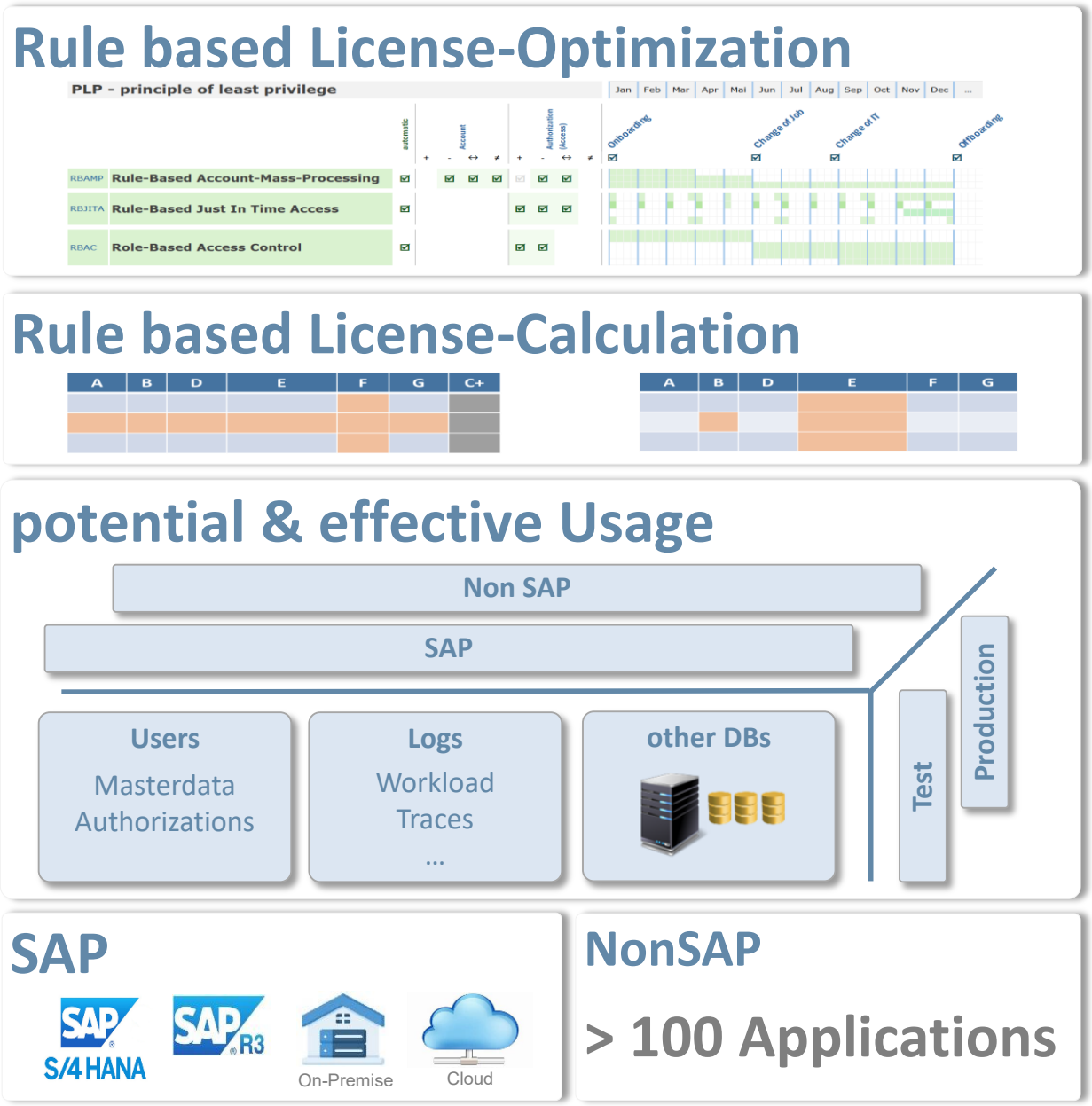
- manuelle Überwachung der Activities

- definierte Risiken
- automatisierte Überwachung der Activities

5. licenseManager [LM]

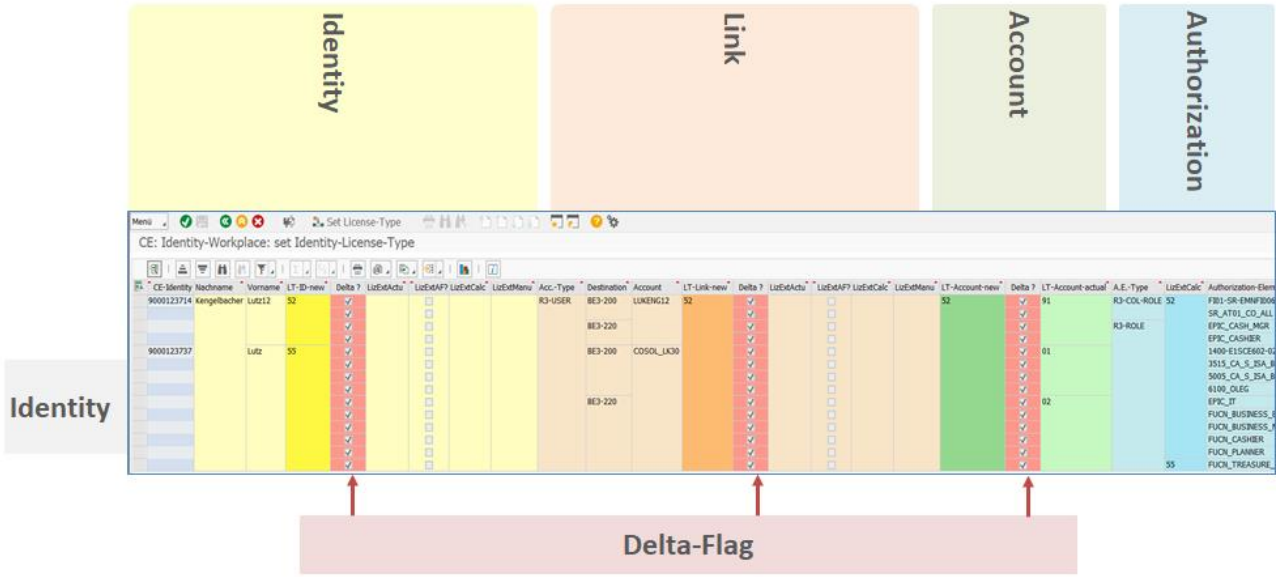
Der licenseManger **kalkuliert** pro Identity & Account den **anzuwendenden Lizenztyp**.

5.A Big-Picture



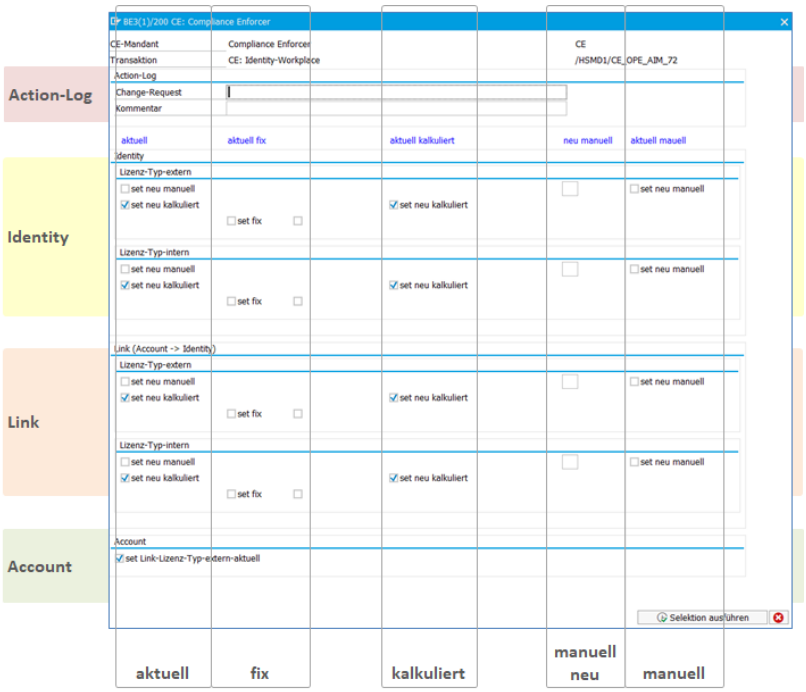
5.B License-Calculator

- 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.



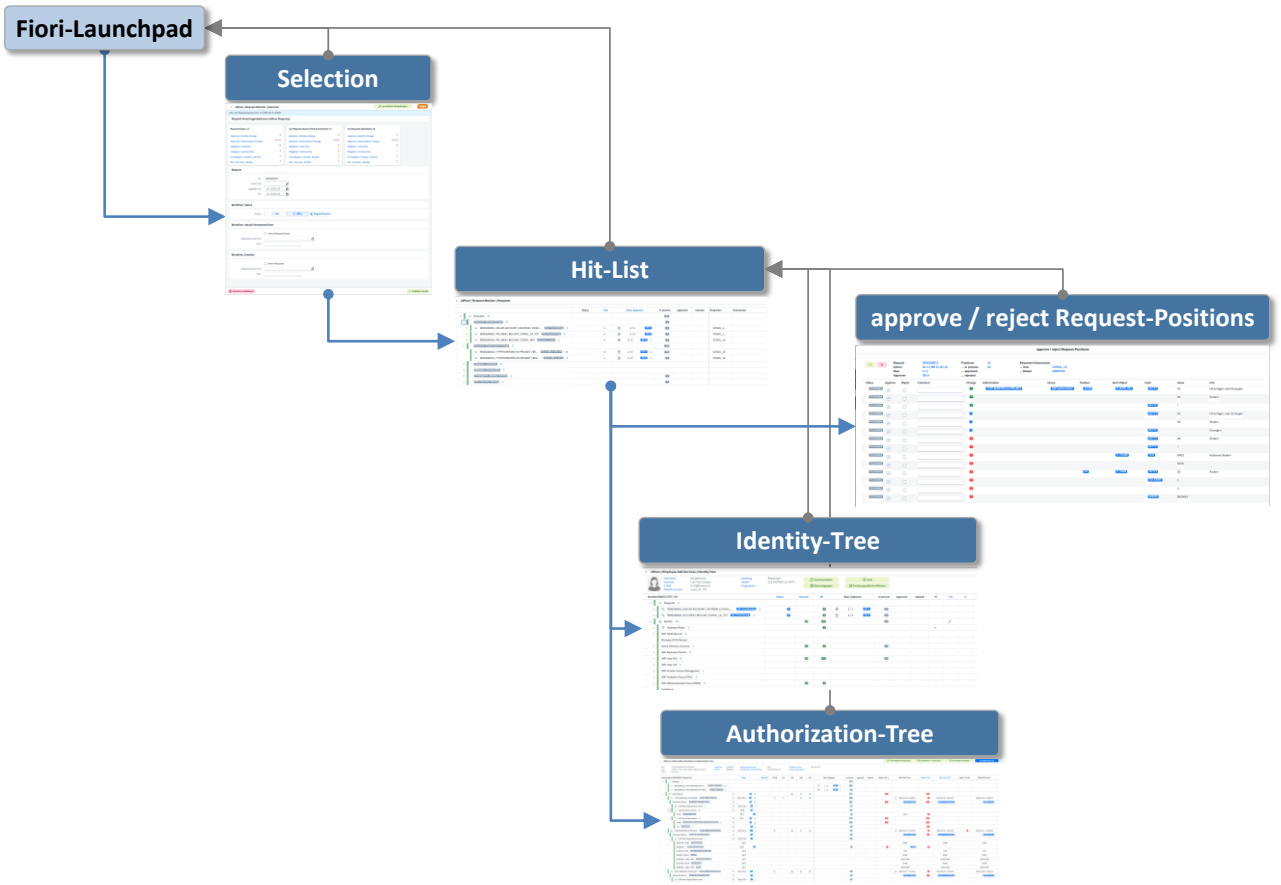
5.C License-Update

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



6. Requests & Workflow

6.A Request-Monitor (Webbrowser / Fiori)



6.B Workflow-Customizing (Decision-Table)

Fokus		Standard	Standard	Standard	Standard	Standard	Standard	Standard	Standard	Standard	Standard	Standard	Standard	Standard	div.	Standard	Ident-WP RBAMP	BACKGROUND RBAMP	CC		HR	BW	CRM	CRM	SolMan
Bemerkung			Default ohne Request			Default mit Request	Workflow		WF-ok -> exec Action							Sync: auto-create	Masse	Masse		weitere					Sync: auto-create BUPA
Step			Action & exec	Action & exec	Action & exec	request & exec	Action	ok	nok	exec	exec	exec	exec	exec	exec	Sync	Action	Action	Action	Action	Action	Action	Action	Action	Action & exec
Anzahl Checks			1	1	1	2	3	2	2	2	2	2	2	3		4	4	4	6	5	5	5	5	5	5
Conditions																									
CE-Action				Z_840_REAS Z_AE_VALID	Z_840_CHG	ACC_CREATE ACC_RE_CRE ACC_PW_SET ACC_LOCK ACC_UNLOCK ACC_DELETE Z_AE_PROV	ACC_CREATE ACC_RE_CRE ACC_PW_SET ACC_LOCK ACC_UNLOCK ACC_DELETE Z_AE_PROV	Z_WF_OK	Z_WF_NOK	ACC_CREATE ACC_RE_CRE	ACC_PW_SET	ACC_UNLOCK	ACC_LOCK ACC_DELETE Z_AE_PROV	Z_840_VALI (RBAMP)	ACC_CREATE	ACC_CREATE ACC_RE_CRE ACC_PW_SET ACC_LOCK ACC_UNLOCK ACC_DELETE Z_AE_PROV Z_840_VALI	ACC_DELETE Z_840_VALI	ACC_CREATE ACC_RE_CRE ACC_PW_SET ACC_LOCK ACC_UNLOCK ACC_DELETE Z_AE_PROV	ACC_CREATE ACC_RE_CRE ACC_PW_SET ACC_LOCK ACC_UNLOCK ACC_DELETE Z_AE_PROV Z_840_VALI	ACC_CREATE ACC_RE_CRE ACC_PW_SET ACC_LOCK ACC_UNLOCK ACC_DELETE Z_AE_PROV	ACC_CREATE ACC_RE_CRE ACC_PW_SET ACC_LOCK ACC_UNLOCK ACC_DELETE Z_AE_PROV	ACC_CREATE ACC_RE_CRE ACC_PW_SET ACC_LOCK ACC_UNLOCK ACC_DELETE Z_AE_PROV	ACC_CREATE ACC_RE_CRE ACC_PW_SET ACC_LOCK ACC_UNLOCK ACC_DELETE Z_AE_PROV	ACC_CREATE ACC_RE_CRE
CE-Action-Trigger			Z_WF_OK	Z_WF_OK	Z_WF_OK	Z_WF_OK	Z_WF_OK	Z_WF_OK	Z_WF_OK	Z_WF_OK	Z_WF_OK	Z_WF_OK	Z_WF_OK	Z_WF_OK	Z_WF_OK	Z_WF_OK	Z_WF_OK	Z_WF_OK	Z_WF_OK	Z_WF_OK	Z_WF_OK	Z_WF_OK	Z_WF_OK	Z_WF_OK	Z_WF_OK
Destination							*									*	*	*	*	*	G+H*	G+3*	G*C*	G*C*	G+S*
CE-Organisation																			externe	weitere	interne	interne externe	interne	externe	
Task-Type																									
IDENT-WP	10													IDENT-WP			IDENT-WP								
IDENT-CREA	11																		IDENT-CREA	IDENT-CREA	IDENT-CREA	IDENT-CREA	IDENT-CREA	IDENT-CREA	
REQUEST-WP	12																		REQUEST-WP	REQUEST-WP	REQUEST-WP	REQUEST-WP	REQUEST-WP	REQUEST-WP	
SHORTCUT	13																		SHORTCUT	SHORTCUT	SHORTCUT	SHORTCUT	SHORTCUT	SHORTCUT	
SELF-SERV	14																								
IDENT-SYNC	16															IDENT-SYNC									IDENT-SYNC
RBAMP	16																	RBAMP							
BACKGROUND (Y / N)	17													BACKGROUND		BACKGROUND		Y							

Actions																									
ESB-CE-Action-Subset			SPACE	SPACE	SPACE	SPACE	SPACE	SPACE	SPACE	SPACE	SPACE	SPACE	SPACE	SPACE	SPACE	SPACE	SPACE	SPACE	SPACE	SPACE	SPACE	SPACE	SPACE	SPACE	SPACE
ESB-CE-Action-Position			**1000**	**1005**	**1005**	**1010**	**1020**	**1500**	**1505**	**1030**	**1032**	**1034**	**1036**	**1038**	**2020**	**2010**	**2012**	**2100**	**2110**	**2410**	**2510**	**2610**	**2620**	**2720**
X47-CE-Action			SPACE	SPACE	SPACE	SPACE	SPACE	SPACE	SPACE	SPACE	SPACE	SPACE	SPACE	SPACE	SPACE	SPACE	SPACE	SPACE	SPACE	SPACE	SPACE	SPACE	SPACE	SPACE	SPACE
X47-CE-Action-Pos.			100'000	204'000	105'000		440'000	760'000	760'000	634'000	630'000	620'000	600'000	603'000	134'000	440'000	100'000	440'000	440'000	440'000	440'000	440'000	440'000	440'000	100'000
X32-WF-Act.-Pos.							_ 100 _ 0									_ 100 _ 0		_ 100 _ 0	_ 100 _ 0	_ 100 _ 0	_ 100 _ 0	_ 100 _ 0	_ 100 _ 0	_ 100 _ 0	
WF-Responsible							**AIM-Admin**									**AIM-Admin**		**O-I**	**O-I**	**C-PS**	**BW-Admin**	**SAP-CRM**	**O-I**		
X47-CE-Action			↓ SPACE	↓ SPACE	↓ SPACE	↓ SPACE	↓ SPACE	↓ SPACE	↓ SPACE	↓ SPACE	↓ SPACE	↓ SPACE	↓ SPACE	↓ SPACE	↓ SPACE	↓ SPACE	↓ SPACE	↓ SPACE	↓ SPACE	↓ SPACE	↓ SPACE	↓ SPACE	↓ SPACE	↓ SPACE	↓ SPACE
X47-CE-Action-Pos.			↓ 100000	↓ 204000	↓ 105000	↓	↓ 440000	↓ 760000	↓ 760000	↓ 634000	↓ 630000	↓ 620000	↓ 600000	↓ 603000	↓ 134000	↓ 440000	↓ 100000	↓ 440000	↓ 440000	↓ 440000	↓ 440000	↓ 440000	↓ 440000	↓ 440000	↓ 100000
Request			no	no	no	no	yes	no	no	no	no	no	no	no	no	yes	no	yes	yes	yes	yes	yes	yes	yes	no
PopUp			no	yes	no	no	yes	yes	no	no	no	no	no	no	no	yes	no	yes	yes	yes	yes	yes	yes	yes	no
E-Mail			no	no	no	yes	yes	yes	yes	yes	yes	yes	no	no	yes	yes	no	yes	yes	yes	yes	yes	yes	yes	no
Requester						Requester	Requester	Requester	Requester							Requester		Requester	Requester	Requester	Requester	Requester	Requester		
Operator																									
Account						Account & PW				Account & PW	Account & PW	Account			Account & PW										
actual WF-Responsible								actual	actual																
next WF-Responsible							next									next		next	next	next	next	next	next		
SYNC			no	yes	yes	yes	no	no	no	1	no	no	no	1	1	no	no	no	no	no	no	no	no	no	no
AE-provide			no	yes	yes	yes	no	no	no	1	no	no	no	no	1	no	no	no	no	no	no	no	no	no	no
ESB-WF-Act.-Pos.							↓ _ 100 _ 0									↓ _ 100 _ 0		↓ _ 100 _ 0	↓ _ 100 _ 0	↓ _ 100 _ 0	↓ _ 100 _ 0	↓ _ 100 _ 0	↓ _ 100 _ 0	↓ _ 100 _ 0	
1-Step							X									X		X	X	X	X	X	X		
2-Step																									
ESB-WF-Resp.-Pos.																		--							
1-Step-Responsible							↓ AIM-Admin									↓ AIM-Admin		↓ O-I	↓ O-I	↓ C-PS	↓ BW-Admin	↓ SAP-CRM	↓ O-I		
ESB-WF-Resp.-Pos.																									
2-Step-Responsible																									

6.C Request-E-Mail

E-Mail als Request für 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 als 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

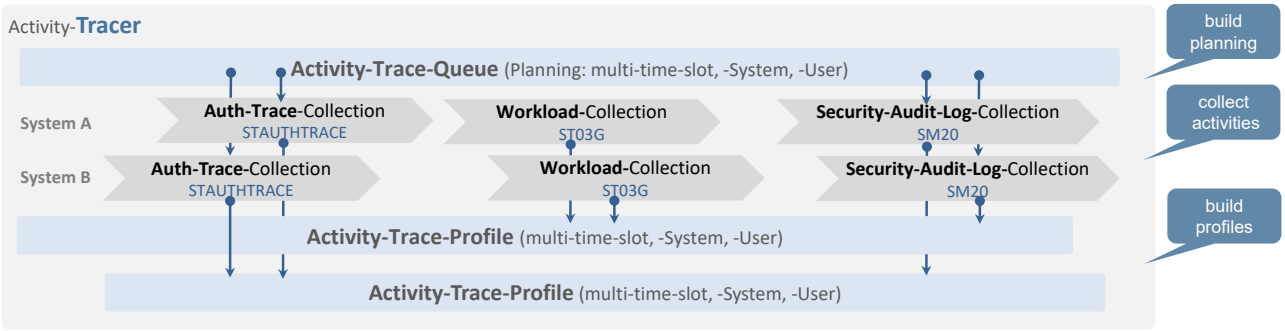
Action	ACC_CREATE
Account-Type	R3-USER
Destination	BE3-220
Account	COSOL_LK30
Password	Oa311469483!
Firstname	Lutz
Lastname	Kengelbacher
E-Mail	lutz30.keng@test.ch

7. Activity-Tracer

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.

7.A Trace -> Profile



7.B Struktur

- 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

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