



Identity and  
**Access Governance**  
for SAP® environments

# A Dynamic Access Governance Approach for Identities in SAP Systems

Lim Huck Hai  
Head of BDO RAS Asia Pacific  
[hlim@bdo.my](mailto:hlim@bdo.my)

Johan Hermans  
CEO  
[johan.hermans@csi-tools.com](mailto:johan.hermans@csi-tools.com)

# Access Governance in SAP environments

- is critical because SAP systems store and manipulate confidential and business-critical structured data
  
- Most organizations focus “only” on
  - Segregation of duties reporting
  - Structuring the user access request process

# Access Governance in SAP environments

- Is managing people's access to data using
  - users, enterprise roles, composite roles, single roles, transaction codes, authorizations, SU24 settings, operating company values, derived roles, security base line, critical access rights, segregation of duties
- By
  - corporate management, business management & subsidiaries, internal control, corporate IT, local IT, internal audit and external audit
- Taken into account the change drivers
  - roll-outs, upgrades, support tickets, new access rights, review access rights, new compliance rules, mergers & de-mergers
- And setting up the management processes which include ownership, communication channels & policies

# Access Governance in SAP environments

WHAT

WHO

WHERE

Enterprise Roles

Composite Roles

Single Roles

Transactions

User-ID

INTERNAL CONTROL

BUSINESS

IT

AUDIT

Internal

External

Compliance Rules | Security Baseline  
CAR & SoD

CHANGE

TRIGGERS

PMO

Upgrades & Roll Outs

Support

Tickets

Access Rights

New & Review

SoD reporting and enforcing Access Request  
Forms do not make up for Access Governance

# Access Governance in SAP environments

- Generic SOD reports gives an overview of the number of SoD's in an organization. It does not sufficiently help each different stakeholder.
- Information missing in most SoD reports:
  - who has almost access
  - which roles need to be removed
  - detailed comparison with previous runs
  - indicate which roles should be isolated from a composite one
  - which roles cause accumulation of access rights
  - ....

Our release 2014 applications will give you insight that goes beyond your dreams



# Find Errors in Roles, Rules & Assignments

## Insight at your fingertips

Result container info							Has Authorization	Has T-code	Executed T-code
UserID/Profil /									
	Logical System	Variant	Query Description	Query	Type	Sox Classification			
<input checked="" type="checkbox"/>	*	*	*	*	*	*			
USER002 (3 items)									
<input type="checkbox"/>	DEMO	<NA>	Maintain FI Posting Periods	ECC_FCLOSA	ARQ	SOX_H	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	DEMO	<NA>	Maintain Customizing FI	ECC_FCSTMA	AR	SOX_C	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	DEMO	<NA>	Maintain FI Posting Periods	FCLOSA	ARQ	SOX_H	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
USER004 (9 items)									
<input type="checkbox"/>	DEMO	<NA>	Maintain A/P Postings with Clearing	ECC_FAPPCA	ARQ	SOX_H	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	DEMO	<NA>	Maintain A/P Parked Documents	ECC_FAPPD7	AO	SOX_M	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	DEMO	<NA>	Maintain A/P Parked Documents Postings	ECC_FAPPPDA	ARQ	SOX_M	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	DEMO	<NA>	Maintain A/P Outgoing Payment Postings	ECC_FAPPPYA	ARQ	SOX_M	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	DEMO	<NA>	Maintain A/P Recurring Documents	ECC_FAPPRDA	ARQ	SOX_C	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	DEMO	<NA>	Maintain FI Posting Periods	ECC_FCLOSA	ARQ	SOX_H	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	DEMO	<NA>	Maintain Customizing FI	ECC_FCSTMA	AR	SOX_C	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	DEMO	<NA>	Maintain A/P Manual Postings	FAPMPA	ARQ	SOX_M	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Profile (causing)									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXXXAPMPA									
FXXXX									

**Inconsistencies in rules or roles!**

Since user has access to the data but cannot start the audited transaction code

**User has access but does not use it**

According to the principle "need-to-know" & "need-to-have" these access rights should be removed



# SoD Reports

track which roles can be removed

<input type="checkbox"/>	USER002	Jeroen Jacobs	Dialog user	Active user	Not locked			
	Profile (causing)	Role (causing)	A	T	E	Role (assigned)	c	E
<input checked="" type="checkbox"/>	*	*	*	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	*	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	SXXXXSM30D	S99SXXXXSM30D	0/1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	S99Z-XXXX-SYSTADM	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	SXXXXTABLA	S99SXXXXTABLA	0/1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	S99Z-XXXX-SYSTADM	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	SXXXXTMSA	S99SXXXXTMSA	1/1	<input type="checkbox"/>	<input type="checkbox"/>	S99Z-XXXX-SYSTADM	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Profile (causing)	Tcode (causing)	E	Profile (causing)				
<input checked="" type="checkbox"/>	*	*	<input checked="" type="checkbox"/>					
	SXXXXSM30D	SM30	<input type="checkbox"/>	SXXXXSM30D				
	SXXXXTABLA	SM30	<input type="checkbox"/>	SXXXXTABLA				
	SXXXXSM30D	SM31	<input type="checkbox"/>	SXXXXSM30D				
	SXXXXTMSA	SM31	<input type="checkbox"/>	SXXXXTMSA				
	Profile (causing)	Object	Authorization	Role (causing)				
<input checked="" type="checkbox"/>	*	*	*	*				
	SXXXXTMSA	S_TABU_DIS	SXXXXTMSA00	S99SXXXXTMSA				

Roles causing  
the access

how

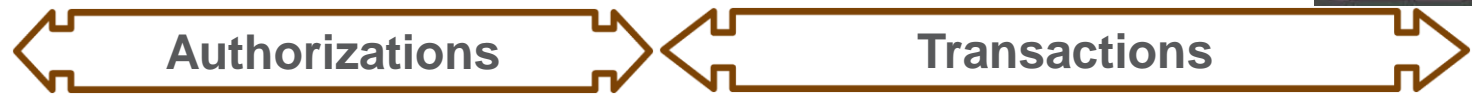
not  
used





assigned  
through

composite role  
used



# Multiple Layered Analyses Gives Insight




Authorizations	Questions			
Authorizations		T-Code		
Authorizations			Menu	
Authorizations				Executed
	Result 1			
		Result 2		

**With CSI Authorization Auditor's layered analysis of causing info you WILL find inconsistencies in Rules, Roles and User-Role Assignments**

# Analysis Cockpit With Drill Down

to monitor your own KPI, KPR, projects, objectives, ...


**Analysis cockpit**

Statistics
Authorizations

+ User counts

+ Composite role counts

+ Single role counts

- Authorization information

Roles with authorizations:	93		Manual authorizations count:	10		0,5%
Total authorizations count:	1980	100,0%	Inactive authorizations count:	1		0,1%
Standard authorizations count:	1561	78,8%	Organizational levels count:	271		13,7%
Maintained authorizations count:	408	20,6%	Overridden org. levels count:	0		0,0%
Modified authorizations count:	0	0,0%	Corrupt authorizations:	0		
Roles with highest authorization between 0 and 25:	93		Roles with highest authorization between 51 and 75:	0		
Roles with highest authorization between 26 and 50:	0		Roles with highest authorization between 76 and 99:	0		

+ Role assign information

+ New concept

+ Query counts

+ Support information

Observe. Think. Act.

Export
Print
Reset layout
Cancel

Export Access
Export Excel
Export PDF
Export XML

# Compare SOD Results !

- In depth analysis of what has been changed

**Result container compare**

Compare SoD result container

Log. System: DUMMY, Type: AGR, Download date (min): 5/07/2013 0:00, Run date (max): 30/09/2013 8:51, STAD date (current): 12/09/2013

SoD run: SoD run 30/09/13 : Users having authorization or t-code

compare with

Archive: Audit run on 02/08/2013 16:28 for users on authorizations an

Archive SoD run: SoD run 02/08/2013: Users having authorization or t-code

		Sod conflict	Variant	Description	Reason code	Definition	Expression	Logical system	Exe #	Exe Δ	User	Role	Total #	Total Δ	Total #	Total Δ	Total #	Total Δ
		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
		CST_T_U1_0003	<NA>	Customizing FI	B_S_C	Uni (U)	Qa	DUMMY	0	0	59	-23	0	59	-23			
		FIN_MD_B2_C_0010	<NA>	Vendor M.D. (Fin.) AND Vendor M.D. (Purch.)	C_F2-	Bi (B2)	Qa AND Qb	DUMMY	0	0	5	-6	0	5	-6			
		FIN_MT_B2_0001	<NA>	FI Posting Periods (Open/Close) AND A/P Manual	A_F1+	Bi (B2)	Qa AND Qb	DUMMY	0	0	4	-10	0	4	-10			
		FIN_MT_B2_0002	<NA>	FI Posting Periods AND A/P Postings with Clearing	A_F1+	Bi (B2)	Qa AND Qb	DUMMY	0	0	4	-10	0	4	-10			
		FIN_MT_B2_0003	<NA>	FI Posting Periods AND A/P Parked Doc. Postings	A_F1+	Bi (B2)	Qa AND Qb	DUMMY	0	0	4	-10	0	4	-10			
		FIN_MT_B2_0004	<NA>	FI Posting Periods AND A/P Outgoing Payment Postings	A_F4+	Bi (B2)	Qa AND Qb	DUMMY	0	0	4	-10	0	4	-10			
		FIN_MT_B2_0005	<NA>	FI Posting Periods AND A/P Recurring Doc.	A_F1+	Bi (B2)	Qa AND Qb	DUMMY	0	0	4	-10	0	4	-10			
		FIN TT B2 C 0008	<NA>	A/P Payment Run AND A/P Proposal Run	C_F3-	Pi (P2)	Qa AND Qb	DUMMY	0	0	4	-6	0	4	-6			

# What is the trend?

## Dashboards of # periods



Observe. Think. Act.

# Role Content is Deviating from Documentation

## Systems can have millions of authorization lines

Update role authorizations											
Roles Overview Updates											
Drag a column header here to group by that column.											
<input type="checkbox"/>	<input type="checkbox"/>	Role name	Description (SAP)	Status	Object	Field	Authorizatio	Values	Codification		Information
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	*	*	*	A	A	A	*	*	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input type="checkbox"/>	S99FXXXARCHMA	F-AR: Maintain A/R Credit Management	<input type="checkbox"/> Maintained	F_BKPF_BUK	BUKRS	00	HELLO	*	<input type="checkbox"/>	<input checked="" type="checkbox"/> Authorizations need to be updated
<input checked="" type="checkbox"/>	<input type="checkbox"/>	S99FXXXARCHMA	F-AR: Maintain A/R Credit Management	<input type="checkbox"/> Maintained	F_KNB1_ANA	BUKRS	00	HELLO	*	<input type="checkbox"/>	<input checked="" type="checkbox"/> Authorizations need to be updated
<input checked="" type="checkbox"/>	<input type="checkbox"/>	WEBFXXXAPSPA	Demo Web	<input type="checkbox"/> Maintained	F_LFA1_BUK	BUKRS	00	!	*	<input type="checkbox"/>	<input checked="" type="checkbox"/> Authorizations need to be updated
<input checked="" type="checkbox"/>	<input type="checkbox"/>	WEBFUXXXAPSPA	Demo Web USA	<input type="checkbox"/> Maintained	F_LFA1_BEK	BRGRU	00	LAX, LOS, NEW, OAK, PAL, SAN, TEY	CUSTOMER, NEW, OAK, PAL, SAN, TEY	<input type="checkbox"/>	<input checked="" type="checkbox"/> Authorizations need to be updated
<input checked="" type="checkbox"/>	<input type="checkbox"/>	WEBFUCIAPSPA	Demo Web Los Angeles	<input type="checkbox"/> Maintained	F_LFA1_BEK	BRGRU	00	LAX, LOS	CUSTOMER	<input type="checkbox"/>	<input checked="" type="checkbox"/> Authorizations need to be updated
<input checked="" type="checkbox"/>	<input type="checkbox"/>	NRBFUXXXAPSPA	NRB demo USA	<input type="checkbox"/> Maintained	F_LFA1_BEK	BRGRU	00	LOS, NEW, NRB, OAK, PAL, SAN, TEY	CUSTOMER, NEW, OAK, PAL, SAN, TEY	<input type="checkbox"/>	<input checked="" type="checkbox"/> Authorizations need to be updated
<input checked="" type="checkbox"/>	<input type="checkbox"/>	NRBFUCIAPSPA	NRB demo Los Angeles	<input type="checkbox"/> Maintained	F_LFA1_BEK	BRGRU	00	HIHI, LOS, NRB	CUSTOMER	<input type="checkbox"/>	<input checked="" type="checkbox"/> Authorizations need to be updated
<input checked="" type="checkbox"/>	<input type="checkbox"/>	NRBFXXXAPSPA	NRB demo Belgium	<input type="checkbox"/> Maintained	F_LFA1_BUK	BUKRS	00	3333	3200	<input type="checkbox"/>	<input checked="" type="checkbox"/> Authorizations need to be updated
<input checked="" type="checkbox"/>	<input type="checkbox"/>	CLAFUNXXAPSPA	Demo 8 Aug New York	<input type="checkbox"/> Maintained	F_LFA1_BUK	BUKRS	00	1111	0100	<input type="checkbox"/>	<input checked="" type="checkbox"/> Authorizations need to be updated
<input checked="" type="checkbox"/>	<input type="checkbox"/>	CLAFUCXXAPSPA	Demo 8 Aug California	<input type="checkbox"/> Maintained	F_LFA1_BEK	BRGRU	00	CLA, OAK, PAL, SAN, TEY	CUSTOMER, NEW, OAK, PAL, SAN, TEY	<input type="checkbox"/>	<input checked="" type="checkbox"/> Authorizations need to be updated
<input checked="" type="checkbox"/>	<input type="checkbox"/>	CLAFUCIAPSPA	Demo 8 Aug Los Angeles	<input type="checkbox"/> Maintained	F_LFA1_BEK	BRGRU	00	CLA	CUSTOMER	<input type="checkbox"/>	<input checked="" type="checkbox"/> Authorizations need to be updated
<input checked="" type="checkbox"/>	<input type="checkbox"/>	AAAFUCXXAPSPA	Demo IIA California	<input type="checkbox"/> Maintained	F_LFA1_BEK	BRGRU	00	LOS, OAK, PAL, SAN, TEY	CUSTOMER, NEW, OAK, PAL, SAN, TEY	<input type="checkbox"/>	<input checked="" type="checkbox"/> Authorizations need to be updated
<input checked="" type="checkbox"/>	<input type="checkbox"/>	AAAFUCIAPSPA	Demo IIA Los Angeles	<input type="checkbox"/> Maintained	F_LFA1_BEK	BRGRU	00	LOS, XXX	CUSTOMER	<input type="checkbox"/>	<input checked="" type="checkbox"/> Authorizations need to be updated
<input checked="" type="checkbox"/>	<input type="checkbox"/>	BBBFUXXXAPSPA	Demo 12-24 USA	<input type="checkbox"/> Maintained	F_LFA1_BEK	BRGRU	00	FLOR, JEF, LOS, OAK, PAL, SAN, TEY	CUSTOMER, NEW, OAK, PAL, SAN, TEY	<input type="checkbox"/>	<input checked="" type="checkbox"/> Authorizations need to be updated
<input checked="" type="checkbox"/>	<input type="checkbox"/>	BBBFUCXXAPSPA	Demo 12-24 California	<input type="checkbox"/> Maintained	F_LFA1_BEK	BRGRU	00	LOS, OAK, PAL, SAN, TEY	CUSTOMER, NEW, OAK, PAL, SAN, TEY	<input type="checkbox"/>	<input checked="" type="checkbox"/> Authorizations need to be updated
<input checked="" type="checkbox"/>	<input type="checkbox"/>	BBBFUCIAPSPA	Demo 12-24 Los Angeles	<input type="checkbox"/> Maintained	F_LFA1_BEK	BRGRU	00	LOS	CUSTOMER	<input type="checkbox"/>	<input checked="" type="checkbox"/> Authorizations need to be updated
<input checked="" type="checkbox"/>	<input type="checkbox"/>	MOLFUXXXAPSPA	Demo May 10 USA	<input type="checkbox"/> Maintained	F_LFA1_BEK	BRGRU	00	LOS, NEW, OAK, PAL, SAN, TEY	CUSTOMER, NEW, OAK, PAL, SAN, TEY	<input type="checkbox"/>	<input checked="" type="checkbox"/> Authorizations need to be updated
<input checked="" type="checkbox"/>	<input type="checkbox"/>	MOLFUCIAPSPA	Demo May 10 Los Angeles	<input type="checkbox"/> Maintained	F_LFA1_BEK	BRGRU	00	LOS	CUSTOMER	<input type="checkbox"/>	<input checked="" type="checkbox"/> Authorizations need to be updated
<input checked="" type="checkbox"/>	<input type="checkbox"/>	STEFUXXXAPSPA	Demo USA	<input type="checkbox"/> Maintained	F_LFA1_BEK	BRGRU	00	LOS, NEW, OAK, PAL, SAN, TEY	CUSTOMER, NEW, OAK, PAL, SAN, TEY	<input type="checkbox"/>	<input checked="" type="checkbox"/> Authorizations need to be updated
<input checked="" type="checkbox"/>	<input type="checkbox"/>	STEFUCIAPSPA	Demo Los Angeles	<input type="checkbox"/> Maintained	F_LFA1_BEK	BRGRU	00	LOS, STE	CUSTOMER	<input type="checkbox"/>	<input checked="" type="checkbox"/> Authorizations need to be updated
<input checked="" type="checkbox"/>	<input type="checkbox"/>	AAAFUXXXAPSPA	Demo IIA USA	<input type="checkbox"/> Maintained	F_LFA1_BEK	BRGRU	00	FLOR, JEF, LOS, OAK, PAL, SAN, TEY	CUSTOMER, NEW, OAK, PAL, SAN, TEY	<input type="checkbox"/>	<input checked="" type="checkbox"/> Authorizations need to be updated

# Master – Derived Analysis

## Detect and Manage Role Deviation

- Deviations from template roles need to be detected easily

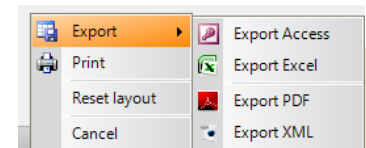
Create / maintain composite roles

Roles

Result

		Cre	Ne	Role name	Description (SAP)		Information					
			*	*	*		*					
				S99Z-UXXX-CFO	CFO USA		The role already exists					
				S99Z-UCSX-CFO	CFO San Diego		The role already exists					
				S99Z-UCPX-CFO	CFO Palo Alto		The role already exists					
		Cre	Ne	Cre	Ne	Re	De	De	Role name	Description (SAP)		Information
									NRBFUCFXAPSPA	NRB demo Palo Alto		The role already exists
									S99SXXXBASEA	S-GEN: Basic Authorizations for all users		This is a non derivable role
									S99SXXXSE16D	S-GEN: Display Tables (SE16)		The role is not found in the template composite
		Cre	Ne	Role name	Description (SAP)		Information					
				S99Z-UCOX-CFO	CFO Oakland		The role already exists					
				S99Z-UCLA-CFO	CFO Los Angeles		The role already exists					
				S99Z-NXXX-CFO	CFO Netherlands		The role already exists					
				S99Z-BXXX-CFO	CFO Belgium		The role already exists					

Observe. Think. Act.





# Reverse Engineering of all roles is now possible



- Use your SAP system to extract the needed info
  - *"Who can almost do" vs. "Who can do"*
  - *"Who can do" vs. "Who did"*
  - Extract organizational data from specific roles
  - Rebuild roles automatically based on templates

# Reports Transactions Usage

what users can do versus what users did



**Result container - Audit results**

Result container info

Drag a column header here to group by that column.

Logical System	Variant	Query	Query Description	Type	Sox Classification	Executed T-code	UserID/Role	User/Role description
DUMMY	<NA>	AAMMPA	Maintain Asset Manual Postings	ARQ		<input checked="" type="checkbox"/>	USER010	John Daby
DUMMY	<NA>	AAMSPA	Maintain Asset Sales, Donation, Scrappi...	ARQ		<input checked="" type="checkbox"/>	USER010	John Daby
DUMMY	<NA>	FAPIV2	Release purchase invoice via FB02 inste...	AR		<input checked="" type="checkbox"/>	USER010	John Daby
DUMMY	<NA>	FAPMPA	Maintain A/P Manual Postings	ARQ		<input checked="" type="checkbox"/>	USER010	John Daby
DUMMY	<NA>	FARMPA	Maintain A/R Manual Postings	ARQ		<input checked="" type="checkbox"/>	USER010	John Daby

Role (causing)	Tcode (causing)
S99FXXXXXARMPA	F-21
S99FXXXXXARMPA	F-42
S99FXXXXXARMPA	FB01
S99FXXXXXARMPA	FB02
S99FXXXXXARMPA	FB07
S99FXXXXXARMPA	FB08
S99FXXXXXARMPA	FB09
S99FXXXXXARMPA	FB11
S99FXXXXXARMPA	FB16N
S99FXXXXXARMPA	FBR1
S99FXXXXXARMPA	FBR2

Role (causing)	Object	Autho
S99FXXXXXARMPA	F_BKPF_BUK	00
S99FXXXXXARMPA	F_BKPF_KOA	00

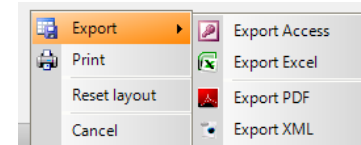
Logical System	Variant	Query	Query Description
DUMMY	<NA>	FARPCA	Maintain A/R Post
DUMMY	<NA>	FARPPA	Maintain A/R Post

**User transactions overview**

Drag a column header here to group by that column.

User ID	Full username	Type	Group	Lock status	Transaction	Missing
10	*	*	*	*	*	> 0
USER010	John Daby	Dialog user		Not locked	F-41	10
USER010	John Daby	Dialog user		Not locked	F-43	81
USER010	John Daby	Dialog user		Not locked	F-44	13
USER010	John Daby	Dialog user		Not locked	F.61	4
USER010	John Daby	Dialog user		Not locked	F110	22
USER010	John Daby	Dialog user		Not locked	FB01	220
USER010	John Daby	Dialog user		Not locked	FB03	3
USER010	John Daby	Dialog user		Not locked	FB05	151
USER010	John Daby	Dialog user		Not locked	FB08	17
USER010	John Daby	Dialog user		Not locked	FB10	1
USER010	John Daby	Dialog user		Not locked	FB12	2

Observe. Think. Act.

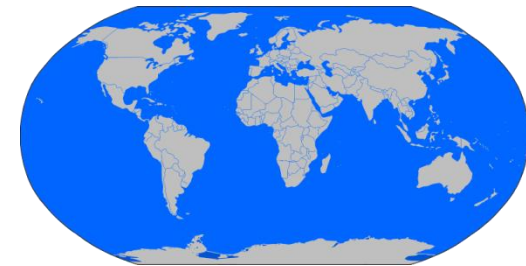


# Read role content of old roles & adjust

- Organizational perspective
  - Define Requirements on data level
  - Define Requirements on process level
- System perspective
  - Codify the WHAT requirements
  - Codify the WHERE requirements
  - Build all SAP roles automatically
- Assign roles using business language



**WHAT**



**WHERE**

Domains (\*)

XXXX - Master

- BXXX - Belgium
- NXXX - Netherlands
- UXXX - USA
  - UNXX - New York
  - UTXX - Texas
  - UCXX - California
    - Vendors
      - UCLA - Los Angeles
      - UCDX - Oakland
      - UCPX - Palo Alto
      - UCSX - San Diego
  - FXXX - France
  - YYYY - TaskWorkbook - Type 2

Workbook: Domain workbook

Drag a column header here to group by that column.

General				Rol		Authorization restrictions					
Modu	Field	Description	Objects	M	T	A	Master XXXX	Belgium BXXX	Netherlands NXXX	USA UXXX	New York UNXX
F	KTOPL	Chart of Accounts	*	*	*	*	*	EURO	EURO	EURO	EURX
F	BUKRS	Company Code	*	*	*	*	*	3200	3100	0100, 0101	EURX
F	BRGRU	Authorization group	F_LFA1_BEK	*	*	*	*	TBD	NET	ACC, LOS, NEW, OAK, PAL, SAN, TEX	NEW
K	KOKRS	Controlling Area	*	*	*	*	*	EURO	EURO	EURO	EURX
M	WERKS	Plant	*	*	*	*	*	3200	3100	0101, 0102, 0103	0101
M	EKORG	Purchasing Organization	*	*	*	*	*	3200	3100	0100	0100

Domains (\*)

- XXXX - Master
  - BXXX - Belgium
  - NXXX - Netherlands
  - UXXX - USA
    - UNXX - New York
    - UTXX - Texas
    - UCXX - California
      - UCLA - Los Angeles
      - UCOX - Oakland
      - UCPX - Palo Alto
      - UCSX - San Diego
  - FXXX - France
  - YYYY - TaskWorkbook - Type 2

Workbook: Domain w

Drag a column head

Modu	Field					Master XXXX	Belgium BXXX	Netherlands NXXX	USA UXXX	New Y UNXX
F	KTOPL	Chart of Accounts	*	*	*	*	EURO	EURO	EURO	EURC
F	BUKRS	Company Code	*	*	*	*	3200	3100	0100, 0101	.
F	BRGRU	Authorization group	F_LFA1_BEK	*	*	*	TBD	NET	ACQ, LOS, NEW, OAK, PAL, SAN, TEX	NEW
K	KOKRS	Controlling Area	*	*	*	*	EURO	EURO	EURO	EURC
M	WERKS	Plant	*	*	*	*	3200	3100	0101, 0102, 0103	0101
M	EKORG	Purchasing Organization	*	*	*	*	3200	3100	0100	0100
V	VKORG	Sales Organization	*	*	*	*	3200	3100	0100	0100
V	SPART	Division	*	*	*	*	01, 02	01, 02	03	03

## WHERE

Authorization restrictions

Total row count: 13

Domain workbook / Venc

Workbook: Task workbook

Drag a column header here to

Module	Field	Description	Objects	Modules	Taskcodes	Actions	TaskWorkbook - Type 2 YYYY
*	KOART	Account type	*	*	AP*	*	K
*	KOART	Account type	*	*	AR*	*	D
*	KTOKK	Vendor account group	*	*	*	*	NORM

## WHAT

Role name indicators

Authorization restrictions

# Build roles automatically

Role (SAP): AAAPBXXXAPRA (\*)

Role name ☒ AAAPBXXXAPRA

Short description Payment run

Description

**CSI Accelerator®**

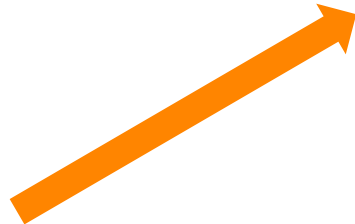
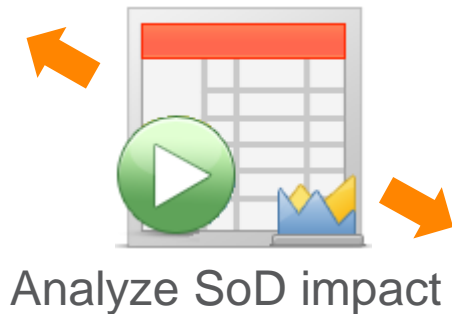
The authorizations are created correctly.  
Added object field authorizations: 0  
Changed object field authorizations: 2

OK

Transactions Authorizations Composite roles Derived roles Users Documents Norm

Drag a column header here to group by that column.

Status	Object	Field	Authorization	Values	Codification	New
*	A	A	A	*	*	<input checked="" type="checkbox"/>
Maintained	F_REGU_BUK	BUKRS	00	3200	3200	<input type="checkbox"/>
Standard	F_REGU_BUK	FBTCH	00	02, 03, 11, 12, 13, 14, 15, 21, 22, 23	#No match#	<input type="checkbox"/>
Standard	F_REGU_KOA	FBTCH	00	02, 03, 11, 12, 13, 14, 15, 21, 22, 23	#No match#	<input type="checkbox"/>
Maintained	F_REGU_KOA	KOART	00	K	K	<input type="checkbox"/>
Standard	S_TCODE	TCD	00	F110	#No match#	<input type="checkbox"/>
Manual						<input checked="" type="checkbox"/>



Approve



Decline



Observe. Think. Act.

Output xml





- With CSI tools we focus on applications to analyze and manage the content of the roles and user-id
- Do not forget that
  - the role is the most important attribute of a user-id
  - in your SAP system most information is available about transaction usage, operating company values, user activities, ... and that with CSI tools this information is used to highlight inconsistencies in rules, roles and user-role assignments
- Next to all these unique features, CSI applications allow you of course to run SOD reports and integrate it even with external systems to enable preventive SOD checking on user and role level.

# Globally Referenced

by hundreds of customers

CSI tools' references are essentially "Fortune 1000" accounts and medium accounts in various sectors like Aerospace & Defense, Automotive, Bank & Insurance, Chemical, Consultancy and Audit, Energy, Oil & Utilities, ICT and Telecom, Manufacturing Industry, Pharmaceutical and Health, Public Organizations, Retail, Transport, etc.



- Automation of monthly SOD reporting and user access request procedure
- Role analytics
  - % of access rights granted through accumulation of access rights
  - % SoD conflicts not being used by end-users (access right removal)
  - % SoD conflicts used by end-users (implementation of compensating controls)
- Rule analytics
  - List transaction codes currently not monitored but used
  - Check the status of optional authorization objects in rule sets

- Health check SAP authorizations
- Implementation of internal control structure and process
  - Assess which risks have no controls and which risks have too much controls
- Reverse engineering of current role concept
- Implementation of RBAC (Role Based Access Controls) concept
- Integrate custom ticketing system with preventive SOD engine of CSI Authorization Auditor



# Identity and Access Governance

for SAP® environments

Thank you



Lim Huck Hai  
Head of RAS Asia Pacific  
[hlim@bdo.my](mailto:hlim@bdo.my)



Johan Hermans  
CEO  
[johan.hermans@csi-tools.com](mailto:johan.hermans@csi-tools.com)