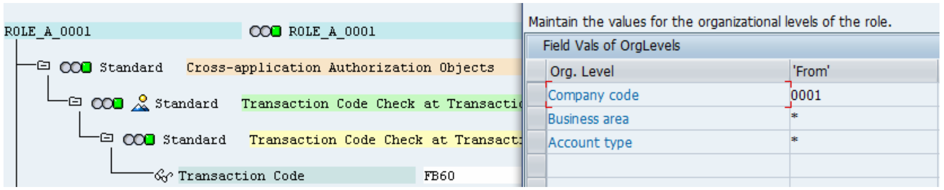
NOTE AUGUST 2011

Organization Rules in GRC AC 10

Organizational rules allow you to filter „false positives” from the risk analysis.

What does that mean?

You have a role concept with master derived roles, where e.g. the leading organizational level is the company code with a corresponding organizational value set.
Role_A_0001 for Company Code 0001 – (FB60)



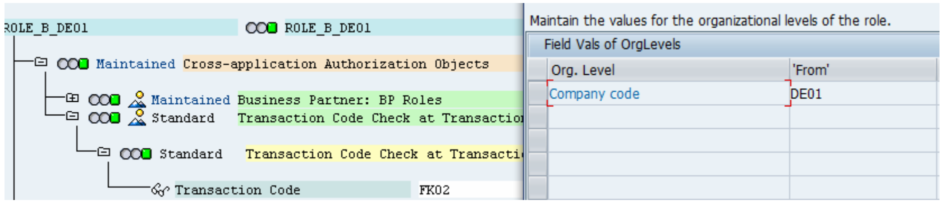
```
ROLE_A_0001            ROLE_A_0001
 Standard  Cross-application Authorization Objects
   Standard  Transaction Code Check at Transacti
     Standard  Transaction Code Check at Transact
       Transaction Code                FB60
```

Maintain the values for the organizational levels of the role.

Field Vals of OrgLevels

Org. Level	'From'
Company code	0001
Business area	*
Account type	*

Role_B_DE01 for Company Code DE01 – (FK02)



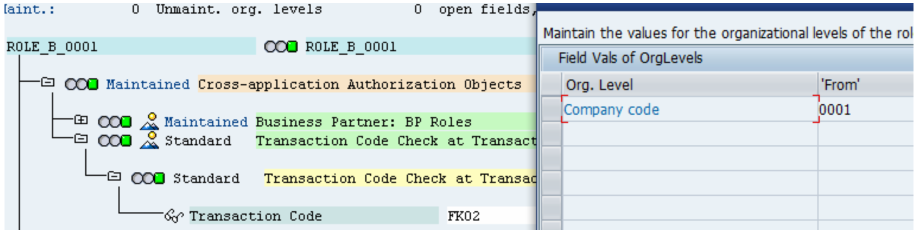
```
ROLE_B_DE01            ROLE_B_DE01
 Maintained Cross-application Authorization Objects
   Maintained Business Partner: BP Roles
   Standard   Transaction Code Check at Transactio
     Standard  Transaction Code Check at Transacti
       Transaction Code                FK02
```

Maintain the values for the organizational levels of the role.

Field Vals of OrgLevels

Org. Level	'From'
Company code	DE01

The Role_A_0001 now contains transaction FB60 (posting of vendor invoices), whereas Role_B_0001 contains transaction FK02 (changing vendor master data).



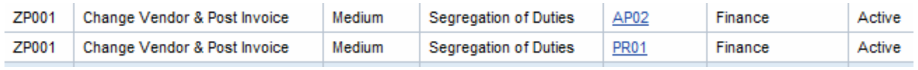
```
aint.:          0  Unmaint. org. levels          0  open fields,
ROLE_B_0001            ROLE_B_0001
 Maintained Cross-application Authorization Objects
   Maintained Business Partner: BP Roles
   Standard   Transaction Code Check at Transact
     Standard  Transaction Code Check at Transac
       Transaction Code                FK02
```

Maintain the values for the organizational levels of the rol

Field Vals of OrgLevels

Org. Level	'From'
Company code	0001

A combination of transaction FK02 (e.g. function ID PR01) and FB60 (e.g. function ID AP02) is a SOD risk reflected by the risk ID ZP001,e.g..



ZP001	Change Vendor & Post Invoice	Medium	Segregation of Duties	AP02	Finance	Active
ZP001	Change Vendor & Post Invoice	Medium	Segregation of Duties	PR01	Finance	Active

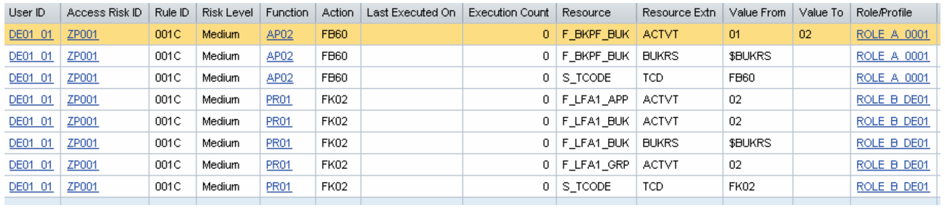
A user who gets the above roles assigned would have a combination of both transactions according to a regular rule set, and would show up with a SOD risk if the organizational values are not considered.

This could be a “false positive” as the user can actually not call FK02 and FB60 for the same company code (legal entity) – depending on the company’s policies.
For filtering these “false positives” you can utilize organizational rules.

There are multiple ways to set up organizational rules depending on your actual filter requirements, but always be careful when setting them up, so that you do not accidentally eliminate “real positives”.

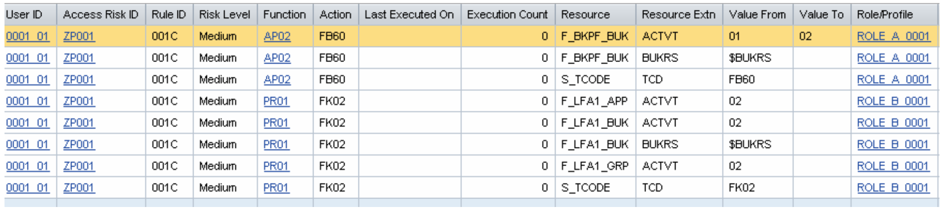
Situation:

User DE01_01 has the role Role_B_DE01 and the role Role_A_0001.
With that he has transaction FK02 and FB60, but for different company codes.
When we run a regular risk analysis for this user, he would show up with a SOD conflict, as he has transaction FK02 as well as FB60 assigned.



User ID	Access Risk ID	Rule ID	Risk Level	Function	Action	Last Executed On	Execution Count	Resource	Resource Extn	Value From	Value To	Role/Profile
DE01_01	ZP001	001C	Medium	AP02	FB60		0	F_BKPF_BUK	ACTVT	01	02	ROLE_A_0001
DE01_01	ZP001	001C	Medium	AP02	FB60		0	F_BKPF_BUK	BUKRS	$BUKRS		ROLE_A_0001
DE01_01	ZP001	001C	Medium	AP02	FB60		0	S_TCODE	TCD	FB60		ROLE_A_0001
DE01_01	ZP001	001C	Medium	PR01	FK02		0	F_LFA1_APP	ACTVT	02		ROLE_B_DE01
DE01_01	ZP001	001C	Medium	PR01	FK02		0	F_LFA1_BUK	ACTVT	02		ROLE_B_DE01
DE01_01	ZP001	001C	Medium	PR01	FK02		0	F_LFA1_BUK	BUKRS	$BUKRS		ROLE_B_DE01
DE01_01	ZP001	001C	Medium	PR01	FK02		0	F_LFA1_GRP	ACTVT	02		ROLE_B_DE01
DE01_01	ZP001	001C	Medium	PR01	FK02		0	S_TCODE	TCD	FK02		ROLE_B_DE01

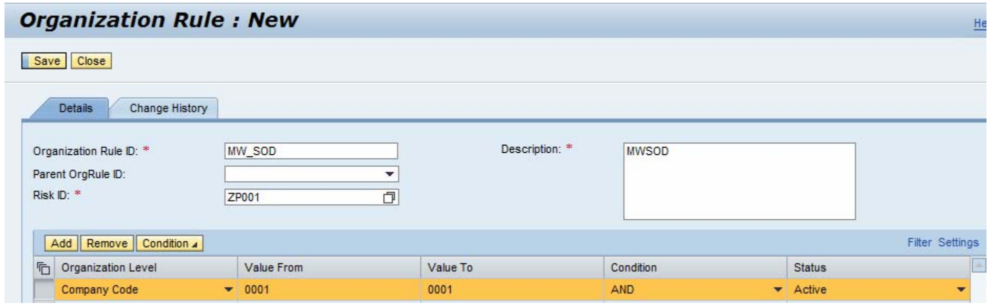
User 0001_01 has the roles Role_A_0001 and Role_B_0001 assigned.
With that he has FK02 and FB60 within one company code, and would also show up in the risk analysis.



User ID	Access Risk ID	Rule ID	Risk Level	Function	Action	Last Executed On	Execution Count	Resource	Resource Extn	Value From	Value To	Role/Profile
0001_01	ZP001	001C	Medium	AP02	FB60		0	F_BKPF_BUK	ACTVT	01	02	ROLE_A_0001
0001_01	ZP001	001C	Medium	AP02	FB60		0	F_BKPF_BUK	BUKRS	$BUKRS		ROLE_A_0001
0001_01	ZP001	001C	Medium	AP02	FB60		0	S_TCODE	TCD	FB60		ROLE_A_0001
0001_01	ZP001	001C	Medium	PR01	FK02		0	F_LFA1_APP	ACTVT	02		ROLE_B_0001
0001_01	ZP001	001C	Medium	PR01	FK02		0	F_LFA1_BUK	ACTVT	02		ROLE_B_0001
0001_01	ZP001	001C	Medium	PR01	FK02		0	F_LFA1_BUK	BUKRS	$BUKRS		ROLE_B_0001
0001_01	ZP001	001C	Medium	PR01	FK02		0	F_LFA1_GRP	ACTVT	02		ROLE_B_0001
0001_01	ZP001	001C	Medium	PR01	FK02		0	S_TCODE	TCD	FK02		ROLE_B_0001

Situation:

Now we create an organizational rule that “filters” the Company Code 0001:

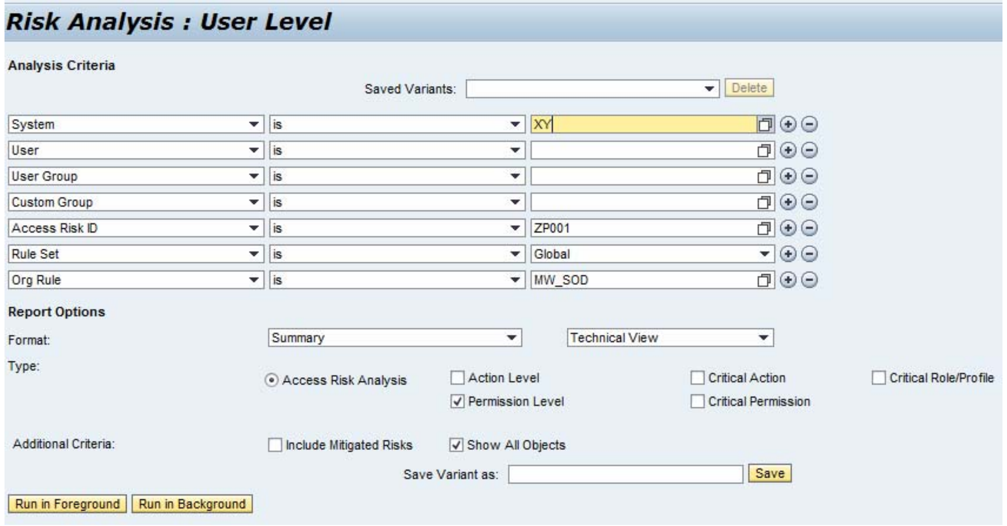


Organization Rule : New

Organization Rule ID: * MW_SOD
Parent OrgRule ID:
Risk ID: * ZP001
Description: * MWSOD

Organization Level	Value From	Value To	Condition	Status
Company Code	0001	0001	AND	Active

In a next step we want to apply this organizational rule to the analysis.



Risk Analysis : User Level

Analysis Criteria

Saved Variants:

System	is	XY
User	is	
User Group	is	
Custom Group	is	
Access Risk ID	is	ZP001
Rule Set	is	Global
Org Rule	is	MW_SOD

Report Options

Format: Summary Technical View

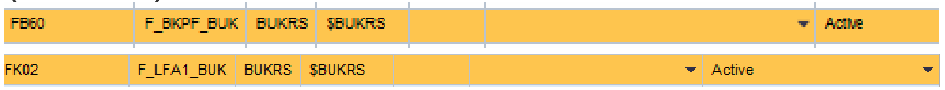
Type: ● Access Risk Analysis ☐ Action Level ☑ Permission Level ☐ Critical Action ☐ Critical Permission ☐ Critical Role/Profile

Additional Criteria: ☐ Include Mitigated Risks ☑ Show All Objects

Save Variant as:

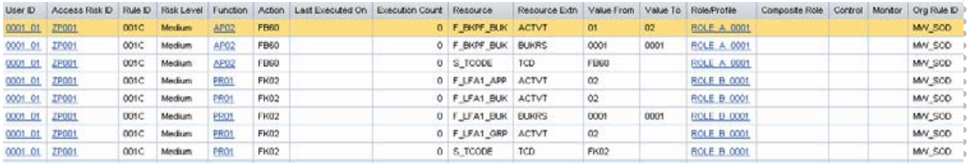
NOTE!

Please be aware that the corresponding organizational value has to be set to *Active* in the functions, and that the rules need to be regenerated (Generate Rules).



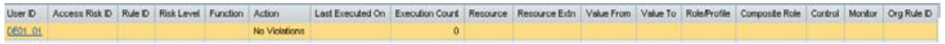
FB60	F_BKPF_BUK	BUKRS	$BUKRS			Active
FK02	F_LFA1_BUK	BUKRS	$BUKRS			Active

After that, only the user 0001_01 will continue to show up in the risk analysis report when the corresponding organization rule is applied.



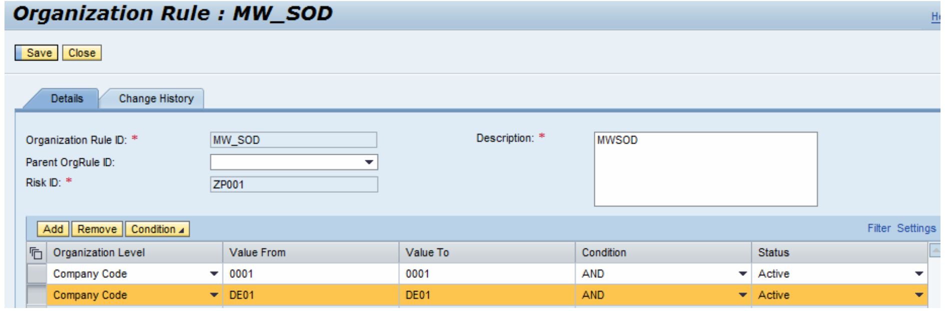
User ID	Access Risk ID	Rule ID	Risk Level	Function	Action	Last Executed On	Execution Count	Resource	Resource Extn	Value From	Value To	Role/Profile	Composite Role	Control	Monitor	Org Rule ID
0001_01	ZP001	001C	Medium	AP02	FB60		0	F_BKPF_BUK	ACTVT	01	02	ROLE_A_0001				MW_SOD
0001_01	ZP001	001C	Medium	AP02	FB60		0	F_BKPF_BUK	BUKRS	0001	0001	ROLE_A_0001				MW_SOD
0001_01	ZP001	001C	Medium	AP02	FB60		0	S_TCODE	TCD	FB60		ROLE_A_0001				MW_SOD
0001_01	ZP001	001C	Medium	PR01	FK02		0	F_LFA1_APP	ACTVT	02		ROLE_B_0001				MW_SOD
0001_01	ZP001	001C	Medium	PR01	FK02		0	F_LFA1_BUK	ACTVT	02		ROLE_B_0001				MW_SOD
0001_01	ZP001	001C	Medium	PR01	FK02		0	F_LFA1_BUK	BUKRS	0001	0001	ROLE_B_0001				MW_SOD
0001_01	ZP001	001C	Medium	PR01	FK02		0	F_LFA1_GRP	ACTVT	02		ROLE_B_0001				MW_SOD
0001_01	ZP001	001C	Medium	PR01	FK02		0	S_TCODE	TCD	FK02		ROLE_B_0001				MW_SOD

User DE01_01 will not have a SOD conflict listed when the organizational rule is applied.



User ID	Access Risk ID	Rule ID	Risk Level	Function	Action	Last Executed On	Execution Count	Resource	Resource Extn	Value From	Value To	Role/Profile	Composite Role	Control	Monitor	Org Rule ID
DE01_01					No Violations		0									

You want to create an organizational rule that generally eliminates all possible "false" positives for roles that are strictly assigned based on organizational level differentiation, meaning that users should never have SOD within one legal entity, but may definitely perform these functions for different company codes. The rule could look like this:



Organization Rule : MW_SOD

Organization Rule ID: * MW_SOD

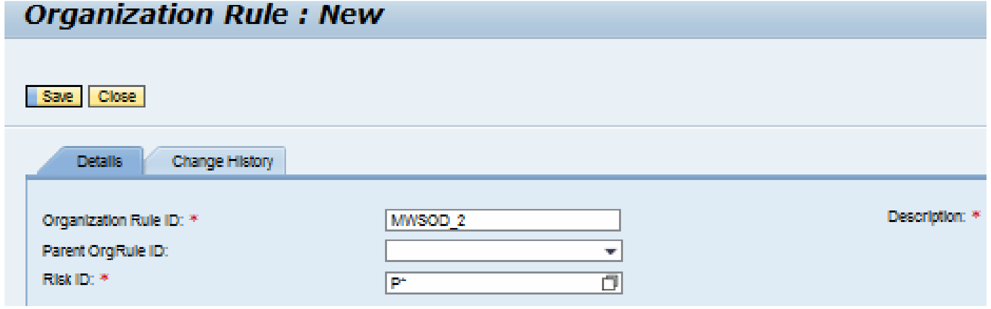
Parent OrgRule ID:

Risk ID: * ZP001

Description: * MWSOD

Organization Level	Value From	Value To	Condition	Status
Company Code	0001	0001	AND	Active
Company Code	DE01	DE01	AND	Active

The risk ID could be generic:



Organization Rule : New

Organization Rule ID: * MWSOD_2

Parent OrgRule ID:

Risk ID: * P*

Description: *