Quick Reference Guide

Virsa Compliance Calibrator for SAP v5.2 "Organizational Rules and Organizational Level Reporting"

Purpose:	Use this Quick Reference Guide to understand and create Organizational Rules and perform organization level reporting
Why:	For Organizational Rules - to remove false positive SoDs based on organizational level segregation. For Organizational Level Reporting – to run analysis and distribute results for certain areas of an organization
When:	Perform this task after Compliance Calibrator v5.2 has been successfully installed and base set of rules have been loaded
How often:	Once after installation, then as needed

Overview

Organizational rule functionality has been created to eliminate false positives based on organizational level restrictions. It is important to understand that organizational rules should only be used in those specific situations where a customer has made a conscious decision to segregate via organizational levels.

For example, a customer may have a shared service center where they allow a team member to both process vendor invoices and create AP payments. Normally, this would be a high risk level conflict. However, the shared services center has specifically segregated their team members so that they cannot do these two functions for the same organizational levels.

In our examples below, the shared service center has segregated so that the user who can enter vendor invoices for plants BR01 or BR03 cannot process payments for company code 1000 (since plants BR01 and BR03 are part of company code 1000). In this example, a conscious decision was made to deal with the conflict via segregating org levels so for this risk, organization level rules are applicable.

This functionality should not be used to try to group users into reports by organizational levels in order to distribute SoD reports to various management levels. Organization level rules should only be used for exception based reporting in order to remove false positive conflicts that result from organization level segregation. Because of the sizable performance impact that organization level rules can have, they should be used minimally for only those situations where the company has made a conscious decision to segregate via org levels.

Organizational Level reporting is what can be used in order to consolidate reports of conflicts for a specific organizational unit to assist in distributing reports to the risk owners of each area.

Both Organizational level reporting and Organizational Rules are described in this QRG.



Virsa Compliance Calibrator for SAP v5.2 "Organizational Rules and Organizational Level Reporting"

ORGANIZATIONAL RULES

Business Case

During the remediation phase, the business owner who is responsible for the Procure to Pay business process has indicated that one of the risks that is coming up for the user Jane Doe is a false positive. The owner's justification is that this person cannot do these functions in the same organizational level, therefore, the conflict cannot be exploited.

In this example, the user Jane Doe can enter invoices for plants BR01 and BR03 (which are part of company code 1000), however, she can only process payments for company 2000. Therefore, she can't actually enter a fictitious vendor invoice and then render payment to the same vendor as the organization levels are preventing her from doing this.



Therefore, the business owner feels that Jane Doe should be excluded from the report using Organizational Rules



Virsa Compliance Calibrator for SAP v5.2

"Organizational Rules and Organizational Level Reporting"

Step 1: Open Compliance Calibrator

- 1. Open your web browser.
- 2. Enter the URL for Compliance Calibrator: http://<servername>:<port>/webdynpro/dispatcher/virsa/ccappcomp/ComplianceCalibrator
- 3. Log onto Compliance Calibrator as a user with Administration privileges.

Step 2: Schedule the Organization User Mapping job

- 1. Click the **Configuration** tab.
- 2. Click on Org. User Mapping
- 3. Complete the following fields:
 - System ID
 - User
- 4. Click the **Background** button.

Compliance Calibrator - I	Microsoft Internet Explorer								
Ele Edit View Favorites Iools Help									
🚱 Back 🔻 🕥 👻 😰	🏠 🔎 Search 🤺 Favorites 🔗 🔗	• 📚 🖬 • 🛄 🇱 🦓							
Address http://ldcivfd:5770	00/webdynpro/dispatcher/virsa/ccappcomp/C	omplianceCalibrator		▼ 🗗 Go Links »					
Virsa (Informer Rule Architec	Compliance Calibrator	Welcome Jayne Gibbon Log C on Debug Analysis Daemon BG Daemon	ff About						
Default Values Deformance Tuning	0	F00.6.0							
Additional Options Mitigating Controls	System ID: User:	* to:							
Workflow Miscellaneous	Foreground Background)							
 MIC User Mappings MIC Risk Mappings 									
Connectors Logical Systems Cross Systems									
Data Extraction Master User Source									
 User Mapping Custom User Group 									
Upload Objects Rule Upload									
Background Job Org. User Mapping									
Custom Tabs Upload Informer Reports									
SAP Adapter									
🙆 Done				Local intranet					



Virsa Compliance Calibrator for SAP v5.2

"Organizational Rules and Organizational Level Reporting"

- 5. Schedule the job to execute immediately and then periodically after that. Best practice is the job should be run at least weekly.
- 6. This job will bring over the data of what organization levels each user is assigned.

Compliance Calibrator - I	Microsoft Internet Explorer								_ & ×	
<u>File Edit View Favorites</u>	Ele Edit View Favorites Iools Help									
😮 Back 🔻 🕑 🔻 📓 🎧 🔎 Search 🌟 Favorites 🚱 🔗 🔌 📓 🛪 📙 🔣										
Address Address Address Address	ddress a http://dov/d.57700/webdynpro/dspatcher/visa/ccappcomp/ComplanceCalibrator									
SAP Virsa (Compliance Calib	rator We r Configuration Debu	Icome Jayne Gibbon g 🖌 Analysis Daemon 🍸	Log Off About	SAP NetWoaver					
 Risk Analysis Default Values 	Schedule Org User	r Extraction Backg	round Job		C					
Performance Tuning	Schedule Selection									
Additional Options Mitigating Controls Workflow Miscellaneous MIC User Mappings MIC Disc Mappings	Job Name: ⊙ Immediate start ⊜ Delayed start	Organizational User Mag Date: 8/14/2007 ार्?	Time: 8:53:48 PM							
Connectors	Period Selection									
 Logical Systems Loross Systems Data Extraction Master User Source User Mapping Custom User Group Upload Objects Rule Upload Background Job Org. User Mapping Custom Tabs Upload Informer Reports SAP Adapter 	Schedule Periodically Schedule Reset	C Daily C <u>VVeekly</u> Monthly End Date:	1 Day(s) 1 Week(s) 1 Month(s)							
Done								Subscription Local inf	ranet	

Step 3: Determine what is being segregated by Org Levels and for which risks

- 1. Identify which Risk is being mitigated by segregating organizational levels.
- 2. In the example below, it is risk ID P003 Process Vendor Invoices and AP Payments
- 3. Discuss with Business Process Owners what organizational levels should NOT be combined
- 4. In the example below, users should not have access to enter vendor invoices for plants BR01 or BR03 and also be able to pay vendors in company code 1000.

Step 4: Enable the organizational level variables in the functions.

- 1. Click on the Rule Architect tab and expand Functions and then click Search.
- 2. Enter the first function that is part of the risk that needs an organizational rule and click Search.

Quick Reference Guide

Virsa Compliance Calibrator for SAP v5.2

"Organizational Rules and Organizational Level Reporting"

- 3. Highlight the Function and select Change.
- 4. Select the Permissions tab.
- 5. For each Action under this function, expand the action and find the permission that contains the organizational levels that are being segregated.
- 6. In this example, permission F_BKPF_BUK for action F-07 restricts which company code the transaction code can be executed for.
- 7. Check to make sure there is a valid activity (01 not 03) and change the status from **Disable** to **Enable**. Do this for both the activity and the org variable.
- 8. For the organizational field itself, ensure you leave the \$ value as is.
- 9. Save the function.



Quick Reference Guide

Virsa Compliance Calibrator for SAP v5.2

"Organizational Rules and Organizational Level Reporting"

- 10. Repeat this process for the second function that makes up the risk to be segregated by Organizational levels.
- 11. In this example, permission M_RECH_WRK for action MIRO restricts which plant the transaction code can be executed for.



Quick Reference Guide

Virsa Compliance Calibrator for SAP v5.2

"Organizational Rules and Organizational Level Reporting"

Step 5: Create the Org Rule

- 1. Return to the Rule Architect tab, expand the Organization Rules menu and click Create.
- 2. You can use a naming convention that will tell the user which Organizational Rules ID should be entered in the risk analysis selection.
- 3. Enter the Risk ID that is relevant for this org rule and the corresponding organizational levels that should be reviewed.
- 4. In this example below, the settings are indicating that only those users that have access to company code 1000 AND plants BR01 or BR03 will actually have a segregation of duties conflict.

🗿 Compliance Calibrator - Micro	osoft Internet	Explo	rer										_ & ×
<u>File Edit View Favorites Too</u>	Ele Edit View Favorites Iools Help												
🕒 Back 🔻 🕥 👻 🗾 💋 🏠	🖕 Back 🔻 🕗 👻 🖹 🖉 🏠 🔎 Search 🧏 Favorites 🤣 😒 👻 🔔 🎬 👻 🛄 🎉 🎇												
Address i http://dcivfd:57700/w	ddress 🗃 http://dcivld:57700/webdynpro/dispatcher/virsa/ccappcomp/ComplanceCalibrator 🔽 🗗 Go 🛛 Links **												
SAP Virsa Col	mpliance	ert Mor	librator Welcome Jay	ne Gibbor sis Daemor	BG	Log Off A	Abou	It SAP NotW		1			
Rule Library	Create O	rgani	zation Rule										
 Business Processes Rule Sets Functions Risks Rules Rules 	Org Rule ID: Description: Parent Org R	ule:	P003_1000 Payments in CC 1000	/Invoicing i	n plan								
Critical Roles Critical Profiles	Risk		Org. Level	From	То	Search Type	-	Status					
 Organization Rules Create 	P003*		Company code (BUKRS)	- 1000		AND	₹ E	Enable	•				
Search	P003*	٦	Plant (WERKS)	BR01		OR	- E	Enable	•				
 Supplementary Rules Utilities 	P003*		Plant (WERKS)	BR03		OR	- 1	Enable	•				
Function Mass Maintenance	_						_						
		1											
		1											
	Save Clear												
🙆 Done												Local intranet	

5. Save the Organization Rule



Virsa Compliance Calibrator for SAP v5.2

"Organizational Rules and Organizational Level Reporting"

Step 6: Run Organization Rule Analysis

- 1. Go to the Informer tab, and expand Risk Analysis
- 2. Click on Org. Level
- 3. In Analysis Type, choose Org Rule.
- 4. Enter the Organization Rules for which you want to analyze.
- 5. Enter the User ID(s) that you want to analyze.
- 6. Execute the report.

📲 Compliance Calibrator - Microsoft Internet Explorer									
Ele Edit View Favorites Tools Help 🦓									
🕒 Back 🔻 🕗 🔻 🖻 🐔 🔎 Search 🐈 Favorites 🤣 🔗 👻 🦕 🖀 👻 🛄 🕉									
ddress 🗿 http://dcivfd:57700/webdynpro/dispatcher/virsa/ccappcomp/ComplanceCalibrator									
Virsa Compliance Calibrator Welcome Jayne Gibbon									
▼Management View Risk Analysis - Org. Level									
 Risk Volations Users Analysis Comparisons Analysis Type: Org Rule Analysis Type: Org Rule Controls Library Controls Library Controls Library User: User:<									
	Local intranet								



Virsa Compliance Calibrator for SAP v5.2

"Organizational Rules and Organizational Level Reporting"

7. Note that now Jane Doe does not show up anymore. Only Joe Black does as he has access to company code 1000 and plants BR01 or BR03 which means his conflict is a true conflict.

File Site Year Reports Search * Frances Frances * * * * * * * * * * * * * * * * * * *	🕘 Compliance Calibrator	r - Microsoft Internet Explorer						_ 8 ×		
Image: Interrute interrut	<u>File Edit View</u> Favorite	je Edit Vjew Favorites Tools Help 🦓								
	🕽 Back 🔻 🕗 🛩 🖹 🙆 🏠 🔎 Search 👷 Favorites 🤣 🗟 👻 🦕 🕋 🛩 🛄 🎉									
	Address 🗟 http://idcivfd:5	57700/webdynpro/dispatcher/virsa/ccap	pcomp/ComplianceCalibrator					💌 🔁 Go 🛛 Links 🎽		
• Management View Org Level Analysis at Permission Level - Summary Report © © © © © © © © © © © © © © © © © © ©	SAP Virsa	a Compliance Calibrato	ON Welcome Ja	yne Gibbon ysis Daemon 👔 BG D	Log Off Abou	t				
• User Analysis • User Analysis • Rule Subrary • Rule Subrary • Rule Analysis • Rule Subrary • Rule Subrary • Rule Subrary • Rule Analysis • Rul	Management View Risk Violations	Org Level Analysis at Per	mission Level - Sum	mary Report	© 🤉	🖻 🤽 🖿 🖪				
• Comparisons Comparisons • Comparisons Fortilicting Actions Risk Description Level Business Process Mitigating Control Monito Org Rule Description • Rules Library • Conditions Library Post Outgoing Payments (F=OT) and Postones (HRO) Postones (HRO) <td>Users Analysis Dolo Analysis</td> <td>User Id: Joe Black (1999998)</td> <td>User</td> <td>Group: ORGLEVEL</td> <td></td> <td>System: ECC</td> <td>6.0</td> <td></td>	Users Analysis Dolo Analysis	User Id: Joe Black (1999998)	User	Group: ORGLEVEL		System: ECC	6.0			
 Aleris Rules Library Controls Library Controls Library User Level Role Level Role Level Role Reports Gog Level Audit Reports Background Job M I of 1 pages PB No. of rows per page:: 10 (Total no. of rows: 1) 	Comparisons	Conflicting Actions	Risk Description Level	Business Process	Mitigating Control	Monitor Org Rule Descri	iption			
• Ofg Level • MC • Audit Reports • Security Reports • Background Job	Alerts Rules Library Controls Library Risk Analysis User Level Role Level HR Objects	Post Outgoing Payments (F-07) and Enter incoming Invoice (MIRO)	P00301601: Create fictitious vendor invoice and initiate payment for it	Procure to Pay		P003_1000:Paym in CC 1000/Invoic plants BR01 or Bl	nents cing in R03			
	 MC Audit Reports Security Reports Background Job 	K (1 of 1 pages) H	No. of rows per page:: 10] (Total no. of rows: 1)						
								T		

There is the option in configuration to have Org Rules considered when updating the management reports.

The default is set to no. What this means is that when the management reports are updated, none of the org rules are used. This will result in 100% of the users being shown as having the conflict, even those such as Jane Doe that don't really have the conflict based on organizational segregations. If this option is set to "YES", all possible variations or org value combinations MUST be created.

Quick Reference Guide

Virsa Compliance Calibrator for SAP v5.2 "Organizational Rules and Organizational Level Reporting"

Compliance Calibrator - I	Microsoft Internet Explorer	_ 8 ×							
<u>E</u> le <u>E</u> dit <u>V</u> iew F <u>a</u> vorites	Tools Heb	A 7							
🕽 Back = 🕤 👻 🖻 🐔 🔎 Search 👷 Favorites 🤣 🔝 = 😓 🏭 🐇									
Address 🔕 http://dcivfd:5770	00/webdynpro/dispatcher/virsa/ccappcomp/ComplianceCalibrator	💌 🔁 Go 🛛 Links 🎽							
SAP Virsa (Compliance Calibrator Welcome Jayne Gibbon Log Off About								
▼ Risk Analysis	Risk Analysis - Additional Options								
Default Values Performance Tuning Additional Options	This option determines whether the SoD Supplementary table is checked when running a Risk Analysis. The default value is No. If the value is set to Yes SoD Supplementary entries are checked when running a Risk Analysis.								
Mitigating Controls Workflow	Include Role/Profile Mitigating Controls in User Analysis								
Miscellaneous MiC User Mappings MiC Risk Mappings Connectors	To include Role or Profile-based Mitigation Controls in User-based Risk Analysis reports set this value to Yes The risk analysis will include User-level Mitigation Controls IDs if there is one If not, the report will display either the Role-based or Profile-based Mitigation Control ID in that order. The default value is No.								
Logical Systems Cross Systems Data Extraction	Enable Offline Risk Analysis Yes The default value is Yes.								
Master User Source User Mapping Custom User Group Upload Objects Rule Upload	Consider Org. Rules when updating the Management reports and during Risk Analysis Web Service Call. Yes This option determines whether to consider Org Rules when updating the Management Reports in Informer and during th Analysis Web Service Call. Default value is No								
Backend Sync Background Job Search	Convert Users, roles and profiles to upper case Yes This option converts users, roles and profiles to Upper Case (recommended for SAP systems). The default value is YES. Setting the value to NO disables this feature.								
Alert Generation									
Org. User Mapping Custom Tabs Upload Informer Reports SAP Adapter	[Save] [Cancel]								
Done		Local intranet							



Virsa Compliance Calibrator for SAP v5.2 "Organizational Rules and Organizational Level Reporting"

For example, say in addition to company code 1000 with plants BR01 or BR02, a conflict would also exist if a person had company code 3000 with plants CAP1 or CAP2. In the example below, new user Billy White has the conflict, but with company code 3000 and plant CAP1.





Virsa Compliance Calibrator for SAP v5.2 "Organizational Rules and Organizational Level Reporting"

Just like in the previous example, if risk analysis at the Org Rule is run for these users, using the org rule created for Company Code 1000 with plants BR01 or BR03, only Joe Black will show up.

Complance Calibrator - Microsoft Internet Explorer									
Be Edit View Favorites Itolis Help									
🚱 Back ▼ 🗇 ▼ 🖹 🖉 🏠 🔑 Search 🛠 Favorites 🚱 😥 ▼ 🌽 🗮 × 🛄 🏭 🦓									
Address 🕘 http://ldcivfd:5	gáres 👔 http://dci/dci57200/webdynpro/dspatcher/visa/ccappcomp/ComplanceCalibrator 🔽 🔂 Go 🛛 Linis "								
SAD		Welcome	was Cibboa		SAP Hattwarer			<u> </u>	
Virs:	a Compliance Calibrato	r	ayne oloboll	Log Off About					
Informer Rule Arch	itect / Mitigation / Alert Monitor / Co	onfiguration Debug Ana	lysis Daemon BG Da	aemon		$\langle \rangle \square$			
Management View Risk Violations	Org Level Analysis at Per	mission Level - Sum	mary Report	6 🤉	🖻 🤽 🖨 🕼				
Users Analysis Role Analysis	User Id: Joe Black (1999998)	Use	r Group: ORGLEVEL		System	: ECC 6.0			
Comparisons	Conflicting Actions	Risk Description Leve	Business Process	Mitigating Control	Monitor Org Rule	Description			
Alerts Rules Library Controls Library Risk Analysis User Level Role Level HR Objects	Post Outgoing Payments (F-07) and Enter Invoice (MIRO)	P00301601: Create fictitious vendor invoice and initiate payment for it	Procure to Pay		P003_100 CC 1000// plant br01	Payments in nvoicing in or br02			
Audit Reports Security Reports Background Job	N C 1 pages N N	Vo. of rows per page:) (Total no. of rows: 1)						
Done							Second Intra	anet	

Quick Reference Guide

Virsa Compliance Calibrator for SAP v5.2 "Organizational Rules and Organizational Level Reporting"

When config option Consider Org Rules is set to yes, then all risks for which at least 1 org rule has been created will be filtered through the org rules. In this case, since there is only an org rule for company code 1000, only Joe Black will show as having this conflict, even though in actuality, Billy White should have it as well. This is seen in the user analysis below. Basically, it only shows the user with the violation

🚈 Compliance Calibrato	or - Microsoft Internet Explorer	_ & ×
Ele Edit View Favorite	tes Iook Help	27
😋 Back 👻 💮 👻 💌	📓 🏠 🔎 Search 👷 Favorites 🚱 😒 👻 🐂 🛄 🏭	
Address 🕘 http://idcivfd:	:57700/webdynpro/dispatcher/virsa/ccappcomp/ComplanceCalibrator	🔻 🔁 Go 🛛 Links 🎽
SAP Virs	a Compliance Calibrator Welcome Jayne Cibbon Log Off About	<u> </u>
 Management View 	Management View - User Analysis Summary as of 07-Sep-2007	
Risk Violations	Segregation of Duties	
Role Analysis Comparisons Alerts	Cal Month/Year 09/2007 V System ECC 6.0 V SALE graphics	
Rules Library Controls Library	User Group ORGLEVEL Graphics Rendering Problem	
Risk Analysis Audit Deports	Violation Count By Permission	
Security Reports		
Background Job	No. of Users Analyzed 4	
	Users with Notations 3 75%	
	Users mail violations 1 20%	
	Critical Actions and Roles	
	SAP graphics	
	Number of Users Analyzed 4 Graphics Rendering Problem	
	Number of Critical Actions 560	
	Number of Critical Roles/Profile 0	
	Users with Critical Actions 2	
Done		Local intranet
		, , , , , , , , , , , , , , , , , , , ,



Virsa Compliance Calibrator for SAP v5.2 "Organizational Rules and Organizational Level Reporting"

Below is the same report when this configuration option is set to "no" so that org rules are not included.





Virsa Compliance Calibrator for SAP v5.2 "Organizational Rules and Organizational Level Reporting"

Only if a new org rule is created for company code 3000, plants CAP1 or CAP2 is created, will Billy White show on the management reports.

Therefore, if this configuration option is set, it's imperative that the company create all necessary org level rules, otherwise the reporting will contain false negatives (not all users who actually have the conflicts will be shown).

In CC 5.2, there is the option to create a mitigating control at the Org Rule level, versus at the risk level.

🔮 Compliance Calibrator - M	licrosoft Inter	net Explore	r									_ 8 ×
Ele Edit View Favorites	e Edit View Favorites Iools Help											
🗿 Back 🕶 🔘 🔻 📓 😚 🔎 Search 👷 Favorites 🛷 😥 📾 👻 🧫 🏭 🕷												
Address) http://idcivfd:5770	dress 🌒 http://dciv/dci57700/webdynpro/dspatcher/vrsa/ccappcomp/ComplanceCalbrator 👻 💕 Go Unks									Go Links "		
Address in http://dowdis5770 Virsa C Informer Rule Architect - Controls Library - Administrators - Business Units - Mitigating Controls - Create - Search - Mitigated Notes - Mitigated Users - Mitigated Roles - Mitigated Roles - Mitigated Profiles - HR Mitigation	Ovvebdynpro/d Compliance Matgation Search Re User ID 10000000	xpatcher/vrr ce Calil Alert Monit esults - I Name Joe Black	AA/CORPCOMP	(ComplanceCalbrator Welcome ration Debug An User Org. Rule Mitigating Control ID ORGRULE1	Jayne Gibbo alysis Daemo P00301601	A BG Daes	Log O non Valid To 9/6/2008	Monitor PAREDESR	Status		¥ (2)	Go Units »
	Add Chan	ge Delete]									×
Done											Second Second Second	net



Virsa Compliance Calibrator for SAP v5.2 "Organizational Rules and Organizational Level Reporting"

When you create a mitigation control at the org rule level, this mitigation will NOT come over when you run normal risk analysis.

Compliance Calibrato	r - Microsoft Internet Explorer							_ 8
je Edit Vjew Favorites Itols Help 🦓								
🕽 Back 🕶 💿 🕆 💌 🖻 🏠 🔎 Search 👷 Favorites 🚱 🔗 🛬 🦕 🎬 🛪 🛄 🎇								
dress 🜒 http://dciv/d:57700/webdynpro/dispatcher/virsa/ccappcomp/ComplanceCalibrator 🔻 💕 Go 🛛 Links								
Virsa	a Compliance Calibrato	Or Welcome	a Jayne Inalysis (Gibbon Daemon 🖉 BG Daemo	Log Off About			
Management View Risk Violations	User Analysis at Permiss	ion Level - Summa	ry Re	port	C 🧐 🖻	2 🗅 🖪		
Users Analysis Role Analysis	User Id: Jane Doe (1999996)	User Gro	up: ORG	BLEVEL	System	ECC 6.0		
Comparisons	Conflicting Actions	Risk Description	Level	Business Process	Mitigating Control	Monitor		
Alerts Alerts Rules Library Controls Library Risk Analysis User Level Role Level	Post Outgoing Payments (F-07) and Enter Invoice (MIRO)	P00301601: Create fictitious vendor invoice and initiate payment for it	High	Procure to Pay				
Org. Level	User Id: Billy White (1999997)	User Gro	up: ORG	BLEVEL	System	: ECC 6.0		
MIC Audit Reports Gecurity Reports Background Job	Conflicting Actions	Risk Description	Level	Business Process	Mitigating Control	Monitor		
	Post Outgoing Payments (F-07) and Enter Invoice (MIRO)	P00301601: Create fictitious vendor invoice and initiate payment for it	High	Procure to Pay				
	User Id: Joe Black (1999998)	User Gro	up: ORG	GLEVEL	System	ECC 6.0		
	Conflicting Actions	Risk Description	Level	Business Process	Mitigating Control	Monitor		
	Post Outgoing Payments (F-07) and Enter Invoice (MIRO)	P00301601: Create fictitious vendor invoice and initiate payment for it	High	Procure to Pay				
	User Id: TB01 TK20 all Dummy User	for (1999999) User Gro	up: ORG	BLEVEL	System	ECC 6.0		
	Conflicting Actions	Risk Description	Level	Business Process	Mitigating Control	Monitor		
	Post Outgoing Payments (F-07) and Enter Invoice (MIRO)	P00301601: Create fictitious vendor invoice and initiate payment for it	High	Procure to Pay				
	I of 1 pages FIN	No. of rows per page:	10 (To	tal no. of rows: 4)				
one	ier builes []						l locali	tranet

Quick Reference Guide

Virsa Compliance Calibrator for SAP v5.2 "Organizational Rules and Organizational Level Reporting"

The mitigation will only show when you run the Org Rule report. What this would allow you to do is to have separate mitigations based on the org rules for the same risk and same user. For example, a user might have the same risk, but for two different org rules. You would be able to attach the mitigation for one of the org rules, but not for the other. Therefore, when you run the org rule report, the mitigation would just show against the org levels mitigated, where the other org rule report would not be mitigated.





Virsa Compliance Calibrator for SAP v5.2 "Organizational Rules and Organizational Level Reporting"

Access Enforcer

Org Rules and Mitigations can also be included during the Access Enforcer Risk Analysis. A prerequisite to this is that the org rules must be set up in Compliance Calibrator as defined above.

1. The first step is to log into Access Enforcer, click on the configuration tab and then choose Risk Analysis. Under Select Compliance Calibrator Version, the check box for Perform Org Rule Analysis must be selected.

Please note that when selected, it operates similarly to if you set the config option in Compliance Calibrator to consider org rules. Therefore, if you set this, you need to ensure that ALL possible org level combinations are built into your org rules, or it will exclude possibly valid conflicts.

Access Enforcer Informer	Configuration						
нн X	Risk Analysis						
Request Configuration	Select Options						
Priority	Default Analysis Type	Object Level					
Application Configuration Employee Type Configuration	Consider Mitigation Controls						
Number Ranges	Save						
Risk Analysis							
Mitigation	Select Compliance Calibrator Version						
Attributes Service Level	Version	5.2 Web Service					
Password Self Service	URI	http://ldcivfd.wdf.sap.corp:57700/VirsaC(
Custom Fields	UserName	webuser					
Support	Password						
Workflow	rassword	•••••					
Provisioning	Perform Org Rule Analysis						
Approvers	Save						
Connectors							



Virsa Compliance Calibrator for SAP v5.2

"Organizational Rules and Organizational Level Reporting"

The URI for Org Rule Search URI must be completed. This URI can be found under the Web Services - VirsaCCOrgRules5_3Service

SAP I	/irsa Access E	nforcer ™	Welcome Susan Stanleton
Access Enforcer	Informer Con	figuration	
N N Request Configuration	Mitigation		
Request Type	Select Options		
Priority	Allow Approvers To approv	e Access despite conflicts	
 Application Configuration Employee Type Configuration 	Default Duration (in days) fo	or the Mitigation Control	365
Number Ranges	Mitigation URI		http://iwdf2275.wdf.sap.corp:50000/VirsaCCMit
 Risk Analysis 	Risk Search URI		http://iwdf2275.wdf.sap.corp:50000/VirsaCCRis
Mitigation	Org Rule Search URI		http://iwdf2152.wdf.sap.corp:50000/VirsaCCOr
 Attributes Service Level 			
Password Self Service	Save		
VirsaCCActionUsa VirsaCCDescriptio VirsaCCFunction5 VirsaCCMitigation VirsaCCOrqRules VirsaCCRisk5_0S	geService onReader5_OService _OService 5_OService 5 <u>_3Service</u> ice		
Image of the second se second second sec	sisService		
	rvice5_2Service		

1. Display of AE request with risk and org rule violations for Risk ID P001. Select Risk P001 and click 'Mitigate'.

4	Access Enforcer												
	нн ×	~,~		DCIW			×						
	 Request For Approval 	Rol	es/Profi	les									
	 Create Request 				_							Select	
	Search Request	_	System	Role/Profile Ivame		ype Ri	ole/Profile Description		Valid From	Valid To	Owner	SystemAction	n
	Request On Hold	Ľ	DCM	US:FLVM MAINTE	NANCE) v	/endor Master Maintenance		09/13/2007 🛅	12/31/9999	Cyrus Perkins	ADD	
	Approver Delegation Conv Request										(GFERRING)		
	Request Audit Trail												
	Reaffirm												-
		Si	nulate										
			Ri	sk Violation	Oritical	Trans	ection						
		-	10		Critical	muns	succion						
			Risk ID	Risk Descript	ion			Org Ru	les	V	iolation Count	Status	_
		÷	BSCI	Basis Critica	Actions						2	•	1
		٠	HRMD	HR Master D	ata						2	•	
		٠	P001	Create fictitio	ous vendor ar	nd initi:	iate payment to the vendor	CORPO	RATE;FRANCE;		32	٠	
		۲	P002	Maintain a fio	titious vendo	rand	direct disbursements to it				6	٠	
													-
		M	1	1 💌 🕨 🗎									
		L.S	ianto	Continue	. I								
		IVI	igate Jh	Continue	2								
			8										

Quick Reference Guide

Virsa Compliance Calibrator for SAP v5.2 "Organizational Rules and Organizational Level Reporting"

2. Click on 'Search' icon for Org Rules to search for Org rule to mitigate

N N X	Mitigation							
Create Request	Assign Mitigation Control							
 Search Request Request On Hold 	Risk ID	P001						
Approver Delegation Copy Request	Valid From*	M/VONG 09/14/2007						
Request Audit Trail	Valid To*	09/13/2008	-					
 Reaffirm 	Reference No*		٩					
	Org Rules Assigned							
	Org Rules*		9					
	Functional Area*] 40)					
	Management Approver*							
	Mitigation Monitor*	Select	•					
	Save Cancel Create							

3. Search result displays all relevant org rules for Risk ID P001* to select for mitigation. You can select all or one org rule at a time.

4	Access Enforcer								
	нн ×	Org F	Rule Search						
	Request For Approval	Org F	Rules						
Create Request Search Request			Org Rule ID	Description	Org Level	From Value	To Value	Search Value	Status
	 Request On Hold 		CORPORATE	Corporate Shared Services	BUKRS	3000	3000	OR	true
	 Approver Delegation 		CORPORATE	Corporate Shared Services	BUKRS	4000	4000	OR	true
	 Copy Request 		FRANCE	France Market	BUKRS	BE11	BE11	OR	true
	 Request Audit Trail 		FRANCE	France Market	BUKRS	BE11	BE11	OR	true
	Reaffirm		FRANCE	France Market	EKORG	BE10	BE10	OR	true
L		Com	Cani						

Select Org Rule ID 'Corporate' to mitigate and click 'Continue'

Quick Reference Guide

Virsa Compliance Calibrator for SAP v5.2 "Organizational Rules and Organizational Level Reporting"

4. Click on 'Search' icon to search for existing mitigation control

Access Enforcer								
H H X	Mitigation							
Create Request	Assign Mitigation Control							
Search Request	Risk ID	P001						
Request On Hold	User Name	MWONG						
 Approver Delegation Copy Request 	Valid From*	09/14/2007						
Request Audit Trail	Valid To*	09/13/2008	-					
Reaffirm	Reference No*		9					
	Org Rules Assigned		- 4D					
	Org Rules*	CORPORATE;	٩					
	Functional Area*		1					
	Management Approver*]					
	Mitigation Monitor*	Select						
	Save Cancel Create							

5. Select Mitigation Control 'Corporate' and click 'Continue'

1											
	H H ×	Mitig	ation Controls								
	Request For Approval Oreste Request	Selec	t Controls								
	Search Request		Control ID	Description	Bussiness Unit	Management Approver					
	Request On Hold	۲	CORPORATE	Mitigating corporate shared services risks.	F100	MBOND					
	Approver Delegation Conv. Remuset	0	MC0001	F100	MBOND						
	Request Audit Trail	0	FI_0005	This mitigating control can be used across the enterprise related to Risks P001, P002 & P003. If there is a need to	F100	BRAMMARDS					
	 Reaffirm 										
		K	🖣 1/1 💌 🕨 🌶								
		Continue Cancel									



Virsa Compliance Calibrator for SAP v5.2 "Organizational Rules and Organizational Level Reporting"

6. Select Mitigation Monitor and click 'Save'

Access Enforcer									
K H X	Mitigation								
Create Request	Assign Mitigation Control								
Search Request	Risk ID	P001							
Request On Hold	User Name	MWONG							
Approver Delegation Copy Request	Valid From*	09/14/2007	-						
Copy Request Request Audit Trail	Valid To*	09/13/2008	-						
Reaffirm	Reference No*	CORPORATE	0						
	Org Rules Assigned								
	Org Rules*	CORPORATE:	0						
	Functional Area*	FI00							
	Management Approver*	MBOND	7						
	Mitigation Monitor*	JMURPHY 🔽							
	Save Cancel Create								

7. Org Rule 'Corporate' is mitigated for Risk P001. Click 'Continue'

нн ×	0,0		DOW			Y						
 Request For Approval 	Rol	es/Profi	les									
 Create Request Search Request 		System	Role/Profile Name		Туре	Role/Profile Desc	ription		Valid From	Valid To	Owner	Select SystemAction
 Request On Hold Approver Delegation 		DCM	O <u>vs::FLVM_MA</u>	INTENANCE	Ð	Vendor Master N	laintenance		09/13/2007 📑	12/31/9999 📑	Cyrus Perkins (CPERKINS)	ADD
Copy Request												
 Request Audit Trail 												
 Reaffirm 												
	5	mulate										
		Ri	sk Violation	Critic	al Tra	neaction						
				01100		modelion						
		Risk ID	Risk Des	cription		in Succion		Org Ru	les	Vi	iolation Count	Status
	Đ	Risk ID BSCT	Risk Des Basis Cr	cription itical Actions				Org Ru	les	V	iolation Count 2	Status
	÷	Risk ID BSCT HRMD	Risk Des Basis Cr HR Mast	cription itical Actions er Data				Org Ru	les	V	iolation Count 2 2	Status
	•	Risk ID BSCT HRMD P001	Risk Des Basis Cr HR Mast Create 1	cription itical Actions er Data ictitious vendor	andi	initiate payment to	the vendor	Org Ru	Ies IORATE;FRANCI	Vi E;	iolation Count 2 2 32	Status
	+	Risk ID BSCT HRMD P001 P002	Risk Des Basis Cr HR Mast Create Maintain	cription itical Actions er Data ictitious vendor a fictitious vend	and i dor ar	initiate payment to	the vendor nents to it	Org Ru	Ies 'ORATE;FRANCI	Vi E;	iolation Count 2 2 32 6	Status
	•	Risk ID BSCT HRMD P001 P002	Risk Des Basis Cr HR Mast Create 1 Maintain	cription itical Actions er Data ictitious vendor a fictitious vend	and i dor ar	initiate payment to nd direct disburser	the vendor nents to it	Org Ru	Ies P ORATE; FRANCI	Vi E;	olation Count 2 2 32 6	Status
		Risk ID BSCT HRMD P001 P002	Risk Des Basis Cr HR Mast Create 1 Maintain	cription filcal Actions er Data ictitious vendor a fictitious vendor	and i dor ar	initiate payment to	the vendor nents to it	Org Rul	IES 'ORATE;FRANCI	Vi E;	olation Count 2 2 32 6	Status
	+ + +	Risk ID BSCT HRMD P001 P002	Risk Des Basis Cr HR Mast Create 1 Maintain	ancel	and i	initiate payment to	the vendor nents to it	Org Rul	Ies 'ORATE;FRANCI	Vi E;	olation Count 2 2 32 6	Status

Quick Reference Guide

Virsa Compliance Calibrator for SAP v5.2 "Organizational Rules and Organizational Level Reporting"

8. Click on 'Risk Violations' tab. Result displays Org Rule 'Corporate' is mitigated.

Access Enforcer									
K N X	Request No. : 112								
Create Request	General Information								
Search Request	User Data			Request	or And Manager Da	ta			
Request On Hold	User	м	ae Wong(MWONG)	Requesto	or	Mae Wor	ng(MWONG)		
Approver Delegation Conv Request	Email	m	ae.wong@tdcdemomail.sap-ag.de	Email		mae.wor	ng@tdcdemomail	.sap-ag.de	
Copy Request Request Audit Trail	Telephone	+1	1 610 222 1123	Manager		Fox Wils	on(FVMLSON)		
Reaffirm	Company	ID	ES Hi-Tech	Email		fox.wils	on@tdcdemomail	.sap-ag.de	
- ricumin	Employee Type	/pe Permanent Employee Applications							
	Request Type		hange Account	Туре	Type Application Ca		ategory		
	Priority	н	HIGH More		SAP DCM		Production		
	Roles/Profiles	PD P	rofiles Risk Violations 🎘 Mitigat	ion 🔎 🛛 Co	mments Reques	t Justificatio	n Attachr	nents	
	System Type	System	Risk Description	I	Org Rules		Violation Count	Status	
	SAP	DCM	Basis Critical Actions				2	•	
	SAP	DCM	HR Master Data				2		
	SAP	DCM	Create fictitious vendor and initiate payme	nt to the vendor	CORPORATE;FRAN	CE;	32		
	SAP	DCM	Maintain a fictitious vendor and direct disk	R		6			

9. Click on 'Mitigation' tab. Result displays Org Rule 'Corporate' is mitigated by Mitigation Control ID 'Corporate'

4	Access Enforcer										
	N N ×	Reques	t No. : 112								
	Create Request	General	Information								
	Search Request	User Dat	ta				Reque	stor And Manag	jer Data		
	Request On Hold	User		Mae Wo	ng(MWONG)		Reque:	stor	Mae V\	ong(MWONG)	
	Approver Delegation	Email		mae.wo	ng@tdcdemomail.sa	o-ag.de	Email		mae.w	ong@tdcdemom	ail.sap-ag.de
	Copy Request	Telephor	e	+1 610	222 1123		Manag	er	Fox W	ilson(FWLSON)	
	Request Audit Trail	Company	/	IDES HI-	Tech		Email		fox.wi	lson@tdcdemom	ail.sap-ag.de
	• Reathrm	Employee	е Туре	Perman	ent Employee		Applic	ations			
		Request	Туре	Change	Account		Туре	Application	Category	<i>i</i>	
		Priority		HIGH	More		SAP	DCM	Productio	n	
		-									_
		Rol	les/Profiles	PD Profiles	Risk Violation	is 🎜 🛛 Mitigati	ion 🍋 📂	Comments R	equest Justificat	ion Attac	hments
		System	Risk Description	1	Org Rules	Contro	ol ID Fi	unctional Area	Approver	Valid From	Valid To
		DCM	Create fictitious initiate payment	s vendor and to the vendor	CORPORATE	CORF	PORATE F	100	MBOND	09/14/2007	09/13/2008



Virsa Compliance Calibrator for SAP v5.2

"Organizational Rules and Organizational Level Reporting"

ORGANIZATIONAL LEVEL REPORTING

Business Case

As part of the remediation phase, each organizational structure has individual owners who are responsible for reviewing segregation of duties in their areas. Therefore, they are requesting to separate the reports so that they only see users who have conflicts within their certain organizational structures.

Step 1: Schedule the Organization User Mapping job

1. This is the same job that is scheduled in Step 2 of the Organization Rule section above. This job must be scheduled in order to run Org level reporting.

Step 2: Run the Org Level Analysis

- 1. What this does is allow you to select users that have access to a specific organizational level and then run SoD analysis against this population.
- 2. In the example below, if you were to run this report, it would pull all users who have ANY access to BUKRS (company code 0001) and then run the normal SoD rules against them.
- 3. This access to company code 0001 might come via display roles or update roles.
- 4. This does NOT do any kind of org rule analysis, it just selects what individuals you want to run the report against.
- 5. Remember, this report won't just show conflicts that contain BUKRS, it will show all conflicts for users that have access to company code 0001 anywhere.

🗿 Compliance Calibrato	or - Microsoft Internet Ex	plorer			_ & ×
Ele Edit Vew Favorit	es <u>T</u> ools <u>H</u> elp				AT
😋 Back 🔻 🐑 👻 💌	😰 🏠 🔎 Search 👷	•Favorites 🕢 🍰 🦉 🕶 📒	🛍 🚳		
Address 🛃 http://idcivfd:	57700/webdynpro/dispatch	er/virsa/ccappcomp/ComplianceCalibrator			💌 🛃 Go 🛛 Links 🦉
SAP Virs	a Compliance C	alibrator Welcome J Monitor Configuration Debug	ayne Gibbon	Log Off About	
 Management View Risk Violations 	Risk Analysis - C	rg. Level			
Users Analysis Role Analysis Comparisons	System:	All 💌			
Alerts Rules Library	Analysis Type: Organizational Level:	Company code (B •			
Controls Library Risk Analysis User Level	Organizational Value:	0001 to:			
Role Level HR Objects	Risks by Process: *	All			
MIC Audit Reports	Risk ID:	to:	e C		
Security Reports Background Job	Rule Set:	GLOBAL D			
	Report Type:	Permission Level			
	Report Format:	summary ¥	More Options		
	Execute Simulation 6	ackground Reset Search Variant Sa	ave Variant		
8					
4					



Virsa Compliance Calibrator for SAP v5.2 "Organizational Rules and Organizational Level Reporting"

Copyright

© Copyright 2006 SAP AG. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors.

Microsoft, Windows, Outlook, and PowerPoint are registered trademarks of Microsoft Corporation.

IBM, DB2, DB2 Universal Database, OS/2, Parallel Sysplex, MVS/ESA, AIX, S/390, AS/400, OS/390, OS/400, iSeries, pSeries, zSeries, z/OS, AFP, Intelligent Miner, WebSphere, Netfinity, Tivoli, Informix, i5/OS, POWER, POWER5, OpenPower and PowerPC are trademarks or registered trademarks of IBM Corporation.

Adobe, the Adobe logo, Acrobat, PostScript, and Reader are either trademarks or registered trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Oracle is a registered trademark of Oracle Corporation.

UNIX, X/Open, OSF/1, and Motif are registered trademarks of the Open Group.

Citrix, ICA, Program Neighborhood, MetaFrame, WinFrame, VideoFrame, and MultiWin are trademarks or registered trademarks of Citrix Systems, Inc.

HTML, XML, XHTML and W3C are trademarks or registered trademarks of W3C[®], World Wide Web Consortium, Massachusetts Institute of Technology.

Java is a registered trademark of Sun Microsystems, Inc.

JavaScript is a registered trademark of Sun Microsystems, Inc., used under license for technology invented and implemented by Netscape.

MaxDB is a trademark of MySQL AB, Sweden.

SAP, R/3, mySAP, mySAP.com, xApps, xApp, SAP NetWeaver, and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world. All other product and service names mentioned are the trademarks of their respective companies. Data contained in this document serves informational purposes only. National product specifications may vary.

These materials are subject to change without notice. These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.