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.
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.
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.
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.

---

**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.
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.
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.
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.
5. Save the Organization Rule
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.
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.

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.**
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.
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.
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.
Below is the same report when this configuration option is set to “no” so that org rules are not included.
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.
When you create a mitigation control at the org rule level, this mitigation will NOT come over when you run normal risk analysis.
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.
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.
The URI for Org Rule Search URI must be completed. This URI can be found under the Web Services - VirsaCCOngRules5_3Service

1. Display of AE request with risk and org rule violations for Risk ID P001. Select Risk P001 and click ‘Mitigate’.
2. Click on ‘Search’ icon for Org Rules to search for Org rule to mitigate

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.
   Select Org Rule ID ‘Corporate’ to mitigate and click ‘Continue’
4. Click on 'Search' icon to search for existing mitigation control

5. Select Mitigation Control 'Corporate' and click 'Continue'
6. **Select Mitigation Monitor and click ‘Save’**

7. **Org Rule ‘Corporate’ is mitigated for Risk P001. Click ‘Continue’**
8. Click on 'Risk Violations' tab. Result displays Org Rule ‘Corporate’ is mitigated.

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