Job Aid 14 Role Level

**USE**

This report can be used analyze for risk violations at the role level.

**INFORMATION**

SODs, critical actions or permissions.

**RELATED PROCESSES**

* Process 1: New or Amended Roles
* Process 2: Mitigation Analysis

**SPECIFIC SCENARIOS**

* N/A

| Step | Description | Screenshot |
| --- | --- | --- |
| 1 | Navigate to the ‘Access Management’ tab. |  |
| 2 | Click on the ‘Role Level’ report located in the ‘Access Risk Analysis’ section. |  |
| 3 | In the ‘Analysis Criteria’ section, select the System for which information is required. Since the desired selection is PS1 (Production), ‘\*PS1\*’ was typed in as the system.  The search option can also be used to search for the correct system. Please refer to the ‘Search for Input Values’ reference document (R3) for further information. |  |
| 4 | Analysis for a single techinical role.  In the ‘Analysis Criteria’ section, click on the ‘-‘ at the end of the ‘Risk by Process’ row to remove the row for that search criterion; this criterion is not needed for this scenario. |  |
| 5 | Add the Role. In this case, ‘Z\_VPF\_S\_AR\_GENERAL’ was typed in. The search option can also be used to search for a role. Please refer to the ‘Search for Input Values’ reference document (R3) for further information. |  |
| 6 | In the ‘Report Options’ section, select the first drop down for ‘Format’ and select the level of detail at which information is required. In this case, ‘Detail’ was selected so that the report will show information about why Risks exists. |  |
| 7 | In the ‘Report Options’ section, select the second drop down for ‘Format’ and select the type of information that is required. In this case, ‘Technical View’ was selected so that the report will show technical information about why Risks exists. |  |
| 8 | Analyze for SODs based on user ID.  In the ‘Report Options’ section, select the first dial button for ‘Access Risk Analysis’. Next, select the type of analysis that is required. The options available are:  Action Level: SODs at the transaction level (will include false positives eliminated at the authorization level)  Permission Level: SODs at the authorization level  Critical Action: Critical transactions that limited/no users should have  Critical Permission: Critical authorizations that limited/no users should have  Critical Role/Profile: Critical Roles/Profiles that limited/no users should have  In this case, ‘Permission Level’ was selected so that the report will show SODs that exist at the Permission Level. |  |
| 9 | In the ‘Report Options’ section, check ‘Show All Objects’ under ‘Additional Criteria’. This will ensure that Users with no violations are explicitly listed as such (i.e. ‘No Violations’ will be listed as a line item for such users’ IDs). |  |
| 10 | Run the report in the foreground. If the report is expected to yield a large amount of data, execute the report by running a background job. See the ‘Execute a Background Job’ reference document (R5) for further information. |  |
| 11 | Analyze the data. This data can also be exported. See the ‘Export Data from GRC’ reference document (R8) for further information.  Role Name: SAP role name  Access Risk ID: The 4-digit ID representing each medium-risk (as defined in the standard rule set) for which violations exist  Rule ID: The ID representing the particular rule that was triggered for that Risk  Risk Level: The risk level defined for each Access Risk in the standard rule set  Function: The ID representing the particular function that was triggered  System: The system in which the role is assigned to the user  Action: SAP transaction  Resource: SAP authorization object  Resource Extn: SAP authorization object field  Value From: SAP authorization object field value (start value for a range)  Value To: SAP authorization object field value (end value for a range)  Role/Profile: The single role/profile causing the SOD  Composite Role: The composite role containing the SOD-causing single role (if any exist)  Control: The 10-digit ID representing the Mitigating Control applied for the User with the Access Risk  Monitor: The user ID of the Monitor responsible for the Mitigating Control |  |