Job Aid 13 User Level Simulation

**USE**

This report can be used carry out simulations at the user level for the purpose of understanding whether the addition or removal of certain access either creates or eliminates SODs and other risks.

**INFORMATION**

New risk violations that will result due to changes to user access.

**RELATED PROCESSES**

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

**SPECIFIC SCENARIOS**

* Step 15A: Simulation by Action (transaction).
* Step 15B: Simulation by Role.
* Step 15C: Simulation by Profile.

| Step | Description | Screenshot |
| --- | --- | --- |
| 1 | Navigate to the ‘Access Management’ tab. |  |
| 2 | Click on the ‘User Level Simulation’ 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 | Run a simulation for a single User.  In the ‘Analysis Criteria’ section, click on the ‘-‘ at the end of the ‘User Group’ row to remove the row for that search criterion; this criterion is not needed for this scenario. |  |
| 5 | In the ‘Analysis Criteria’ section, click on the ‘-‘ at the end of the ‘Custom Group’ row to remove the row for that search criterion; this criterion is not needed for this scenario. |  |
| 6 | Add the user ID. In this case, ‘ANNAK’ was typed in. The search option can also be used to search for an ID. Please refer to the ‘Search for Input Values’ reference document (R3) for further information. |  |
| 7 | In the ‘Analysis Criteria’ section, select the ‘Risk Level’ drop down and select the risk level for which information is required. In this case, ‘All’ was selected so that the report evaluates for all risk levels. |  |
| 8 | In the ‘Analysis Criteria’ section, select the ‘Rule Set’ drop down and select the Rule Set against which the report should be executed. In this case, ‘Global’, the MIT Rule Set, was selected. Unless advised otherwise, the selection should always be ‘Global’ for this report. |  |
| 9 | In the ‘Analysis Criteria’ section, select the User Type’ drop down and select the type of users for which information is required. In this case, ‘Dialog’ was selected so that the report only evaluates for dialog users. |  |
| 10 | 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. |  |
| 11 | 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. |  |
| 12 | 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). |  |
| 13 | Analyze for SODs (excluding false positives).  In the ‘Report Options’ section, select the 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. |  |
| 14 | The analysis criteria has now been defined. Click on ‘Next’ to define the simulation criteria. |  |
| 15A-1 | Simulation by Action (transaction).  On the ‘Actions’ tab, click on ‘Add’ to define transaction simulation criteria. |  |
| 15A-2 | Click the drop down on the ‘System’ field and select the system from which a transaction must be added. The user for the simulation exists in PS1; however, the simulation criteria can be from any system connected to GRC. In this case, PS1 is selected. |  |
| 15A-3 | Add the transaction. In this case, ‘PT60’ was typed in. The search option can also be used to search for an Action. Please refer to the ‘Search for Input Values’ reference document (R3) for further information.  NOTE: If transactions should be excluded from the User’s authorization for the simulation, the ‘Exclude Values’ box must be checked. Otherwise, any added transactions will be added to the User’s authorizations for the simulation. |  |
| 15A-4 | 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. |  |
| 15A-5 | Analyze the data. This data can also be exported. See the ‘Export Data from GRC’ reference document (R8) for further information.  Any orange line items represent risks occuring due to simulation criteria.  User ID: User ID of the user with a Risk that has been mitigated  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  Last Executed On: Date of last execution of transaction  Execution Count: Number of times transaction was executed for a specified time period  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 |  |
| 15B-1 | Simulation by Role.  On the ‘Roles’ tab, click on ‘Add’ to define role simulation criteria. |  |
| 15B-2 | Click the drop down on the ‘Role Type’ field and select ‘Technical Role’. For role-based simulation criteria, unless otherwise advised, the selection will always be ‘Technical Role’. |  |
| 15B-3 | Click the drop down on the ‘System’ field and select the system from which a technical role must be added. The user for the simulation exists in PS1; however, the simulation criteria can be from any system connected to GRC. In this case, PS1 is selected. |  |
| 15B-4 | 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.  NOTE: If roles should be excluded from the User’s authorization for the simulation, the ‘Exclude Values’ box must be checked. Otherwise, any added roles will be added to the User’s authorizations for the simulation. |  |
| 15B-5 | 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. |  |
| 15B-6 | Analyze the data. This data can also be exported. See the ‘Export Data from GRC’ reference document (R8) for further information.  Any orange line items represent risks occuring due to simulation criteria.  User ID: User ID of the user with a Risk that has been mitigated  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  Last Executed On: Date of last execution of transaction  Execution Count: Number of times transaction was executed for a specified time period  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 |  |
| 15C-1 | Simulation by Profile.  On the ‘Profiles’ tab, click on ‘Add’ to define profile simulation criteria. |  |
| 15C-2 | Click the drop down on the ‘System’ field and select the system from which a profile must be added. The user for the simulation exists in PS1; however, the simulation criteria can be from any system connected to GRC. In this case, PS1 is selected. |  |
| 15C-3 | Add the profile. In this case, ‘Z#DP:JV\_FY’ was typed in. The search option can also be used to search for a Profile. Please refer to the ‘Search for Input Values’ reference document (R3) for further information.  NOTE: If profiles should be excluded from the User’s authorization for the simulation, the ‘Exclude Values’ box must be checked. Otherwise, any added profiles will be added to the User’s authorizations for the simulation. |  |
| 15C-4 | 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. |  |
| 15C-5 | Analyze the data. This data can also be exported. See the ‘Export Data from GRC’ reference document (R8) for further information.  Any orange line items represent risks occuring due to simulation criteria.  User ID: User ID of the user with a Risk that has been mitigated  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  Last Executed On: Date of last execution of transaction  Execution Count: Number of times transaction was executed for a specified time period  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 |  |