Job Aid 12 User Level

**USE**

This report can be used analyze for risk violations at the user level. The report can also be used to find the mitigating controls assigned to users, as well as any invalid mitigating control assignments.

**INFORMATION**

SODs, critical actions or permissions and critical roles or profiles.

**RELATED PROCESSES**

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

**SPECIFIC SCENARIOS**

* Step 10A: Analyze for SODs based on User ID.
* Step 10B: Analyze for SODs based on User Group.
* Step 10C: Analyze for SODs based on Custom Group.
* Step 10D: Carry out an Access Risk Assessment by User ID.
* Step 10E: Carry out an analysis of Mitigating Controls by User ID.

| Step | Description | Screenshot |
| --- | --- | --- |
| 1 | Navigate to the ‘Access Management’ tab. |  |
| 2 | Click on the ‘User 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 | 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. |  |
| 5 | 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. |  |
| 6 | 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. |  |
| 7 | 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. |  |
| 8 | 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. |  |
| 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). |  |
| 10A-1 | 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. |  |
| 10A-2 | 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. |  |
| 10A-3 | 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. |  |
| 10A-4 | 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. |  |
| 10A-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. |  |
| 10A-6 | Analyze the data. This data can also be exported. See the ‘Export Data from GRC’ reference document (R8) for further information.  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 |  |
| 10A-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. |  |
| 10A-8 | 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. |  |
| 10A-9 | Analyze the data. This data can also be exported. See the ‘Export Data from GRC’ reference document (R8) for further information.  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 |  |
| 10A-10 | Click on the ‘+‘ at the end of the ‘User’ row to add an additional user ID search criterion row for each ID. In this case, one additional row is added; thus, we can analyze for a total of two user IDs. |  |
| 10A-11 | Add the additional user ID. In this case, ‘ANNAK’ was entered previously and ‘MFLAHERT’ was then typed in as an additional ID. The search option can also be used to search for IDs. Please refer to the ‘Search for Input Values’ reference document (R3) for further information. |  |
| 10A-12 | 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. |  |
| 10A-13 | Analyze the data. This data can also be exported. See the ‘Export Data from GRC’ reference document (R8) for further information.  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 |  |
| 10B-1 | Analyze for SODs based on user group.  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. |  |
| 10B-2 | In the ‘Analysis Criteria’ section, click on the ‘-‘ at the end of the ‘User’ row to remove the row for that search criterion; this criterion is not needed for this scenario. |  |
| 10B-3 | 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. |  |
| 10B-4 | Add the user group name. In this case, ‘VPF-TAX’, the user group containing all users in VPF who are part of the Tax area, was typed in. The search option can also be used to search for user groups. Please refer to the ‘Search for Input Values’ reference document (R3) for further information. |  |
| 10B-5 | Run the report in the foreground. |  |
| 10B-6 | You may receive a message stating that running the report in the foreground “could take much time and system resources usage” and asking, “Do you want to continue?”  If the report is expected to yield a large amount of data, click on ‘Cancel’ and execute the report by running a background job. See the ‘Execute a Background Job’ reference document (R5) for further information.  Otherwise, click ‘OK’ to continue. |  |
| 10B-7 | Analyze the data. This data can also be exported. See the ‘Export Data from GRC’ reference document (R8) for further information.  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 |  |
| 10C-1 | Analyze for SODs based on Custom Group.  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. |  |
| 10C-2 | In the ‘Analysis Criteria’ section, click on the ‘-‘ at the end of the ‘User’ row to remove the row for that search criterion; this criterion is not needed for this scenario. |  |
| 10C-3 | 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. |  |
| 10C-4 | Add the custom group name. In this case, ‘VPF’, the custom group containing all users in VPF, was typed in. The search option can also be used to search for custom groups. Please refer to the ‘Search for Input Values’ reference document (R3) for further information. |  |
| 10C-5 | Run the report in the foreground. |  |
| 10C-6 | You may receive a message stating that running the report in the foreground “could take much time and system resources usage” and asking, “Do you want to continue?”  If the report is expected to yield a large amount of data, click on ‘Cancel’ and execute the report by running a background job. See the ‘Execute a Background Job’ reference document (R5) for further information.  Otherwise, click ‘OK’ to continue. |  |
| 10C-7 | Analyze the data. This data can also be exported. See the ‘Export Data from GRC’ reference document (R8) for further information.  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 |  |
| 10D-1 | Carry out an Access Risk Assessment by user ID.  In the ‘Report Options’ section, select the second dial button for ‘Access Risk Assessment’. |  |
| 10D-2 | 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. |  |
| 10D-3 | 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. |  |
| 10D-4 | 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. |  |
| 10D-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. |  |
| 10D-6 | Analyze the data. This data can also be exported. See the ‘Export Data from GRC’ reference document (R8) for further information.  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  System: The system in which the user has the risk  Short Description: The risk level defined for each Access Risk in the standard rule set |  |
| 10E-1 | Carry out an analysis of Mitigating Controls by user ID.  In the ‘Report Options’ section, select the third dial button for ‘Mitigation Analysis’. |  |
| 10E-2 | In the ‘Report Options’ section, select the drop down for ‘Mitigation Analysis’ and select the type of information that is required. The options available are:  Mitigating Controls: Information on all Mitigating Controls assignments  Invalid Mitigating Controls: Information on all invalid Mitigating Control assignments  In this case, ‘Invalid Mitigating Controls’ was selected. |  |
| 10E-3 | 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. |  |
| 10E-4 | 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. |  |
| 10E-5 | 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. |  |
| 10E-6 | 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. |  |
| 10E-7 | Analyze the data. This data can also be exported. See the ‘Export Data from GRC’ reference document (R8) for further information.  User ID: User ID of the user with a Risk that has been mitigated  System: The system in which the user has the risk  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  Control: The 10-digit ID representing the Mitigating Control applied for the User with the Access Risk  Valid From: Date on which assignment of the control to the user begins  Valid To: Date on which assignment of the control to the user ends  Monitor: The user ID of the Monitor responsible for the Mitigating Control |  |