Job Aid 02 User Analysis

**USE**

This report can be used to gain insight into MIT’s overall exposure to risk. The report provides an overview of user violations across all MIT ECC systems.

**INFORMATION**

Risk count by risk type and user.

**RELATED PROCESSES**

* Process 5: Periodic Compliance Reviews

**SPECIFIC SCENARIOS**

* Step 13A: Analyze report data by Mitigated Users. (Pie Chart)
* Step 13B: Analyze report data by Risk Level. (Pie Chart)
* Step 13C: Analyze report data by Critical Actions, Roles and Profiles. (Bar Graph)

| Step | Description | Screenshot |
| --- | --- | --- |
| 1 | Navigate to the ‘Reports and Analytics’ tab. |  |
| 2 | Click on the ‘User Analysis’ report located in the ‘Access Dashboards’ section. |  |
| 3 | The report will show risk violations and critical actions, roles and profiles information for the latest period, across all systems (to which GRC is connected) and user groups, at the user level. The violation count will be given by permission (i.e. each instance of a violation will be counted, even if it is a repeated violation for a user).  The ‘Critical Actions and Roles’ section will state the number of each that were evaluated for the selected user group.  The report data must be appropriately filtered to provide information that can be of use to MIT. |  |
| 4 | In the report filters section, click on the drop down for ‘Year/Month’ to select the time period for which data is required. In this case, ‘2013/05’ is selected. |  |
| 5 | In the report filters section, select the System for which information is required. Click on the Search icon next to ‘System’. Since the desired selection is PS1 (Production), select the Connector for PS1; if necessary, ‘\*PS1\*’ can be used as search criteria to find the correct connector for PS1. Click on ‘OK’. |  |
| 6 | In the report filters section, select the user group for which information is required. Click on the Search icon next to ‘User Group’.  Enter search criteria to search for the desired user group. In this case, ‘VPF-T\*’ is entered to search for all VPF user groups starting with ‘T’.  Click on ‘Start Search’. Select the desired user group from the search results. In this case, ‘VPF-TAX’ is selected.  Click on ‘OK’. |  |
| 7 | In the report filters section, click on the drop down for ‘Violation Count by’ to select the count methodology required for the report. In this case, ‘Access Risk’ is selected to count unique violations per User. |  |
| 8 | Click on ‘Go’ to execute the report based on the criteria that have been defined. |  |
| 9 | The report shows that there are a total of 4 Users in the ‘VPF-TAX’ user group. The report also shows that these 4 Users all have mitigated violations.  In the ‘Critical Actions and Roles’ section, the report shows:   * 4 Users were analyzed * The users were evaluated for violations against 775 Critical Actions and 1 Critical Role/Profile * 0 VPF-TAX Users have Critical Actions * 0 VPF-TAX Users have Critical Roles/Profiles |  |
| 10 | In the report filters section, select another user group for which information is required. Click on the Search icon next to ‘User Group’.  Enter search criteria to search for the desired user group. In this case, ‘VPF-T\*’ is entered to search for all VPF user groups starting with ‘T’.  Click on ‘Start Search’. Select the desired user group from the search results. In this case, ‘VPF-TRAVEL’ is selected.  Click on ‘OK’. |  |
| 11 | Click on ‘Go’ to execute the report based on the updated criteria that have been defined. |  |
| 12 | The report shows that there are a total of 8 Users in the ‘VPF-TRAVEL’ user group. The report also shows that these 8 Users have 11 mitigations, as well as 11 instances (9 High Risk + 2 Medium Risk) of Users with unmitigated violations.  NOTE: Each type of Violation – SOD, Critical Transaction, etc. – is counted only once per User. Thus, a User with only 2 SOD, contributes 1 to the violation count. And a User with 1 SOD and 1 Critical Action, contributes 2 to the violation count.  In the ‘Critical Actions and Roles’ section, the report shows:   * 8 users were analyzed * The users were evaluated for violations against 775 Critical Actions and 1 Critical Role/Profile * 8 VPF-TRAVEL users have Critical Actions * 0 VPF-TRAVEL users have Critical Roles/Profiles |  |
| 13A-1 | Analyze report data by mitigated users.  Scroll over the different pieces of the pie chart to see information about mitigated violations as well as unmitigated violations at different risk levels.  Click on the ‘Mitigated Users’ piece of the pie chart for more information about VPF-TRAVEL users that have Mitigated Risks. |  |
| 13A-2 | 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  User Name: User name associated with the user ID  User Group: User group code  Access Risk ID: The 4-digit ID representing each medium-risk (as defined in the standard rule set) for which violations exist  Risk Description: Business description of the Access Risk  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 |  |
| 13B-1 | Analyze report data by risk level.  Click on the ‘High’ risks piece of the pie chart for more information about VPF-TRAVEL Users that have high risk level risks. |  |
| 13B-2 | 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  User Name: User name associated with the user ID  User Group: User group code  Access Risk ID: The 4-digit ID representing each medium-risk (as defined in the standard rule set) for which violations exist  Risk Description: Business description of the Access Risk  Business Process: The 4-digit ID representing the Business Process to which the Access Risk has been mapped in the standard rule set  Business Process Description: The business description for the Business Process to which the Access Risk has been mapped in the standard rule set |  |
| 13C-1 | Analyze report data by Critical Actions, Roles and Profiles.  Scroll over the different bars of the Bar Graph to see information about Critical Actions and Critical Roles/Profiles.  Click on the ‘Critical Actions’ bar of the Graph for more information about Critical Actions violations. |  |
| 13C-2 | 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  User Name: User name associated with the user ID  User Group: User group code  Access Risk ID: The 4-digit ID representing each medium-risk (as defined in the standard rule set) for which violations exist  Risk Description: Business description of the Access Risk |  |