Job Aid 01 Risk Violations

**USE**

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

**INFORMATION**

Risk count by risk level and process.

**RELATED PROCESSES**

* Process 5: Periodic Compliance Reviews

**SPECIFIC SCENARIOS**

* Step 14A: Analyze report data by Risk Level. (Pie Chart)
* Step 14B: Analyze report data by Business Process. (Table)
* Step 14C: Analyze report data by Business Process. (Bar Graph)

| Step | Description | Screenshot |
| --- | --- | --- |
| 1 | Navigate to the ‘Reports and Analytics’ tab. |  |
| 2 | Click on the ‘Risk Violations’ report located in the ‘Access Dashboards’ section. |  |
| 3 | The report will show risk violations information for the latest period, across all systems (to which GRC is connected) and user groups, at the user level. The 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 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. Click on ‘OK’. |  |
| 6 | In the report filters section, click on the drop down for ‘Analysis Type’ to select the security object (user, role or profile) for which data is required. In this case, ‘User’ is selected. |  |
| 7 | 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’. |  |
| 8 | 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. |  |
| 9 | Click on ‘Go’ to execute the report based on the criteria that have been defined. |  |
| 10 | 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 have 0 unmitigated violations. No pie chart, business process table, or business process bar graph are shown due to the fact that the violation count is 0. |  |
| 11 | 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’. |  |
| 12 | Click on ‘Go’ to execute the report based on the updated criteria that have been defined. |  |
| 13 | 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 12 unmitigated violations.  The graphic displays are populated based on information regarding the 12 unmitigated violations.  The User Level analysis report (12), reports that:   * 8 users have unimitigated Basis Critical Transactions * 2 users have unmitigated Finance SODs * 2 users have unmitigated Procure to Pay SODs |  |
| 14A-1 | Analyze report data by risk level.  Scroll over the different pieces of the pie chart to see information about unmitigated violations at each risk level.  Click on the ‘Medium’ risk level piece of the pie chart for more information about medium risks. |  |
| 14A-2 | Analyze the data. This data can also be exported. See the ‘Export Data from GRC’ reference document (R8) for further information.  Access Risk: The 4-digit ID representing each medium-risk (as defined in the standard rule set) for which violations exist  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  No. of Violations: The number of violations for each Access Risk that exist |  |
| 14A-3 | Click on the ‘No. of Violations’ link for each Access Risk to view the Users that have violations for that Risk. In this case, clicking on ‘1’ for Access Risk ‘F028’ shows the 7 VPF-TRAVEL Users that have related violations. |  |
| 14B-1 | Analyze report data by Business Process.  Scroll over the different line items of the Business Process Table to see information about unmitigated violations for each Business Process.  Click on the ‘Finance’ risk level row of the Table for more information about Finance Risks. |  |
| 14B-2 | Analyze the data. This data can also be exported. See the ‘Export Data from GRC’ reference document (R8) for further information.  Access Risk: The 4-digit ID representing each Finance-Risk (as defined in the standard rule set) for which violations exist  Description: Business description of the Access Risk  Risk Level: The risk level defined for each Access Risk in the standard rule set  No. of Violations: The number of violations for each Access Risk that exist |  |
| 14C-1 | Analyze report data by Business Process.  Scroll over the different bars of the Business Process Bar Graph to see information about unmitigated violations for each Business Process.  Click on the ‘BS00’ Risk bar of the Graph for more information about Basis Risks. |  |
| 14C-2 | Analyze the data. This data can also be exported. See the ‘Export Data from GRC’ reference document (R8) for further information.  Access Risk: The 4-digit ID representing each Basis-Risk (as defined in the standard rule set) for which violations exist  Description: Business description of the Access Risk  Risk Level: The risk level defined for each Access Risk in the standard rule set  No. of Violations: The number of violations for each Access Risk that exist |  |