Job Aid 11 Mitigation Control Report

**USE**

This report can be used to find information on the mitigating controls defined in GRC.

**INFORMATION**

Approvers, monitors and risks mitigated by a mitigating control as defined in the system.

**RELATED PROCESSES**

* Process 2: Mitigation Analysis

**SPECIFIC SCENARIOS**

* N/A

| Step | Description | Screenshot |
| --- | --- | --- |
| 1 | Navigate to the ‘Reports and Analytics’ tab. |  |
| 2 | Click on the ‘Mitigation Control Report’ report located in the ‘Access Risk Analysis Reports’ section. |  |
| 3 | Add the Mitigating Control ID. In this case, ‘MC\*TAX\*’was typed in to include all Mitigating Controls for the VPF-TAX area. The search option can also be used to search for a specific ID. Please refer to the ‘Search for Input Values’ reference document (R3) for further information. |  |
| 4 | Click on the ‘-‘ at the end of the ‘Short Description’ row to remove the row for that search criterion; this criterion can be used with wild cards (\*) for scenarios where information is only required for Mitigating Controls relating to some specific criteria noted in the short description. |  |
| 5 | Click on the ‘-‘ at the end of the ‘Access Risk ID’ row to remove the row for the Access Risk search criterion; this criterion can be used for scenarios where information is only required for Mitigating Controls relating to specific Access Risks. |  |
| 6 | Click on the ‘-‘ at the end of the ‘Organization ID’ row to remove the row for the Organization search criterion; this criterion can be used for scenarios where information is only required for Mitigating Controls mapped to a certain Organization in the Organizational Structure defined in GRC. At this initial phase, this criterion will likely not be of use to MIT. |  |
| 7 | 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. |  |
| 8 | Analyze the data. This data can also be exported. See the ‘Export Data from GRC’ reference document (R8) for further information.  Control ID: The 10-digit ID representing the Mitigating Control applied for the User with the Access Risk  Control Description: Business description of the Mitigating Control  Org Unit ID: Numerical code of Org Unit defined in GRC  OrgUnit Description: Business name of Org Unit  Approver: The user ID of the Approver responsible for the Mitigating Control  Monitor: The user ID of the Monitor responsible for the Mitigating Control  Name: Name tied to the user ID of the Monitor  Access Risk ID: The 4-digit ID representing each medium-risk (as defined in the standard rule set) for which violations exist  Access Risk Description: Business description of the Access Risk  System: The system in which the role is assigned to the user  Access Risk Level: The risk level defined for each Access Risk in the standard rule set |  |