HOW-TO Use SAP SUIM OR RSUSR008_009_NEW to Analysing Critical Authorisations

Leon Ye

Contents
Preface ................................................................................................................................. 2
Access the Program ............................................................................................................... 2
Analysing Users with Critical Authorisations .................................................................. 3
  Defining Critical Authorisations .................................................................................. 3
  Create a variant ............................................................................................................. 7
  Execute the report variant with critical authorisations .............................................. 8
Preface

SAP upgraded SUIM (User Information System) which runs program RSUSR008_009_NEW as of SAP Web AS 6.20 with the following Support Packages:

- SAP Web AS 6.20, as of SAPKB62039
- SAP Web AS 6.40, as of SAPKB64003

Access the Program

Transaction **SUIM**
Choose **User**

With Critical Authorisations

OR, Use transaction **SA38**
Use Program **RSUSR008_009_NEW**.
Both brings the following screen up
Analysing Users with Critical Authorisations

You need first define critical authorisations and then combine the critical authorisations into a variant then you run the variant.

Defining Critical Authorisations

Choose on the initial screen.

A dialog box appears:

On the left side Dialog Structure it displays four folders, which form two hierarchies:

- Variants for Critical Authorisations → Critical Authorisations
- Critical Authorisation → Authorisation Data

Double click the Critical Authorisation folder and choose

Then you can enter the Critical Authorisation IDs or copy from a spread-sheet (see the user contributed documentation under ISACA SAP topic). The following screen is based on the copied information from the SAP Critical Authorisations. Please note that the colour draw down can only be manually chosen one by one.
Save your entries.

Double click the **Authorisation Data** folder.
A new view appears.

Choose **New Entries**.

- Fill out all required fields, with an asterisk (*).
  
  Note the following when filling out the fields:
  
  - All entries within a group must have the same operand AND or OR. The individual groups are essentially linked with AND. An OR link is not
allowed (error messages will be shown when you run the variant later. You can fix any errors then).

- You can specify critical data for different authorisation objects within the same group.
- If you specify a transaction code for an ID, all authorisation data required to execute the transaction and maintained in transaction SE93 is automatically entered as critical data, after you have confirmed and saved the dialog box.
- If you leave the From field empty, the program searches for authorisations with spaces " " for the specified field and object.
- If you enter an asterisk (*) in the From field, the report searches for full authorisation for the specified field.
- Any errors in the Authorisation Object fields will be picked up as it will not allow you to enter an object or value it does not exist, but for Transactions the system cannot prevent you to put in a non-exist TCODE.
- Individual entries cannot be put into the change request, has to be put in as NEW ENTRIES.

Example of ZSOS0002
The example above was copied from the spreadsheet:

Save your entries.
Create a variant.

Open the folder **Variants for Critical Authorizations**, and then choose **New Entries**.

Enter the name and description of the variant.

Enter or copy the Authorisation ID and Text into the New Entries

The above IDs were copied from:
Save your entries.

**Execute the report variant with critical authorisations.**

On the initial screen of the report
Choose **For Critical Authorisations**

Use the input help to select an existing variant, and choose *Execute*.

You can also define a report variant, for example, the above screen shot shows the user group excluded TERMINATED and other user groups which may not be relevant to your analysis.
You can use SUIM or report RSUSR008_009_NEW to combine the IDs for critical authorisations in any way, and to create variants with these combinations, for example for segregation of duties purposes.

Samples segregation of duties for business cycles and system securities will be published next year.

Relevant documents already published on ISACA SAP Topic include

- How-to SAP Security Optimisation Self-service
- SAP SOS Sample Report
- SAP Critical Authorisations