Enhancement for table access control: S_TABU_NAM

Given the high criticality and increasing complexity related to table access – SAP® has introduced a new authorization object for a more refined table access control.
The authorization object **S_TABU_NAM** was introduced last year. This authorization object consists of two fields **ACTVT** (Activity) and **TABNAME** (name of table or view).
This concept is valid for generic table access through transactions like **SE16**, **SE16N**, **SE17**, **SM30**, **SM31**, **SM34** as well as generic function modules (e.g. **RFC_READ_TABLE**)

The authority-check was integrated in the function module **VIEW_AUTHORITY_CHECK** as per Release 7x with corresponding Support Packages (Please refer to OSS Notes 141950 and 1434284 for more details).

To make sure the new object is downwards compatible with the previous checks on **S_TABU_DIS** and **S_TABU_CLI** where applicable; the check will only be performed if the check on **S_TABU_DIS** was **not** successful.

Details of check sequence

1. Check on **S_TABU_DIS** with **ACTVT** (Activity) and **DICBERCLS** (Table authorization group). If no authorization group is maintained in **TDDAT**, the check will be performed for **&NC&** (Non-Classified).

2. If this check ***fails***, the corresponding authorization on **S_TABU_NAM** will be checked.

3. If this check fails, the system will terminate with the message "*No Authority*".

4. In case a cross-client table is called for maintenance, the system will perform an additional check on **S_TABU_CLI**.

5. If the line based authority-check on **S_TABU_LIN** is implemented, then this will be checked as a final step.

! Note

If you want to utilize the new object to restrict table access to a particular table or view you have to make sure that no authorization on **S_TABU_DIS** with the corresponding table authorization group is granted. The group access would always overhaul the individual restriction.

Tools

The user information system with the reports **RSUSR002** or **RSUSR070** e.g. does currently not allow checking the logical sequence of **S_TABU_DIS** and **S_TABU_NAM** directly. Therefore report **RSUSR008_009_NEW** can be utilized.

SAP® has provided some tools to help to convert to the newly integrated check.
The report **SUSR_TABLES_WITH_AUTH** will help to determine generic table access for users or single roles.
The transaction **SU24_TABU_NAM** will help to identify parameter transactions, the correct table name as well as the related activity, and allow converting the entries and finally adapting the affected roles.
Please also pay attention to OSS Notes 1500054, 1503975, 1434284.

The integration of the new concept into *GRC – Risk Analysis and Remediation* is described in OSS Note 1541577.