Security Analysis in Custom Transactions

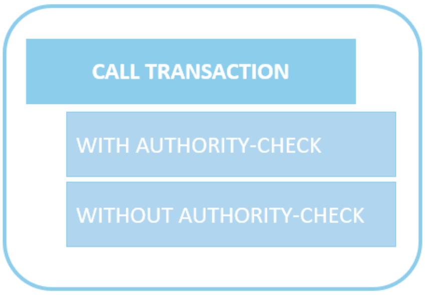
Custom Transactions in SAP environment is a difficult topic when we are talking about Security. There are several reasons behind this statement:

- The Budget regarding the Development of the Custom Transaction is funded by the Business to comply with Business Requirement. Therefore, nothing related to Security as to be considered.
- The Security Analysis usually requires changes into the program code like adding authorization object, changing the CALL TRANSACTION procedure ...
- The person that is behind the development of the Custom Transaction usually does not have knowledge regarding Security principles.
- Several Times, the Custom Transaction is developed using another Transactions as a base (even we found some Transactions that were having other Customer Name instead of the one that requested the development of the Custom Transaction).

So based in the previous points, the Security Analysis of Custom Codes is something that most of the time is not in place in many SAP Customers. For sure, it takes a lot of effort to include a Security Analysis inside the Change of Management Process of an Organization, however it is most cost efficiently to do it now than wait for the near future. This statement is similar to the one that is being used when we talk about changing the SAP Role Model. It is better to start with a SAP Role Model that is following the SAP Best Practices regarding SAP Security than, start with a Role Model that does not comply with them and change it in a couple of years affecting all the SAP Users. When you enhance a Custom Transaction that did not have Authorization Objects, and you add some, you need to ensure that all the Users that currently executes that Transaction is having those new Authorization Objects inside the Roles that they are currently assigned. If the Transactions is having multiples functionally the scenario is much more complex. During this article we will be covering the Key Topics that are part of a Security Analysis in Custom Transaction.

CALL TRANSACTION

The usage of the Function of CALL TRANSACTION when developing SAP Custom Transaction is frequent. This function allows to call an existing Transaction as part of the Program Code, however there are two strategies to perform this call:



Most of the times, the recommendation will be to use the one that requires the authorization objects of the Transaction that is being called (WITH AUTHORITY-CHECK), however if the Custom Transaction purpose is to restrict the functionality of the existing Transaction that is being called, the recommendation will be to perform the call WITHOUT AUTHORITY-CHECK. This is because if you add the requirement of having the authorization objects (of the existing Transaction that is being called), at the end, the User will have the full access to the existing transaction and the restriction that you were trying to apply by the custom transaction will be skipped by the usage of the existing one. As an Example:

- **Transaction Z1 which limits the information of the Material Master Data calls MM01. Since the User requires access to MM01 because of the call from the Transaction Z1**(WITH AUTHORITY-CHECK)**, the User will still have the access to the MM01 Transaction which will surpass the limitation of the Z1 Transaction that you want to apply.**

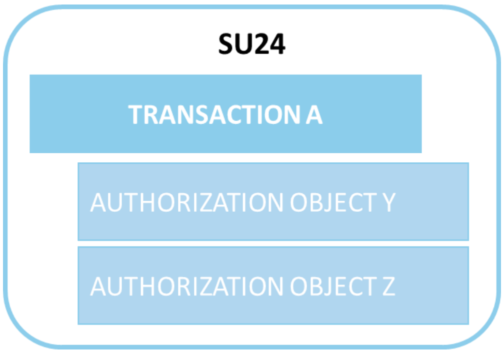
AUTHORIZATION OBJECT

The different authorization objects that exists in SAP are related with different functions therefore it is recommended to select the appropriate authorization object based on the functionality of the Custom Transaction. As an example, we found several times that the authorization object “F_BKPF_BUK” is included in Custom Transactions to restrict the organizational values based in Company Codes, even the functionality of the Transaction is not related with Accounting Documents. Therefore, it is important to state that Authorization Objects are not only applicable for Organizational Values restriction but also for Functionality restriction. Furthermore, the authorization object “F_BKPB_BUK” is a critical authorization object that is being included in several functions inside the SAP Standard Risk Matrix therefore if you use this authorization frequently you will probably increase the SoD conflicts inside your Organization.

On the other side, we would like to cover one thing regarding the setup of authorization objects inside a Custom Transaction. In some cases you have a Custom Transaction that is updating records in a specific table, however it is required to restrict the access based in organizational values, meaning that someone that is having access to the Company Code "A" will not be able to change the records inside the specific table of the Company Code "B". For this case, we found many times that the maintenance activity is included in both authorization objects, the one that controls the activity for changing the records inside the table, and the one that check the Organizational Values where you are allow to perform changes. Since the functionality of the Custom transaction is updating records inside a table, the maintenance activity will only be applicable to the authorization object that manages the rights to change the records of the table (e.g. S_TABU_NAM). Therefore, the authorization object that restrict the organizational value company code should only have display activity.

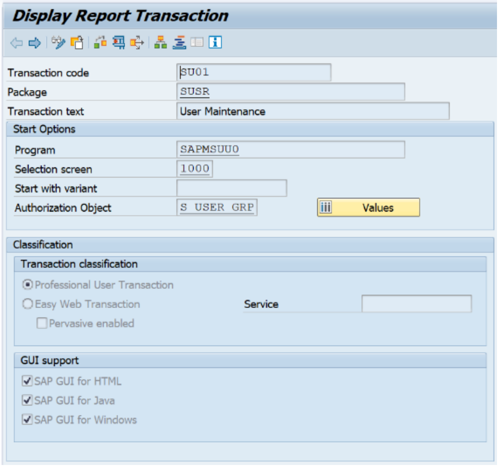
SU24 CONFIGURATION

SU24 configuration usually confuses SAP customers when we are talking about Security inside Custom Transactions. The SU24 configuration helps to link the authorization objects to the Transaction when performing Role Management Activities.



In the previous image, we will find that when creating a role and adding the "Transaction A" the authorization object "Y" and "Z" will be included automatically for Role Maintenance. However, this is not linked directly with the checks that were included inside the Program Code. The checks SHOULD be linked to what is included in the Program Code but this is manually dependent.

Therefore, as a statement we can conclude that the **SU24 configuration SHOULD contain all the authorization checks that were included in the Program Code,** but we need to remember that this need to be performed manually for each Custom Transaction that is going to be developed in our SAP system. It is recommended to run the Transaction **SE93** in order to verify that the information included inside the SU24 configuration is aligned with the Program Code calls:



Display Report Transaction

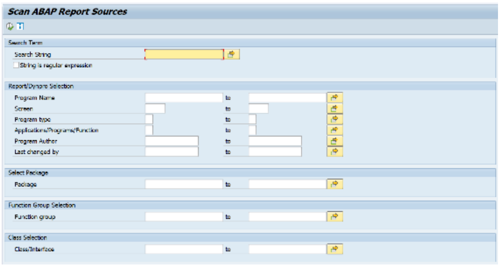
Transaction code: SU01
Package: SUSR
Transaction text: User Maintenance

Start Options
Program: SAPMSUU0
Selection screen: 1000
Start with variant:
Authorization Object: S_USER_GRP

Classification
Transaction classification
● Professional User Transaction
○ Easy Web Transaction
Service:
□ Pervasive enabled

GUI support
☑ SAP GUI for HTML
☑ SAP GUI for Java
☑ SAP GUI for Windows

Furthermore, there is an option to use the program **RS_ABAP_SOURCE_SCAN:**



Scan ABAP Report Sources

Search Term
Search String:
□ String is regular expression

Report/Dynpro Selection
Program Name: to
Screen: to
Program type: to
Applications/Programs/Function: to
Program Author: to
Last changed by: to

Select Package
Package: to

Function Group Selection
Function group: to

Class Selection
Class/Interface: to

<u>5 KEY POINTS TO TAKE HOME</u>

- ❖ Include the Security Analysis as part of the Change Management process of your Organization. The Later the more expensive.
- ❖ Use the authorizations objects that are related with the Functionality of the Custom Transaction. There are plenty options inside SAP.
- ❖ Think about the activities that are related with the Authorization Objects. A wrong selection of activities will trigger several SoD Conflicts.
- ❖ The SU24 configuration SHOULD be linked to the authorization objects that are being called in the Program Code.
- ❖ Verify the SU24 configuration using the Transaction SE93 or the program "RS_ABAP_SOURCE_SCAN".