



# **SAP Authorization logic**

Where did it all go wrong?

**Fourth release 2016**

Johan Hermans

Meta Hoetjes



## ***Table of Contents***

<b>Introduction</b>	<b>3</b>
<b>Two items of SAP security - some history</b>	<b>6</b>
<b>Why did it go wrong?</b>	<b>7</b>
<b>The access path in SAP</b>	<b>11</b>
<b>The logic of transaction codes</b>	<b>11</b>
<b>The illogic of transaction codes</b>	<b>11</b>
<b>The logic of authorization objects</b>	<b>13</b>
<b>The illogic of authorization objects</b>	<b>16</b>
<b>Insight in the access (path)</b>	<b>18</b>
<b>Criteria</b>	<b>19</b>
<b>Reporting risks</b>	<b>23</b>
<b>Reporting risks, what about remediation?</b>	<b>31</b>
<b>Rule set adjustments</b>	<b>31</b>
<b>Make changes to user role assignments</b>	<b>33</b>
<b>Changing the roles</b>	<b>34</b>
<b>Compensating controls</b>	<b>35</b>
<b>CSI tools in external publications</b>	<b>51</b>
<b>About</b>	<b>64</b>



## Introduction

This is the fourth release of our eBook about SAP authorization logics. With this eBook we want to help people getting aware of the real SAP vulnerabilities.

We are also proud to announce that:

- CSI tools has been granted a product and innovation leadership position and we have included the extract of the 2015 Leadership Compass of the KuppingerCole Report;
- CSI tools' Emergency Request tools has received GRC 20/20's 2015 GRC Innovation award;
- CSI tools is nominated as one of the finalist for the 2015 EU Cyber Security & Privacy Innovation Awards;
- CIOReview lists CSI tools as one of "100 most promising SAP solution Providers 2015".
- CIO Story lists CSI tools as "25 most powerful SAP Solution Provider".
- Insights Success Lists CSI tools as one of "50 Most Valuable Tech Companies"

**Johan Hermans and Meta Hoetjes**



Observe. Think. Act.



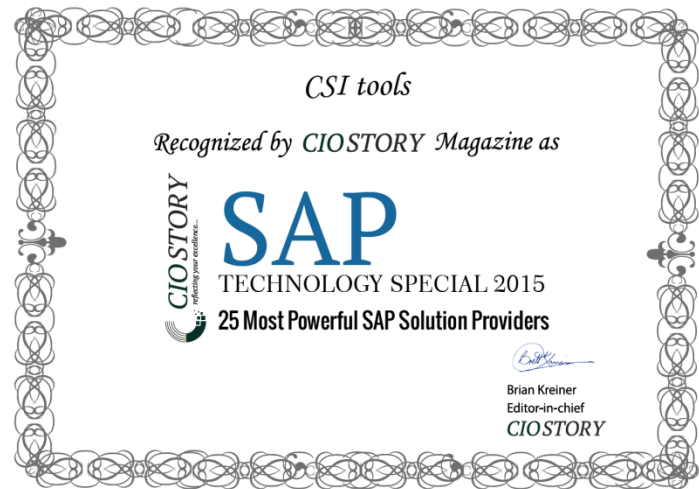
Product Leader  
Access Control / Governance  
for SAP environments  
July 2015



Innovation Leader  
Access Control / Governance  
for SAP environments  
July 2015

# Tech 50

Most Valuable Tech Companies





Some quotes from our readers:

“(...) I must say I was impressed by the quality of your work. (...) It really helps in understanding the SAP authorization logic and the "plane" example was really smart! (...) Thanks again for your contribution to the SAP security world.”

4 Feb. 2015 | **David Métivier**, Senior IT & IS auditor at **Sodexo**, France.

“This should be required reading for everyone involved in security. Thanks for posting!”

31 Dec. 2014 | **Liz O’Sullivan**, SAP Security and Controls Expert at **Swisscom IT Services** - Switzerland

“Initial read and my thoughts are along the lines of what others have found. The first 8 pages explain the complexity of SAP security very well, especially to project managers or leads that don't have a solid understanding of SAP security. Thank you so much.”

27 Jan. 2015 | **Alexander Le**, SAP Security Consultant at **Goodman Fielder Ltd.**, Australia

“I enjoyed your paper and agree with you. It seems most SAP security folks just follow what was done before them and really have no idea of the details or the reason they build roles as they do and spend too much time at just looking at the Tcodes.”

28 Jan. 2015 | **Clark Greenshields**, Security Managing Consultant at **IBM**, USA

## Two items of SAP security - some history

SAP security projects consume enormous budgets without really improving the security. This is caused by misunderstanding the basics of SAP security: the SAP authorizations. 90% of the security administrators do not know how many transaction codes and authorization objects exist in an SAP system. Moreover, if you ask the question what the purpose of a transaction code and an authorization object is with regard to SAP security, the answer is usually wrong. Some key questions we have asked security administrators and the answers we received (figure 1):

How many transaction codes and authorization objects exists in a SAP ECC 6.0 system and what is their purpose?		
	Transaction codes	Authorizations objects
Typical reply from security administrator	20.000	600.000
Purpose?	To manage access rights	To restrict on organizational level
	Transaction codes	Authorizations objects
Reality	+150.000	1.200 for "R/3" functionality
Real purpose?	Only first line of defense	To manage access rights

Figure 1: Example questions and answers

Most people think that you can protect SAP systems by removing and assigning transaction codes to users and that the purpose of authorization objects is to restrict certain organizational levels like company codes, plants, sales organizations etc.

The reality is however completely different: Only the authorization objects assigned to a user gives this user the permission to access the data, regardless if this user can execute the transaction. In a SAP system there can be more than 150.000 transaction codes and there are only 1.200 authorizations objects. Focusing on the authorization objects is more effective, efficient and gives greater agility.

Without going in the details how SAP security really works, everybody understands that if security administrators, auditors and internal control teams do not understand the basics of the two core elements of SAP security, they will never be able to optimize the SAP security. The scary thing is that people strengthen each other misunderstanding and SAP security projects getting more and more complicated and consume enormous budgets without even really improving the security.

### ***Why did it go wrong?***

The early versions of SAP system did not have security checks on who can start a transaction code. The system checked if the user had the required authorization objects with the authorization field values for the data. This early SAP security principle is explained below.

---

*Example early SAP security: The user logs in the SAP system using their log-on credentials. The user has a set of keys (authorizations) to open the lock to the SAP data. If the user wants to change a sales order, he enters transaction code VA02 and makes changes in the sales order. If the user does not have the authorizations to change sales orders, he cannot get to the sales order data.*

---

Setting-up security was complex because the security administrator had to think and develop security with a complete insight and understanding of the authorizations. Only people that were able to structure all those needs and translate this into a concept managed to implement a strong access security.

As from SAP release 3.0 E a new authorization object was invented: S\_TCODE. The definition of SAP was very clear: "The S\_TCODE check is only a first line of defense". The S\_TCODE check does not need to be programmed by the developer, it is checked when a transaction code is launched.

---

*Example how S\_TCODE works: The user logs in the SAP system using their log-on credentials. The user has a set of keys (authorizations) to open the lock to the SAP data and to start certain transaction codes. If the user wants to change a sales order, he enters transaction code VA02 to go the program to change a sales order.*

---

After the user enters transaction code VA02, the system checks if the user has the authorizations to start this transaction code. If the user does not have the authorizations for this transaction code, the user cannot reach the program to make changes. If the user does have the authorizations for this transaction code, the user gets access to the program to change the sales order. If the user does not have the authorizations to change sales orders, he cannot get to the sales order data. Basically, the screen has an additional lock via this new authorization object S\_TCODE.

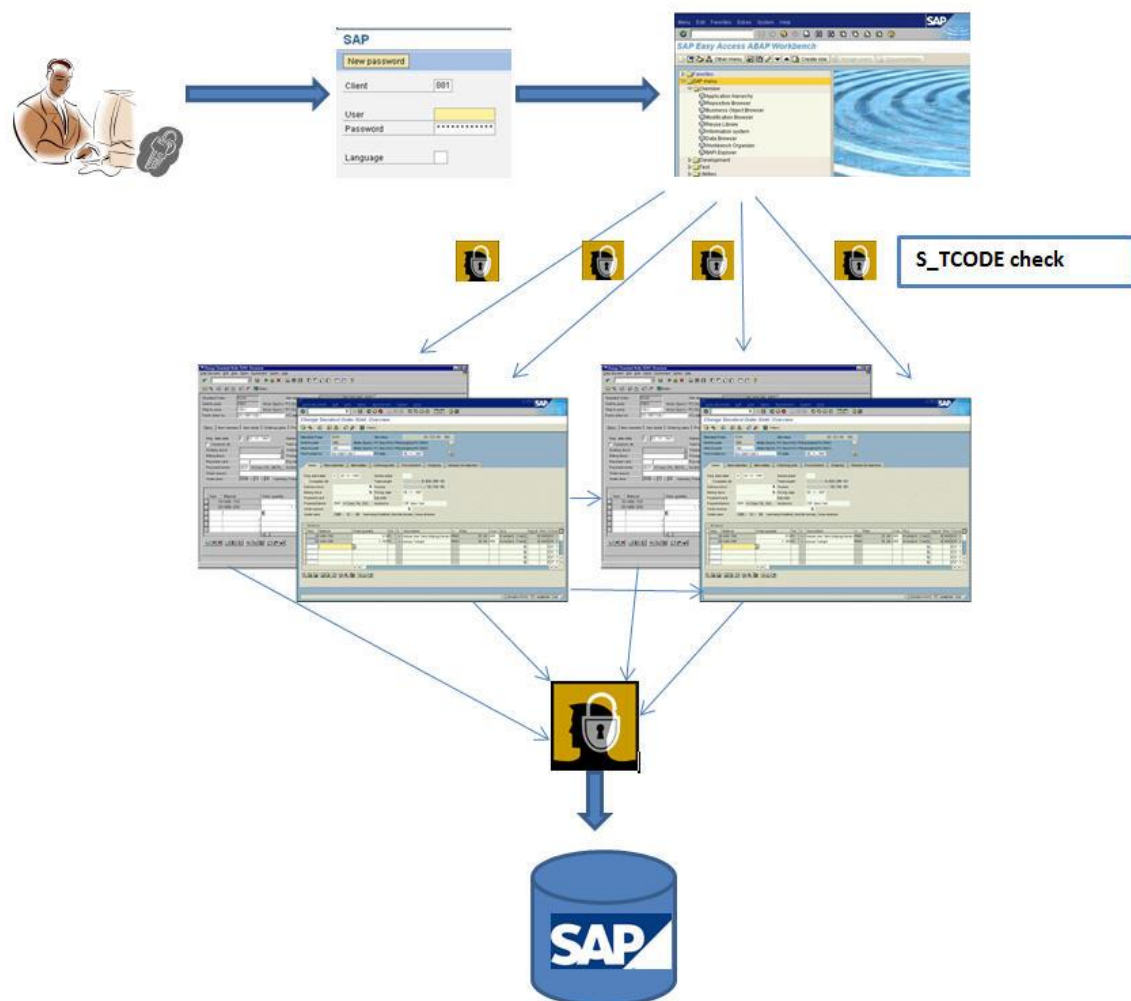


Figure 2: SAP security after the implementation of the S\_TCODE object

After the introduction of this new transaction authorization object suddenly everybody forgot the basics of SAP security and people only verified which transaction codes a user can execute. SAP SE cannot be blamed to add an additional security layer as a first line of defense. The problem however is the reaction of SAP





SE when the helpdesk (OSS<sup>1</sup>) was overloaded with "bugs" stating that the S\_TCODE did not work.

---

*Example of "bug" S\_TCODE not checked: A user starts display order transaction "VA03". The system checks if the user has authorizations to start transaction VA03 (Display sales orders) and if so, the user gets access to **change** the sales order(!): In the display sales order program, the user can click on the change/display button and suddenly the user is in change mode. At this moment the system only checked if the user has change authorizations and the system **did not check** if the user had authorizations to start the **transaction code** change sales order (VA02).*

---

SAP should have explained to all users, consultants and security administrators that it worked as intended. SAP however started implementing additional authority checks in screens, buttons et cetera using the same authorization object S\_TCODE. The consequence is that different kinds of S\_TCODE checks exist. The original S\_TCODE check whenever a user starts the initial transaction code and the other programmed S\_TCODE checks done by SAP in the existing coding. This causes confusion in the SAP community; nobody understands when the S\_TCODE check will take place and people start to think that the transaction code is the most important authorization item to provide access to data.

In the year 2000 SAP launched the SAP Profile Generator (PFCG). The message was clear: With this application security people do no longer need to understand how security of SAP system works. They just collect some transaction codes, push a wizard button, assign some organizational values (like company codes and sales organizations) and the work is done. A dream comes true for all people that are involved in SAP security.

To our big surprise the security in all companies became worse and worse. Companies no longer used experts to manage the security; instead they assigned the responsibility to a person who followed 3-day SAP authorization training and gave them the message: "We use 300 transaction codes, just group and assign them and it is done." They thought that the security was better....

SAP enforced the message that the SAP system would be protected by assigning transaction codes to roles and the roles to users. "Nobody" cared anymore about understanding all the authorizations that were granted in these roles. This focus on transaction codes continued in 2006 when Virsa, a SOD monitoring tool, was bought by SAP SE. The main focus in Virsa is on the assigned transaction codes, so all SAP's security applications are focusing on the transaction codes. Securing access to SAP data with the main focus on transaction codes will have security breaches because the transaction codes are designed only as a first line of defense.

SAP confirms transaction codes can be bypassed in their definition of SAP security in the help file: "To ensure that a user has the appropriate authorizations when he or she performs an action, users are subject to authorization checks. The following actions are subject to authorization checks that are performed before the start of a program or table maintenance and which the SAP applications cannot avoid:

- Starting SAP transactions (authorization object S\_TCODE). Indirectly called transactions are not included in this authorization check.
- Starting reports (authorization object S\_PROGRAM)
- Calling RFC function modules (authorization object S\_RFC)
- Table maintenance with generic tools (S\_TABU\_DIS)"

---

*Example of table maintenance functionality in transaction SE16N: If the authorization object S\_DEVELOP is not properly restricted and the SAP notes are not implemented, it is possible to maintain tables using "&sap\_edit" in the command field.*

---

Now we know that the transaction code authorization object (S\_TCODE) only covers partially the security and can be bypassed, we must understand how to restrict the authorizations in the roles. The focus should not be on the assigned transaction codes, but on the assigned authorizations.

## The access path in SAP

SAP is an integrated client server application. All the data resides in the SAP database server. This server is accessed by the SAP application server where all the authorization checks occur. SAP Authorizations consists of two core elements:

1. transaction codes and
2. authorizations objects with their authorization field values

### ***The logic of transaction codes***

The SAP system has more than 150.000 transaction codes to start a program and millions of ABAP programs. When a user starts a transaction code, the SAP system performs an authority check to verify if the user is allowed to start this transaction code.

### ***The illogic of transaction codes***

It is possible that one transaction code triggers another transaction code. When this is the case, no additional authority check is done on this triggered transaction code (see example below).

---

*Example: how to get access to critical functionality without having the transaction code. Get access to user master data maintenance (transaction code SU01):*

*If a user has no authorization to start transaction code SU01 but is allowed to start all transaction codes that begins with an "O", the user can create a User-id just by starting transaction code OOUS. If we have a look at the transaction code OOUS we see that it will start transaction code SU01 (figure 3).*

Transaction code	OOUS
Package	SP00
Transaction text	Maintain User
Transaction	SU01
Transaction variant	CV_P_OOUS
	<input checked="" type="checkbox"/> Cross-client

Figure 3 Transaction code OOUS starts transaction SU01

If we start transaction SU01, and we have no authorization the system will give an error message that we are not authorized to start SU01 (figure 4).

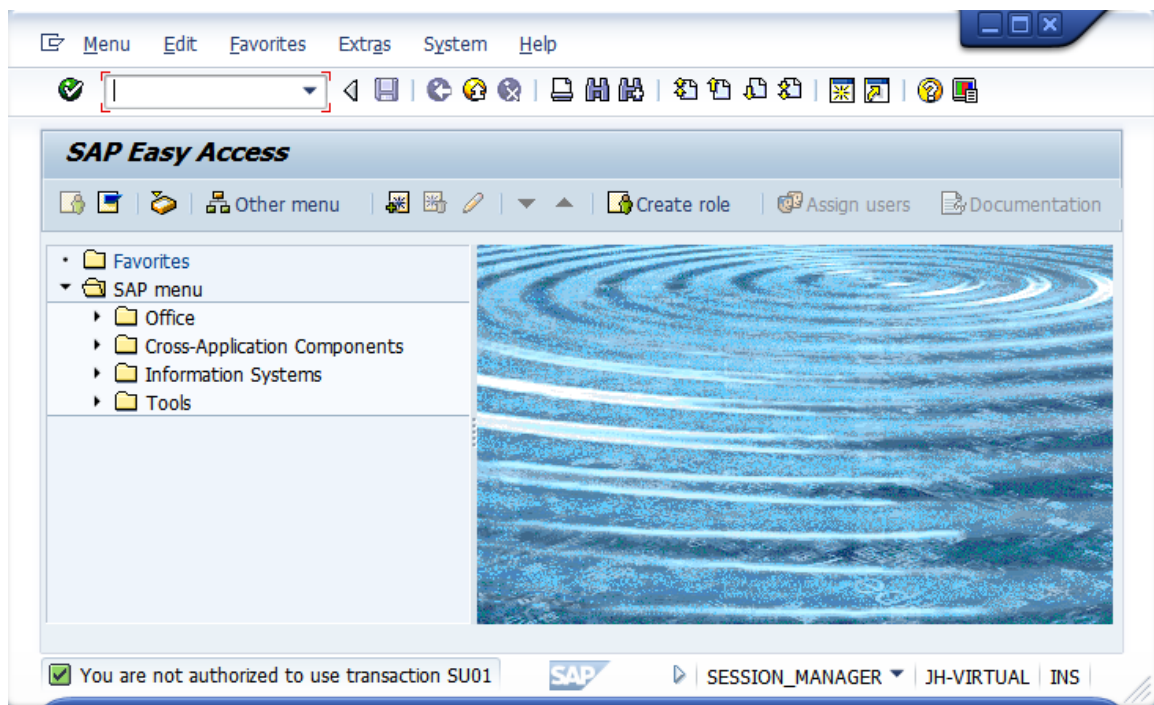


Figure 4 Error message because not authorized

Now if we start transaction code OOUS, the transaction code SU01 is started via transaction OOUS. However no authority checks are performed since the transaction code started was OOUS and not SU01 (figure 5). We have access to the user master data maintenance.

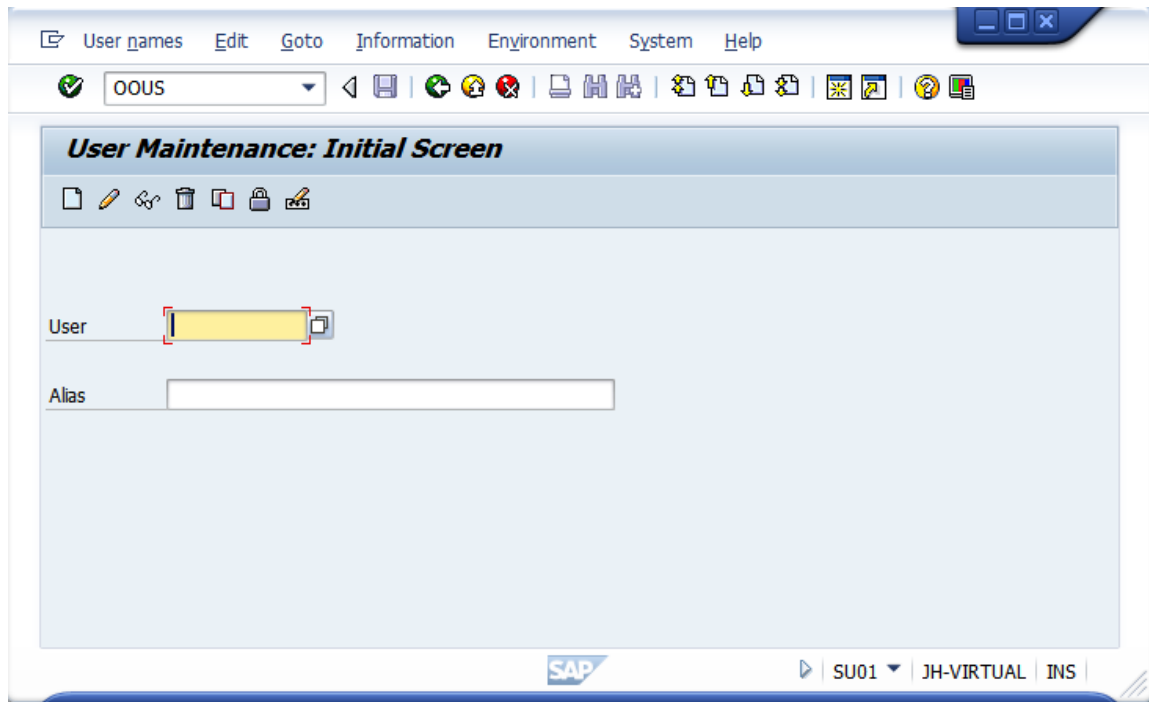


Figure 5 User maintenance via transaction OOUS

Another critical aspect regarding transaction codes is that some transaction codes can be used for different purposes. For example, you can post an Accounts Payable (A/P) document with an Accounts Receivable (A/R) transaction code.

It should be clear that the illogic behavior of transaction codes does not necessary lead to security breaches because the authorizations are checked before the data is accessed.



### ***The logic of authorization objects***

Authorization objects are THE key item in the security of an SAP system. Most people do not understand the difference between an authorization object and an authorization. This causes the confusion when experts are asked how many



authorization objects exist in a system. If we restrict our scope to the OLD R3 functionality (so no CRM, BI, APO, SRM, et cetera), approximately 1.200 authorization objects exist. The naming of an authorization object is technical but extreme logic:

Authorization object: "X\_YYYY\_ZZZ"

- X refers to the module
- YYYY refers to the data element, tables
- ZZZ to specific elements like company codes, document types et cetera,

Let's have a look at some real authorization objects and remove the last three characters (ZZZ elements):

- F\_KNA1\_
- M\_MATE\_
- F\_BKPF\_
- M\_BEST\_
- S\_TABU\_
- S\_USER\_
- ...

Some of readers will now have an "aha feeling" because they recognize and can relate:

The first character (module):

- F: module FI (**F**inance)
- S: Module BC (**S**ystem)
- M: module MM (**M**aterial **M**anagement)
- V: module SD (Sales & Distribution in German language: **V**erkauf)
- P: is not Production planning, but the abbreviation of "**P**ersonell" (therefore Staff, HR)

The second set characters (data elements and tables):

- LFA1: the core table of all suppliers. LF is the abbreviation of **L**ie**F**erante and A is to indicate the A segment of the supplier data so yes LFB1 protects the data of suppliers in the B segment and therefore company code data.
- USER: refers to all tables that manage the SAP users, roles etc.

- BKPF: the core table for all accounting documents (regardless if it is Account Payable or Account Receivable or Assets et cetera)

The third set characters (specific elements):

As most of you know, each module has an organizational level or two. The third set characters are referring to organizational levels and other relevant levels.

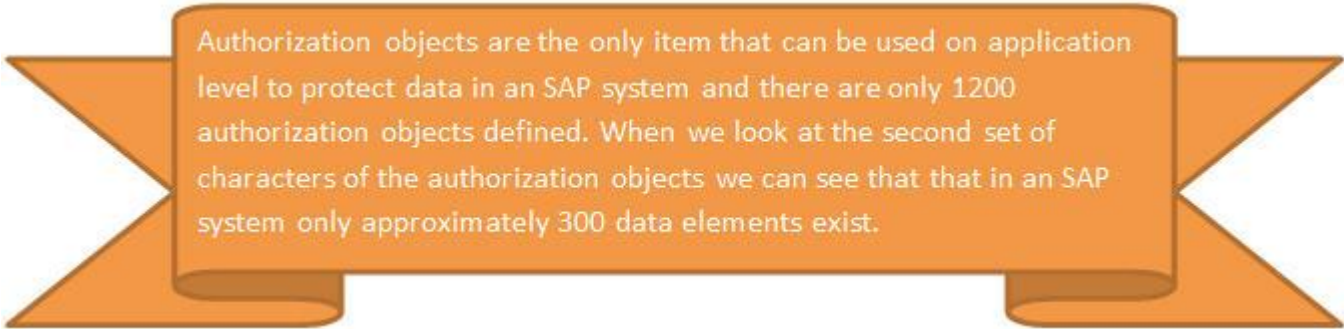
- FI uses Company code (**BU**chungs**KR**eiS or BUKRS or BUK)
- SD uses Sales organization (**Ver**kauf **ORG**anization or VKORG or VKO)
- MM uses Purchase organization (**Ei**n**K**auf **ORG**anization or EKORG or EKO)

These three sets of characters combined ("X\_YYYY\_ZZZ") is the authorization object.

---

*Two examples of authorization objects:*

1. *M\_MATE\_BUK: An authorization object to grant the access to Material Master data of the module Material Management (MM) on company code level*
  2. *M\_BEST\_EKO: An authorization object to grant access to the purchase orders (Bestellung) of the module Material Management on purchase organization level*
- 



Authorization objects are the only item that can be used on application level to protect data in an SAP system and there are only 1200 authorization objects defined. When we look at the second set of characters of the authorization objects we can see that that in an SAP system only approximately 300 data elements exist.

## ***The illogic of authorization objects***

We can probably all agree that the naming convention for the authorization objects are clear and now we are able to analyze that authorization objects like F\_BKPF\_... are used to verify if a user can do a posting in the SAP system.

If you compare this with real life, you would have situations like:

- Cinema ticket is being used to go to the cinema
- Train ticket is being used to take a train
- Plane ticket is being used to take a plane

Besides the logic of the authorization objects, there is are two critical aspect of the authorization concept that we must understand:

1. SAP's authority checks are done sequentially
2. SAP has created multiple authorization objects for the same data.

Let's see what this means in real life situation:

When we have a plane ticket (X\_PLANE), this plane ticket would have the following fields:

- Date
- From
- Destination
- Class

In real life you could have two plane tickets. With these two tickets we can only take two specific paths (flights):

1. One to fly from Amsterdam to New York on July 3th 2014, first class
2. One to fly from Brussels to London on August 16th 2014, economy class

In SAP this is usually done differently, you would have 4 authorization objects:

1. X\_PLANE\_DTE (date)
2. X\_PLANE\_FRM (from)
3. X\_PLANE\_DST (destination)
4. X\_PLANE\_CLS (class)

Now if we would arrange our life like SAP is doing its security, we would get 8 tickets:





1. One ticket to fly from Amsterdam
2. One ticket to fly from Brussels
3. One ticket to fly to New York
4. One ticket to fly to London
5. One ticket to fly on July 3th 2014
6. One ticket to fly on August 16th 2014
7. One ticket to fly first class
8. One ticket to fly economy

Those 8 tickets would be in your wallet. SAP's authority checks are done sequentially which results that you would be able to take a plane from Brussels to New York On August 16th in First class.

### ***Insight in the access (path)***

Whenever you want to set-up or audit SAP security the first thing you probably want to do is to define all possible access paths to the data. However, nobody can define the real access path to the data and nobody can guarantee that the user will remain on this access path and won't push a menu item or another button because there are more than 150.000 transaction codes and all these programs and transaction codes are nested and can be bypassed. Furthermore, the authority checks are done sequentially and nobody can really predict which authorizations are really needed to get access to the data (figure 6).

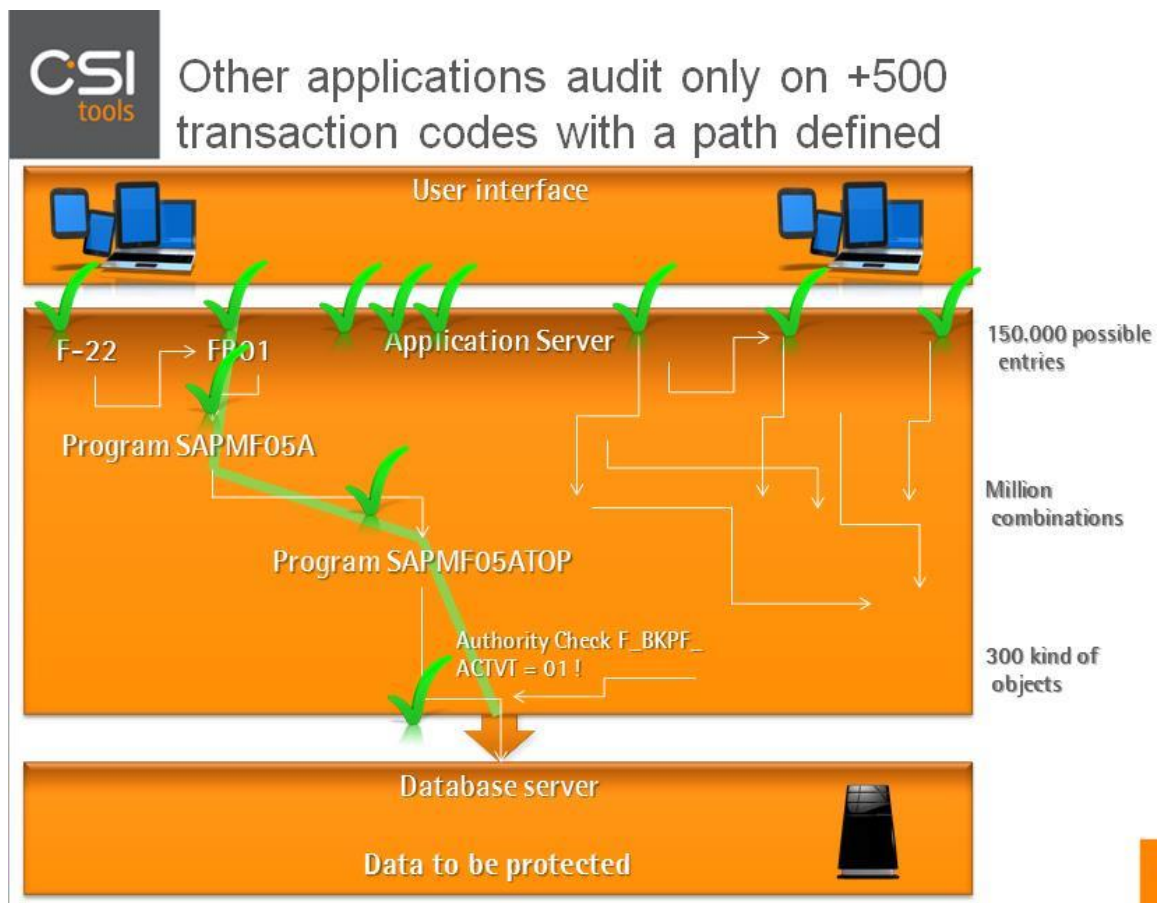


Figure 6: which access path to audit?

CSI tools simplifies and reports people who have the necessary authorizations regardless which transaction codes they have (figure 7).

## CSI tools reveal inconsistencies: who has access to the data, who can start transaction

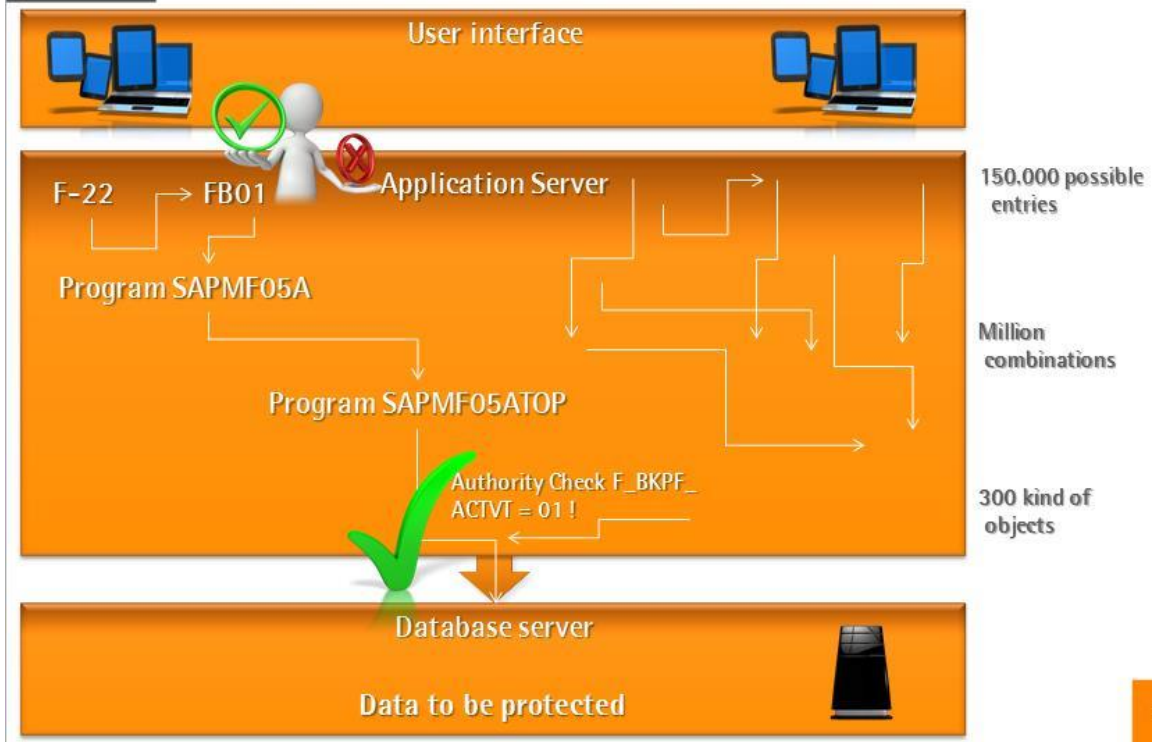


Figure 7: CSI tools reveal inconsistencies: who has access to the data and who can start the transaction

### Criteria

The most difficult aspect when auditing SAP security is to define the criteria you need to report real risks.

If you compare this to another real life situation: assume you want to protect who can go to a cinema in Paris. You need the following authorizations:

- you need to take a train to Paris and
- you need to have a cinema ticket

In CSI tools we report who has a cinema ticket for Paris, because this is the risk. All people that live in Paris do not need the train ticket and people outside Paris can come to Paris by plane or car.

The more criteria you use, the higher the risk that you will not find users who can do a certain functionality (figure 8). Risk management applications like SAP GRC and CSI tools use criteria to report risks. The more criteria is used, the greater the risks of false negatives.

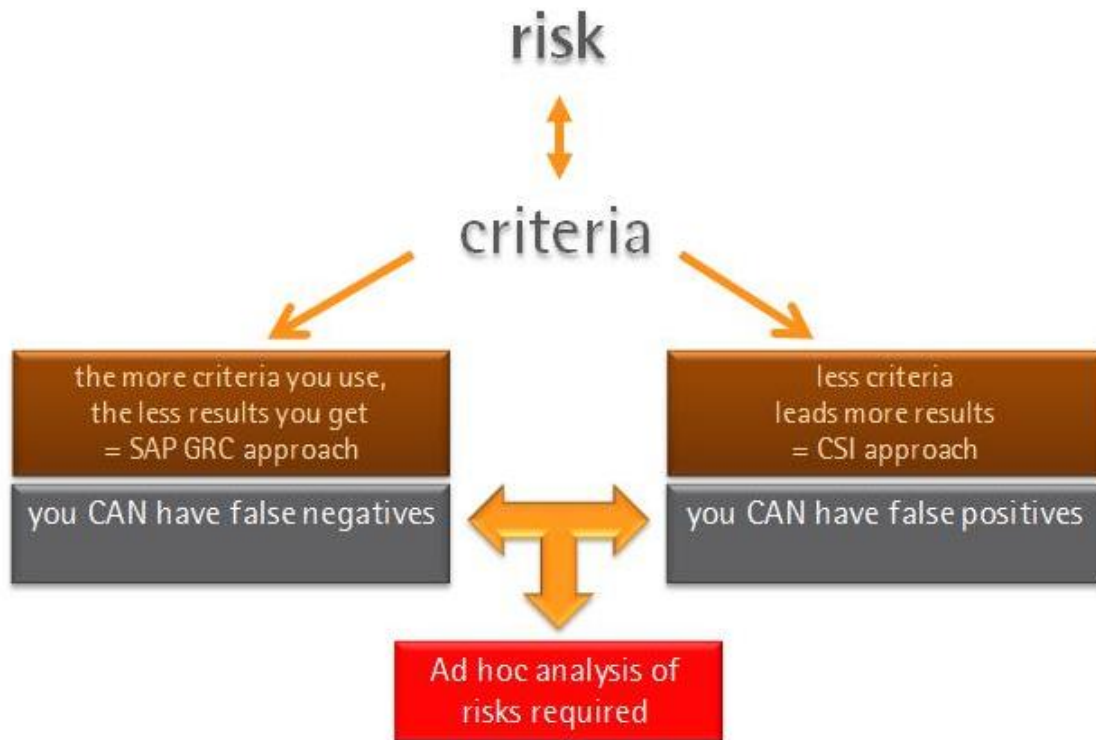


Figure 8: define the right criteria to report the risk

The risk when using SAP GRC is that you miss all the real risks because of the audit logic of SAP GRC. SAP GRC assumes that you cannot use a different path to get to the data and that the other paths are not known by the users. This is clearly wrong since "no one" has a clue about the number of transaction codes and authorization objects. If a user has the authorization objects but does not have the transaction(s) of a certain critical functionality, the user will not be reported in SAP GRC. SAP GRC only analyses and reports with the logic as described in figure 9. SAP GRC uses actions (transaction codes) and permissions (authorization objects and authorization field values). Only users/roles will be reported if they comply with the criteria:

The actions must be activated AND the user/role must have this activated action PLUS

The permissions must not be activated for the action OR if the permissions are activated the user/ role must has these activated permissions

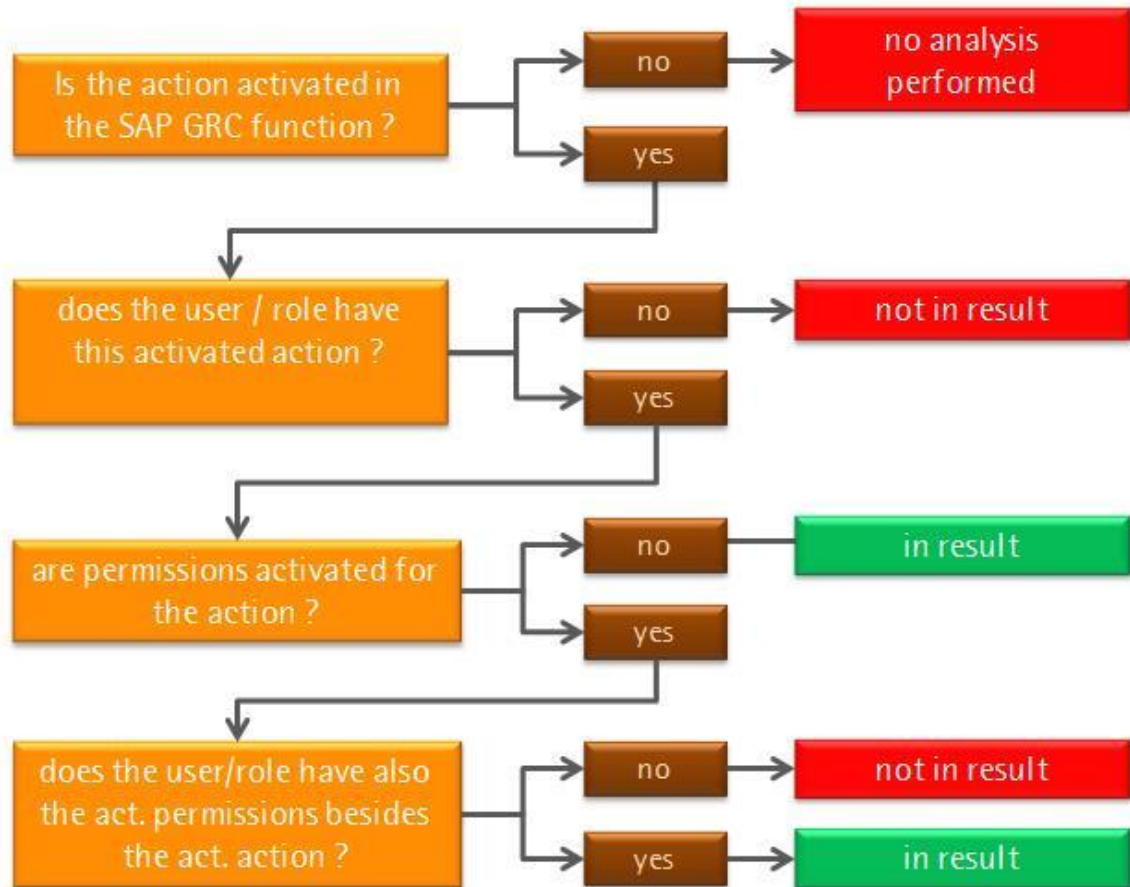


Figure 9: SAP GRC logic

This means that if a certain transaction code is missing in the rule set, SAP GRC does not report the users having access to the critical functionality even if the user does have access using another transaction code!

In CSI tools we use a different approach. The CSI logic will report all users, even if they do not have the transaction code. All users with the critical authorizations are

reported and an indicator shows if a user has the transaction code (figure 10).

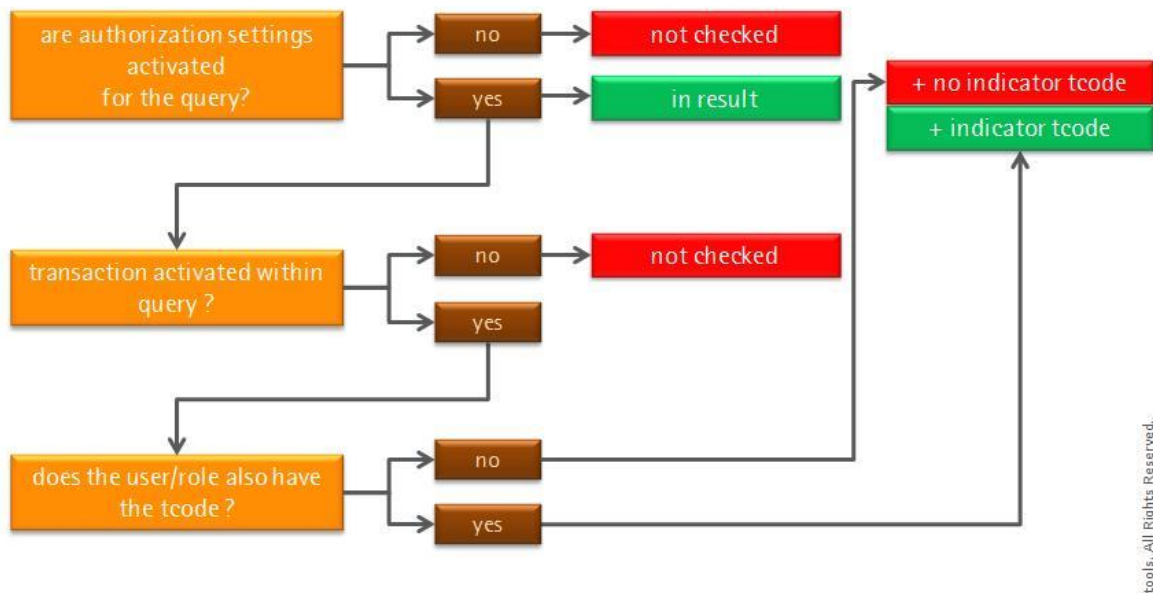


Figure 10: CSI tool logic

CSI will report the real risk. With the focus on the authorization objects with authorization field values instead on the transaction code it does not matter if a transaction is bypassed or not, the risk (user with the critical authorizations) is reported.

SAP GRC will only be perfect if the person who has configured the SAP GRC criteria knows all the transaction codes and knows all the different paths to the data. But this will never be the case; therefore SAP GRC fails to report the real risk. An even bigger problem is that transaction codes can be bypassed. SAP GRC will not report anything since the criteria focusses on the transaction codes. Therefore the exceptions like Remote Function calls must be added to the criteria. The defense of SAP is "all transaction codes that are not to be used should be locked and all the transaction codes that are being used should be verified on its criticality and then added to the criteria. The next chapter will explain why this approach is not feasible.

## Reporting risks

Let's have a look at an example risk and the reporting structure of SAP GRC and CSI tools: Assume we have one SAP system with 5 full access (SAP\_ALL) users and one SOD rule: purchasing tasks may not be combined with financial tasks (purchase vs. finance). This example is defined as SAP GRC criteria in figure 12: The SOD conflict is defined as **Risk F001 Purchasing with Finance**. The risk is a combination of two GRC functions: function Purchase and function Finance. A GRC function is a combination of GRC actions (transaction codes) and GRC permissions (authorization object with authorization field values). SAP GRC translates this Risk into generated rules; every possible combination of transaction codes is translated into a rule. Therefore 4 rules are generated (figure 12).

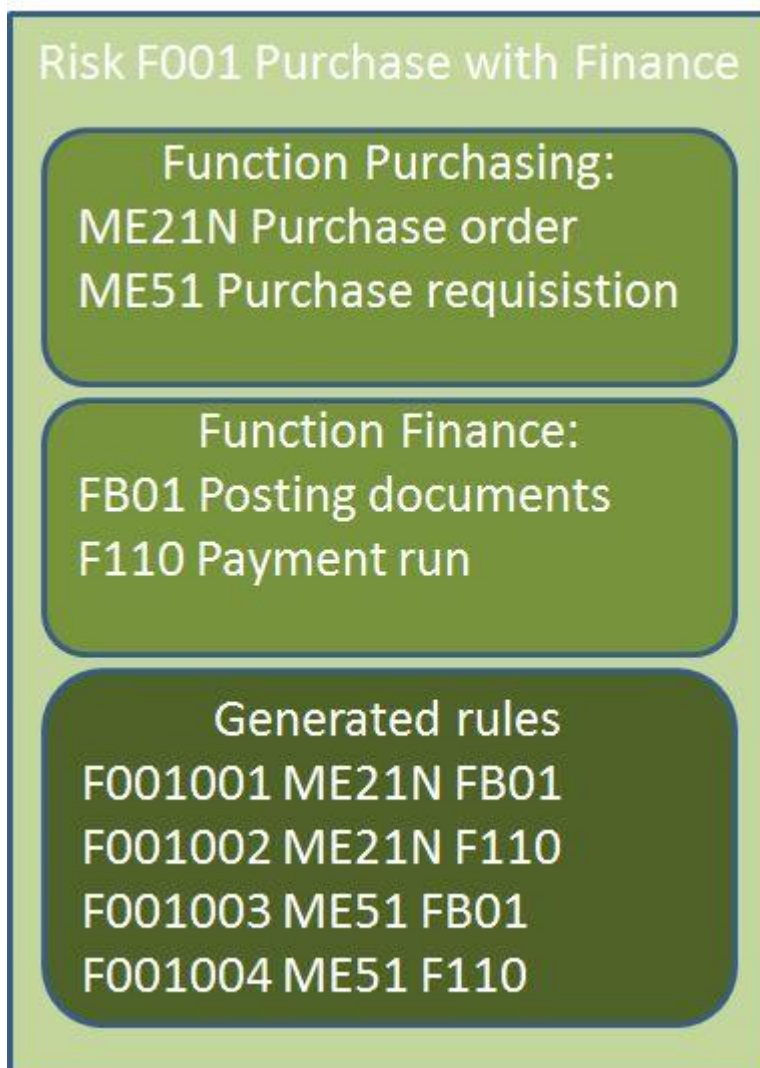


Figure 12: Example criteria Purchasing & Finance risk

The users will be analyzed and reported against these generated rules. This means that our users with full access (5 users in total) will be reported for every generated rule of the SoD conflict (4 rules). Therefore SAP GRC reports having  $5 \times 4 = 20$  conflicts (figure 13).

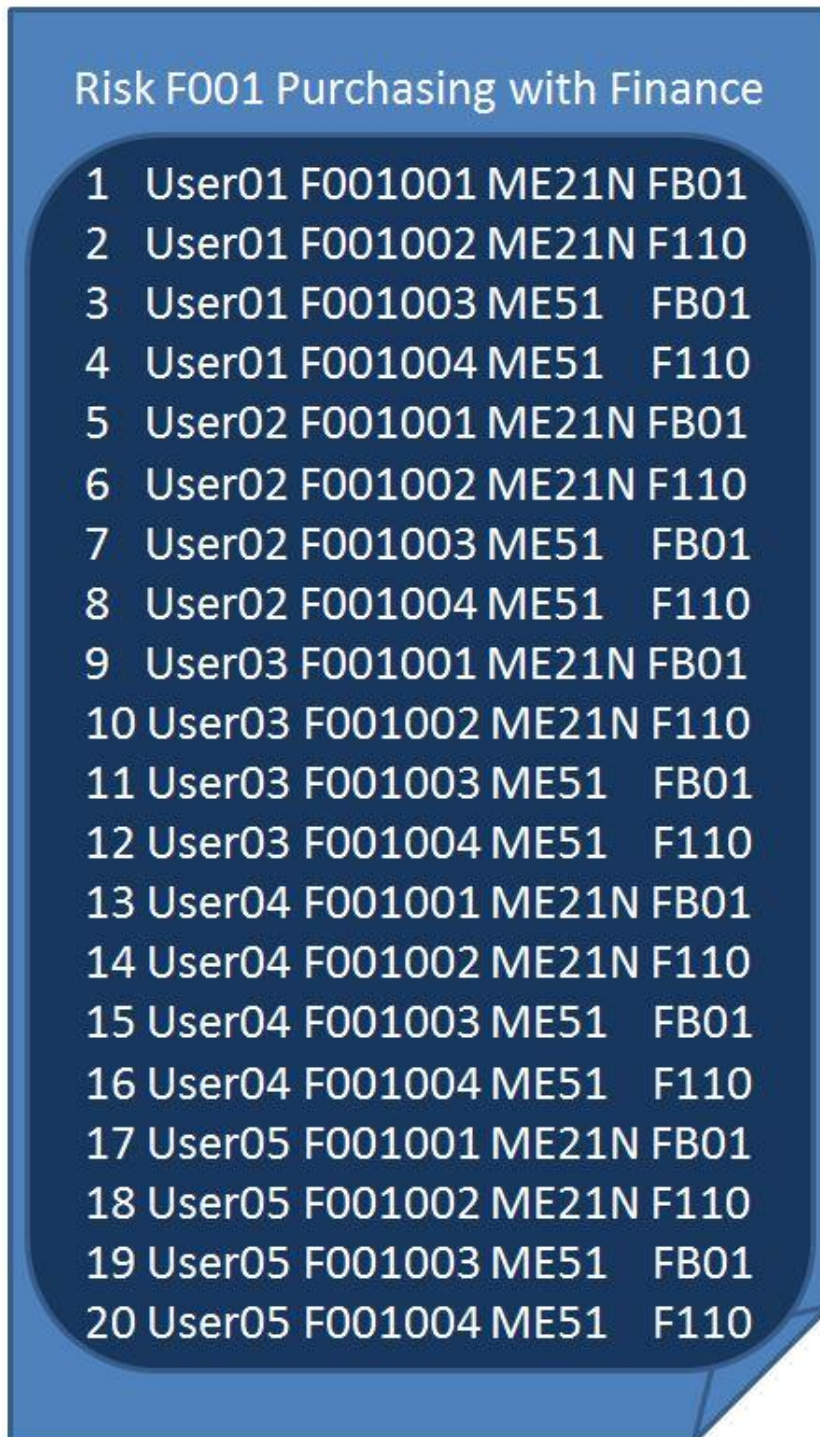


Figure 13: GRC logic for the Purchasing & Finance risk



CSI tools will report the same risk in a more efficient way. The users with full access (5 users in total) will be reported per SoD conflict (1 conflict). CSI tools will report 5 SoD conflicts (figure 14):



Figure 14: CSI tools logic for the Purchasing & Finance risk

The example risk criteria were not complete. According to SAP, all transaction codes for purchasing and finance that are being used should be added to the criteria in the rule set. In this example we will add two transaction codes to the two functions: the transaction codes MExx and MEyy to function purchasing and transaction code FBzz, to function finance (figure 15). SAP GRC translates this same risk with added transaction codes into 12 generated rules. This means that the 5 SAP\_All users will be reported for each rule =  $5 \times 12 = 60$  SOD conflicts will be reported!

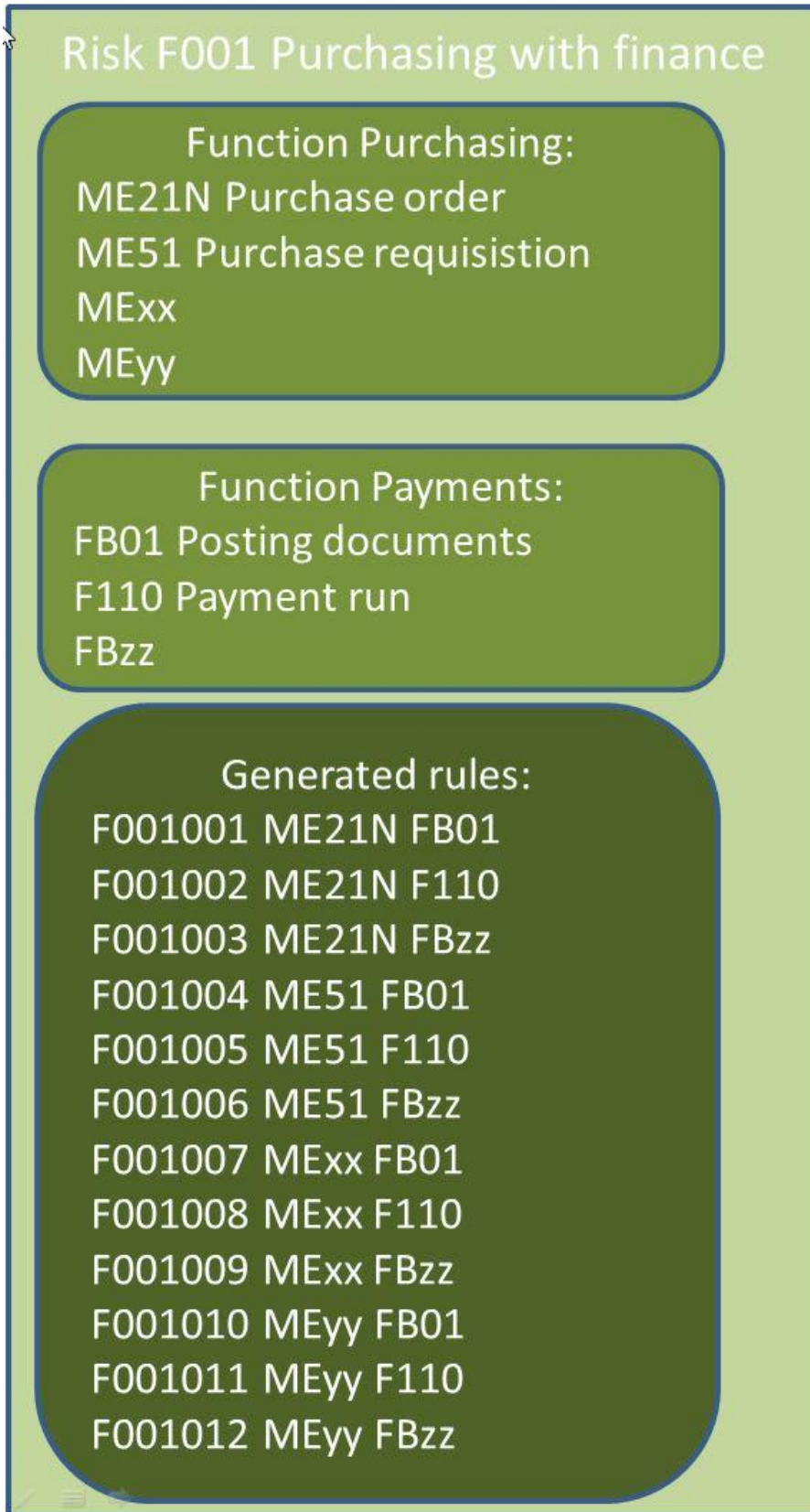


Figure 15: Adjusted criteria for risk

CSI tools will still report 5 SOD conflicts for the 5 SAP\_ALL users, no matter how many transaction codes are assigned to the criteria (figure 16):



Figure 16: CSI logic for the Purchasing and Finance Risk with additional transaction codes

The GRC report will report 60 (!) SoD reports for these 5 SAP\_ALL users (figure 17).

Risk F001 Purchasing with Finance

1. User001 F001001 ME21N FB01
2. User001 F001002 ME21N F110
3. User001 F001003 ME21N FBzz
4. User001 F001004 ME51 FB01
5. User001 F001005 ME51 F110
6. User001 F001006 ME51 FBzz
7. User001 F001007 MExx FB01
8. User001 F001008 MExx F110
9. User001 F001009 MExx FBzz
10. User001 F001010 MEyy FB01
11. User001 F001011 MEyy F110
12. user001F001012 Meyy FBzz
13. User002 F001001 ME21N FB01
14. ....

.....

Risk F001 Purchasing with Finance

57. ....
58. User05 F001010 MEyy FB01
59. User05 F001011 MEyy F110
60. User05 F001012 Meyy FBzz

Figure 17 GRC logic for the Purchasing and Finance Risk with additional transaction codes



This example was just for one conflict. Imagine using a rule set with more conflicts, then you need to process millions of lines to solve the SoD conflicts and for the SoD conflicts that cannot be solved you need to identify and assign compensating controls per line and these millions compensating controls needs to be reaffirmed every time.

This explains why most rule sets in SAP only cover approximately 250 transaction codes, where most companies uses three- to five thousand. A risk management tool should not only focus on what is being used, but also on the 150.000 transaction codes that can be abused. If we would follow the advice from SAP to add all the transaction codes to the rule set, defining and the reporting SoD conflicts becomes a nightmare.

First, **all** the transaction codes that give access to the risk must be added to the criteria in the rule set. This leads to problems because there are more than 150.000 transaction codes in ECC and the limit of the number of rules you can have per GRC risk is 1.679.616. This means that not all the transaction codes that exist in the SAP system can be added to the criteria in the rule set:

If you have four GRC functions then you can assign max. 36 transaction codes per risk because of the limit of the number of rules per GRC risk:  $36*36*36*36=1.679.616$ .

If you have one SoD conflict (GRC risk) with two GRC functions, you can assign 2 x 1.296 transaction codes in the risk.

The more GRC risks you define, the less transaction codes you can assign per GRC risk:

2 GRC functions ( $1296*1296 = 1679616$ )

3 GRC functions ( $118*118*118$ )

4 GRC functions ( $36*36*36*36$ )

5 GRC functions ( $17*17*17*17*17$ )

6 GRC functions ( $10*10*10*10*10*10$ )

The conclusion is that you cannot rely on the transaction codes.

In order to keep reports clean and to be able to solve the SOD conflicts, CSI tools is more efficient, effective and has great agility for the criteria adjustments. Users can drill down into the details to see the roles causing, authorization assigned, usage of



transaction codes et cetera. If changes to the rule set criteria or reporting are needed, it can be easily adjusted and all changes that are made in the rule set are being logged.



## Reporting risks, what about remediation?

Now we have a clear view and understanding what should be reported and we have the reports ready, the next step is to mitigate the risks. There are different ways how risks can be mitigated:

- by adjusting the rule set
- by adjusting the assignment of roles to users
- by changing the role content
- by compensating controls

### Rule set adjustments

To report real risks, the rule set must be correct. The results of the (first) analysis can help defining and fine-tuning the rule set. With CSI tools you have a clear insight in the correctness in the rules, roles, and role assignments because of its multi-layered analysis (figure 18). CSI tools' multi-layer approach is unique. CSI tools was mentioned by analysts Anmol Singh and Brian Iverson in Gartner Market Guide for SOD Controls Monitoring Tools on April 28 2015 <sup>[4]</sup> *"CSI tools' strength is in its multilayer security model for SAP systems"...*

Let's have a look at some examples where the rule set needs fine tuning: Users are reported with critical functionality or SOD conflicts. They have the authorization objects with authorization field values but do not have the transaction code. In CSI tools, the users are reported with an indication that the transaction code is missing. This can be an indication that the rule set is missing transaction code(s) and the users do have access to the critical functionality but they use a transaction code that is not in the rule set. If you would have done the same analysis in SAP GRC, but you did not to add all relevant (custom) transaction codes, the users would not have been reported at all, you will be missing these risks being reported (see chapter 2).

Example report in CSI tools

If we continue with the example above and have a look in the tool itself: the users are reported having authorization objects with authorization field values and/or transaction codes for critical functionality. If the users have the authorization objects with authorization field values, but do not have the transaction(s) for this critical functionality, the users will still be in the report and you can see that there is no checkmark in the column "has T-code", but there is a checkmark in the column "has authorizations". There is an inconsistency in the rule or the role since the user has access to the data (he has the authorization objects and the authorization field values) but cannot start the audited transaction code. The solution is:

- either the ruleset must be adjusted (maybe a custom Z transaction is missing in the rule set?)
- or the role(s) should be adjusted, either the authorization objects and authorization field values must be removed, or the transaction code must be added to the role.

Logical System	Variant	Query Description	Query	Type	Sox Classification	Has Authorization	Has T-code	Executed T-code
<b>USER002 (3 items)</b>								
DEMO	<NA>	Maintain FI Posting Periods	ECC_FCLOSA	ARQ	SOX_H	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DEMO	<NA>	Maintain Customizing FI	ECC_FCSTMA	AR	SOX_C	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DEMO	<NA>	Maintain FI Posting Periods	FCLOSA	ARQ	SOX_H	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>USER004 (9 items)</b>								
DEMO	<NA>	Maintain A/P Postings with Clearing	ECC_FAPPCA	ARQ	SOX_H	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DEMO	<NA>	Maintain A/P Parked Documents	ECC_FAPPD7	AO	SOX_M	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DEMO	<NA>	Maintain A/P Parked Documents Postings	ECC_FAPPPA	ARQ	SOX_M	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DEMO	<NA>	Maintain A/P Outgoing Payment Postings	ECC_FAPPPYA	ARQ	SOX_M	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DEMO	<NA>	Maintain A/P Recurring Documents	ECC_FAPRDA	ARQ	SOX_C	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DEMO	<NA>	Maintain FI Posting Periods	ECC_FCLOSA	ARQ	SOX_H	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DEMO	<NA>	Maintain Customizing FI	ECC_FCSTMA	AR	SOX_C	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DEMO	<NA>	Maintain A/P Manual Postings	FAPMPA	ARQ	SOX_M	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Profile (causing)	Tcode (causing)	Role (causing)
FX00XAPMPA	F-42	S99FX00XAPMPA
FX00XAPMPA	F-18	S99FX00XAPMPA
FX00XAPMPA	FB01	S99FX00XAPMPA
FX00XAPMPA	FB02	S99FX00XAPMPA
FX00XAPMPA	FB07	S99FX00XAPMPA
FX00XAPMPA	FB08	S99FX00XAPMPA
FX00XAPMPA	FB09	S99FX00XAPMPA
FX00XAPMPA	FB11	S99FX00XAPMPA
FX00XAPMPA	FB60	S99FX00XAPMPA
FX00XAPMPA	FB65	S99FX00XAPMPA
FX00XAPMPA	FBL1N	S99FX00XAPMPA
FX00XAPMPA	FBL2	S99FX00XAPMPA
FX00XAPMPA	FBL2N	S99FX00XAPMPA
FX00XAPMPA	FBR1	S99FX00XAPMPA
FX00XAPMPA	FBR2	S99FX00XAPMPA

Profile (causing)	Object	Authorization	Role (causing)
FX00XAPMPA	F_BKPF_BUK	FX00XAPMPA00	S99FX00XAPMPA
FX00XAPMPA	F_BKPF_BUK	FX00XAPMPA01	S99FX00XAPMPA
FX00XAPMPA	F_BKPF_KOA	FX00XAPMPA00	S99FX00XAPMPA
FX00XAPMPA	F_BKPF_KOA	FX00XAPMPA01	S99FX00XAPMPA

Inconsistencies in rules or roles!

Since user has access to the data but cannot start the audited transaction code

User has access but does not use it

According to the principle "need-to-know" & "need-to-have" these access rights should be removed

Figure 18: check on rule, roles and role assignment inconsistencies



*This report gives all the information about the remediation of the risk as well. It shows if the user has been using the critical functionality and includes all the causing information to get insight in the profiles and roles granting the access to the user. The checkmark column next to the "Tcode (causing)" column shows if the user has executed the transaction code (checkmark) or not (no checkmark). If the user has access to the critical functionality but he is not using it, he probably does not need to have this access and the rights should be removed, based on the need to know and need to have principle.*

---

Organizational elements are also very important aspect of risk reporting. With reporting users having SOD conflicts, these conflicts must be real risks. If the SoD conflict for that user is a combination of two functionalities and the user can perform functionality A in Company 1 and functionality B in Company 2 then there is no real risk and the user should not be reported. CSI tools documents all the organizational values in one central place and this information is used in all critical access and SOD conflicts analyses.

### **Make changes to user role assignments**

Analyze if the user with access to a critical functionality (or maybe even a SOD conflict) has been using it. If not, this critical functionality can be removed from the user. The easiest way to remove authorizations from the user is by removing the role(s) that are assigned to the user. The reports in CSI tools provide full insight how to mitigate the risks and which roles can be removed from the user. Use the information of the usage of transaction codes and the usage of the roles to analyze if the user has been using the roles (single and composite) and decide which roles can be removed.

---

*The example report in figure 19 shows the details of the user Jeroen Jacobs having access to table maintenance. We want to remove this critical functionality from this user. The report shows the transaction codes and objects causing access to table maintenance, the profile, authorization, single roles and the composite roles causing access to table maintenance. The user has not been using (column executed "E") the*

transaction codes SM30 and SM31, he has not been using the profiles and single roles that are causing access, but he has been using the composite role S99-XXXX\_SYSTADM. So he needs to have some functionality of this composite role to do his job, but the table maintenance he does not need. With this information we can further investigate which authorizations Jeroen does need from this composite role and search if this functionality can be assigned via a less critical composite role.



## SoD Reports

track which roles can be removed

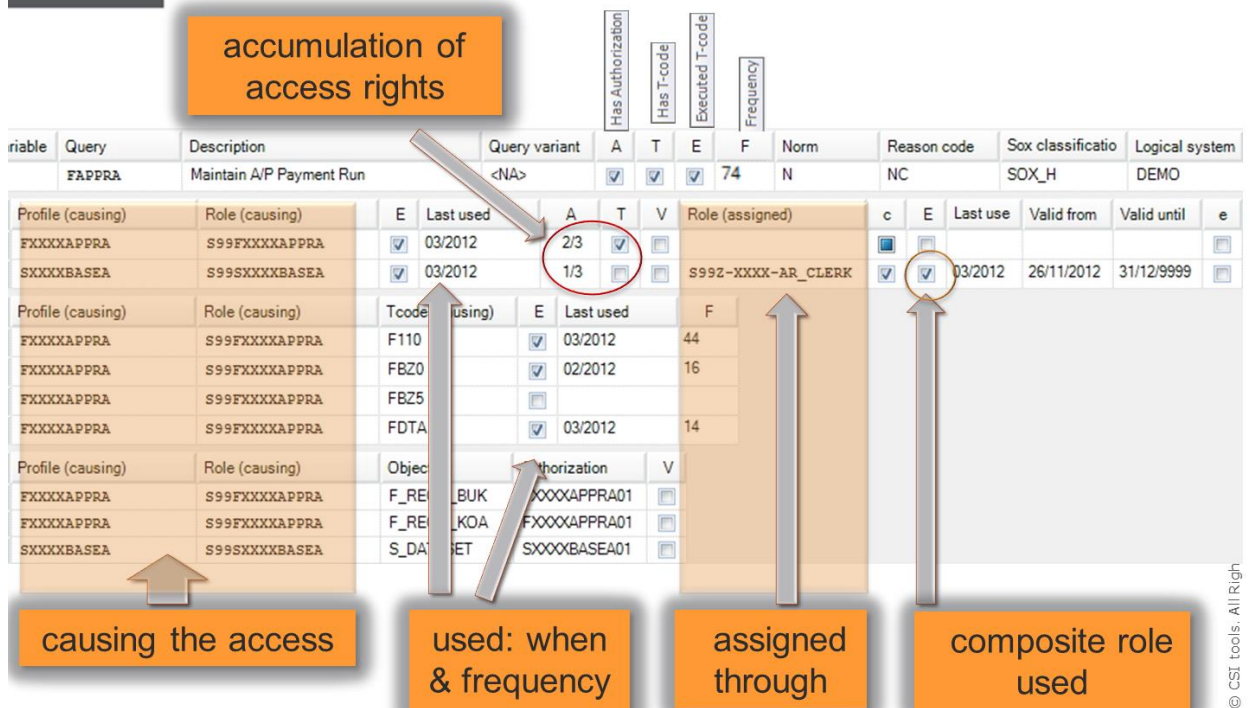


Figure 19: Details information with causing and usage information

## Changing the roles

Another way to mitigate the risks is to make changes to the existing roles. This can be changes in the assignment of single roles to composite roles or changes in assignments of transaction codes and/or authorization objects with the authorization values to single roles. In our last example, we can further analyze if the users that are assigned to the composite role S99Z-XXXX-SYSTADM need to have table maintenance. If they do not need this, the single roles with the transaction codes



and authorization objects with authorization field values for table maintenance (S99SXXXXSM30D, S99SXXXXTABLA and S99SXXXXTTMSA) can be removed from the composite role.

### **Compensating controls**

It is possible that risks cannot be mitigated by changes the roles and/or role assignments. For example if the users need broad access because of back up functions or if only a limit number of users are available to do all the work. If this is the case, then compensating controls needs to be defined and implemented. But this is just the start. The compensating controls needs to be monitored as well and the (test) evidence must be saved and related to the risks. In CSI tools all this is possible, making CSI tools a complete and mature GRC solution.



CSI tools in GRC 20/20's Solution perspective

## CSI tools A Fresh Perspective on Access Controls & SoD



CSI tools is a GRC offering that GRC 20/20 has researched, evaluated, and reviewed with organizations that are using it in changing, distributed, and dynamic business environments. CSI tools provides analytic control solutions that audit and monitor SAP environments, manage and validate authorizations, and build roles tuned to the organizations security requirements and business needs. CSI tools enables organizations to evaluate existing roles, access rights of users, remediate issues, restructure roles to remove unnecessary roles and entitlements, as well as grant and document exceptions for non-compliant access for business reasons. GRC 20/20 has interviewed and engaged several CSI Tool clients and finds that the CSI tools solutions have helped them keep up with access controls and SoD in a way that maximizes their GRC resource efficiency, effectiveness, and agility.

It has been stated that:

Any intelligent fool can make things bigger, more complex and more violent. It takes a touch of genius – and a lot of courage to move in the opposite direction.<sup>1</sup>

While there are many automated access control and SoD solutions available in the market, CSI tools takes a unique and very effective approach. CSI tools accomplishes this by focusing on authorization objects and not simply on transaction codes that other solutions do. Consider that there are roughly 150,000 transaction codes in nested relationships and complexity within SAP environments while there are only approximately 1,200 authorization objects. The exponential impact of access control and SoD around transaction codes produces millions of combinations. Transaction codes provide a rough first line of defense that can be bypassed given the right circumstances, while authorizations objects are what actually manage access rights in the SAP environment. Authorizations assigned to an SAP user give the user permission to access data independent of the user's capability to execute a transaction. While both transaction codes and authorization objects can be used to secure SAP environments, focusing on authorization objects instead of transaction codes is more effective, efficient, and agile.



Some of the capabilities that GRC 20/20 has evaluated in CSI tools that many of its competitors do not always address are:

- Which roles cause accumulation of access rights
- Who has almost access to do something
- Which roles need to be removed
- Which roles should be isolated from a composite one
- Check the access of a role based on documentation

### **The Value of CSI tools**

Successful GRC delivers the ability to effectively mitigate risk, meet requirements, satisfy auditors, achieve human and financial efficiency, and meet the demands of a changing business environment with agility. GRC solutions should achieve better performing processes that utilize more reliable information. This enables a better performing, less costly, and more flexible business environment. Clients engage CSI tools with the goals of understanding and managing risk, ensuring compliance with obligations, improving human and financial efficiencies, enhancing transparency, and managing GRC in the context of business change.

GRC 20/20 measures the value of GRC engagement around the elements of efficiency, effectiveness, and agility. Organizations need to be:

- Efficient. GRC engagement provides efficiency and savings in both human and financial capital. GRC efficiency is achieved when there is a measurable reduction in human and financial capital resources needed to address GRC in the context of business operations.
- Effective. At the end of the day it is about effectiveness. How does the organization ensure risk and compliance is effectively understood, monitored, and managed at all levels of the organization?
- Agile. GRC engagement delivers business agility where organizations can respond rapidly to changes in the business environment (e.g., employees, business relationships, mergers, acquisitions, new laws, and regulations) and communicate to employees GRC context to these changes.



## GRC Efficiency

GRC solutions provide efficiency and savings in human and financial capital resources. Technology solutions that support business and GRC processes reduce operational costs by automating processes, particularly those that take a lot of time consolidating and reconciling information in order to manage and mitigate risk and meet compliance requirements. GRC efficiency is achieved when there is a measurable reduction in human and financial capital resources needed to address GRC in the context of business operations. Their ability to focus on authorization objects and not just transaction codes is more effective, efficient, and agile.

The organizations researched by GRC 20/20 identified the following efficiencies by organizations using CSI tools:

- Cost savings in employee time designing user roles in context of ERP changes
- Automation of access controls and SoD brings efficiency in employee time
- Less spending on external consultants to do manual control validation and SoD monitoring
- Cost savings in internal audit testing and investigation of access controls
- Reduction in external audit fees as they rely more on the automation of access controls and SoD
- Efficiency in assigning and determining appropriate access
- Greater efficiency and savings in resource time documenting user access reviews
- Efficiency in technology processing and overall reporting time savings in which an audit of 10,000 users takes only 15 minutes

## GRC Effectiveness

GRC solutions achieve effectiveness in risk, control, compliance, audit, and business processes. This is delivered through greater assurance of the design and operational effectiveness of controls to mitigate risk, achieve performance, protect integrity of the organization, and meet regulatory requirements. GRC effectiveness is validated when business processes are operating within the controls and policies set by the organization and provide greater reliability of information to auditors and regulators.

The organizations GRC 20/20 interviewed reported the following effectiveness through utilizing CSI tools:



- Access provisioning, monitoring, SoD, and emergency management are now practical through automation as the organization never had the time and resources to properly address these manually
- The organization now audits all roles for SoD issues instead of random sampling
- Reduction in auditor findings related to SoD conflicts
- Reduction in risk exposure as well as business disruption through stronger control enforcement and monitoring
- Performing authorization reviews manually was like “looking for a needle in a haystack” but is now practical and effective with a greater number of SoD conflicts detected and addressed
- Easy to determine users with excessive access, who have SoD conflicts, determine the roles that are causing conflicts or excessive access
- Ability to customize queries to solve specific authorization challenges
- Reduction of 32,000 SoD conflicts to 4,000 in the first month of use

### **GRC Agility**

GRC solutions deliver business agility where organizations are able to rapidly respond to changes in the internal business environment (e.g., employees, business relationships, operational risks, mergers, and acquisitions) as well as the external environment (e.g., economic risk, new laws, and regulations). GRC agility is also achieved when organizations can identify and react quickly to control failures/weaknesses, noncompliance, and adverse events in a timely manner so that action can be taken.

The organizations interviewed reported the following agilities in their compliance and broader GRC processes through working with CSI tools:

- The organization is now able to rapidly find and correct access control and SoD issues
  - Once queries are built and customized they can be readily used at any time
  - Authorizations are more transparent
  - Capability to present conflicting roles to the business in a way they can understand and respond to
  - Ability to manage action items to fix authorization problems
  - Streamlined authorization audits and consultations
  - Ability to continuously monitor role and SoD changes throughout year and not just annually
- Capabilities of CSI tools GRC 20/20 has evaluated the CSI



tools offering and finds that it delivers an integrated and harmonized solution for today's demanding access control and SoD challenges faced by organizations across industries and geographies. CSI tools enables organizations to evaluate the existing roles and access rights of users, remediate issues, restructure roles to remove unnecessary roles and entitlements, as well as grant and document exceptions for non-compliant access for business reasons.

CSI tools delivers the following capabilities to make GRC programs efficient, effective, and agile:

- Rule-Based SoD analysis. Analysis of SoD is built on an extensive set of authorization object analysis that can be built into rules that meet specific business needs and scenarios. SAP has multi-layered security. Other solutions check layers simultaneously to ensure that there are no false positives. CSI tools does five independent checks. By analyzing different layers separately organizations can identify conceptual weaknesses in the roles as well as weaknesses in rules.
- Compliant access provisioning. CSI tools enables compliant access provisioning with workflow for access request, policy analysis, approvals, and access fulfillment.
- Transaction and role analysis. CSI tools uses the executed transaction information to report if SoD conflicts or critical functionality in SAP systems have been executed by users (together with the frequency of usage and last date it was used). This executed transaction information is used to maintain and build roles.
- Emergency access management. CSI tools allows for emergency access management and monitoring of emergency access given in those situations that the organization needs to react and do something quickly.
- Role management and design. CSI tools has advanced functionality to help organizations design and manage roles in the SAP environment and to streamline role redesign based on SoD conflicts and role usage. Roles can even be built automatically through the use of CSI tools. CSI tools provides a complete solution to define SAP roles and assignments and is used to build composite roles.
- Access certification. CSI tools provides a streamlined ability to manage access certification to ensure that the organizations users are given the access rights they need and no more.





- Reporting & dashboards. CSI tools has advanced reporting capabilities that allows organizations to customize queries and reports to their specific scenarios and needs.
- Access remediation. CSI tools enables the process of remediation upon determining there is a conflict through analysis of how access is being given and used and defining remediation tasks to be taken. CSI tools provides answers to questions like: Is the access appropriate? How is the user getting access to these conflicts? Is the user really using this critical functionality and by which roles?
- License manager. CSI tools has a license manager to simulate how SAP licenses will be used given role redesign. The license manager analyzes if the correct SAP licenses are assigned in the SAP system that delivers insights if users and roles are assigned to the correct SAP license. This makes it also possible to simulate how much organizations can save if access rights are reduced.
- Controls organizer. CSI tools documents risks and controls throughout business processes and sub-processes. Control measures like compensating controls can be assigned to mitigate risks and by which configuration controls of SAP settings can be checked automatically. All monitoring and audit evidence is stored.
- Quality assurance. CSI tools has integrated checks to make sure roles are defined and built correctly.
- Codification. CSI tools defines the hierarchical structure on the what and where. Both organizational and non-organizational values can be documented centrally to automate role derivation.

### **Considerations for CSI tools**

Every solution has its strengths and weaknesses, and may not be the ideal fit for all organizations in all situations. While GRC 20/20 has identified many positive attributes of CSI tools to enable GRC programs in access control and SoD monitoring in SAP environments — readers should not see this as a complete and unquestionable endorsement of CSI tools.

Overall, clients have shown a high degree of satisfaction with their use and implementation of CSI tools. Clients have a lot of positive feedback of the solution and find it to be a critical and sustainable platform to their future



SAP access control and SoD monitoring strategies. GRC 20/20 routinely finds that clients are satisfied with CSI tools and find the organization has great customer service and rapidly addresses questions and issues. One organization reported they were very suspicious of CSI tools as they took a different approach to SAP access controls with a focus on authorization objects instead of transaction codes, but was very surprised and pleased with the results, which were always accurate.

Clients of CSI tools do see opportunity for further development and growth within the solution. Clients consistently report they would like to see CSI tools expand to support other ERP systems beyond SAP as they work in a heterogeneous environment. CSI tools has been working hard on user experience and ease of use, but some aspects of the solution organizations find take a level of technical expertise to understand that the average business user needs education on.

CSI tools' article, published in SAPInsider - special report GRC Guidebook<sup>2</sup>

## FEATURED IN



### Maximize the Return on Investment from Your GRC Solutions

#### 13 Essential Elements of Top-Performing GRC Software

The governance, risk, and compliance (GRC) market has expanded dramatically in recent years, with an array of options now available to speed the GRC process and help companies manage compliance in an effective and efficient way. Investing in the correct GRC solutions can yield a high return on investment and greatly enhance an organization's security. To achieve benefits, you need to make sure your solution can handle your GRC needs. The best GRC solutions stand out from the competition with 13 key components:

- **Remediation.** GRC reporting is not only about segregation of duties (SoD) conflicts. It is also about the remediation of these conflicts. You can't mitigate risk without insight into its underlying causes, therefore, the GRC solution must provide the answers to questions like: Is the access appropriate? How is the user getting access to these conflicts? Is the user really using this critical functionality?
- **Flexibility.** Organizations are dynamic and it's essential that solution elements (such as rule sets) are easily adjustable. Changes made to an element of the rule set must be inherited automatically to all related layers of this element to maintain consistency.
- **Fast, relevant results.** The analysis is a snapshot of the SAP system and must contain relevant, timely data.
- **Independence.** The audit department must be able to perform independent audits, using an independent tool with an audit rule set.



- **Short implementation time.** Within one week after implementation, the first results should be reported.
- **Reporting of real issues.** Focus on data elements rather than on transaction codes to report the real issues in understandable and aggregated reports.
- **User-friendliness.** To save time and reduce errors, tasks must be easy to perform and automated if possible.
- **Efficient** role building. Build SAP roles automatically to reduce errors and save time. Use reverse engineering and information about the transactions that were used (STAD data).
- **On-the-fly documentation.** You need to be able to simultaneously implement and document the business process with risks and controls, step by step.
- **Simulation.** Change requests for the users and roles can lead to new GRC implications such as SoD conflicts and unwanted access to critical data. Before implementing changes, the GRC implications must be simulated.
- **Trending information.** Clear insight into the audit results and analysis must be available over time.
- **Full scope.** All SAP systems, even smaller ones, should be included in the scope of the GRC process.
- **Mass changes.** Besides the small changes such as user requests, it is also possible that mass changes to the authorization concept (e.g., implementing new modules or merging organizational levels) are needed. These mass changes must be fully supported.

## An Evolving Approach

CSI tools has been providing targeted products for SAP solutions for GRC since 1997. CSI has kept pace with an evolving market, releasing an entirely new software suite in 2014 consisting of CSI Authorization Auditor 2014, CSI Role Build & Manage 2014, CSI Integrate & Collaborate 2014, CSI Emergency Request and CSI Automated Request Engine 2014. The 13 features recommended above are all included; with supporting rule sets, frameworks, options to automate tasks and change requests, dashboards, trending reports, remediation information, integration with SAP Identity Management, active directory integration, and more. The GRC rule set can also be checked for errors using CSI tools. CSI tools' products are designed

to help companies become and remain compliant in all areas. The CSI tools have been adopted by internal and external auditing companies, GRC consultants, and multinationals for use with SAP solutions for GRC. Consider these two sample scenarios in which CSI tools display key GRC features.

*Sample Scenario 1: Remediation*

The SAP user ID "User002" is used by Jeroen Jacobs. This user has access to critical functionality, causing an audit issue. The report in the system shows the single roles and profiles causing the access, via which composite roles the user has the authorizations or transactions assigned, and if the user is using transactions from these roles (see Figure 1). The report shows that the user is using the transaction codes from the composite role, not the single role. To solve this issue, the single role could be removed from this composite role because the transactions from the single roles are not being used.

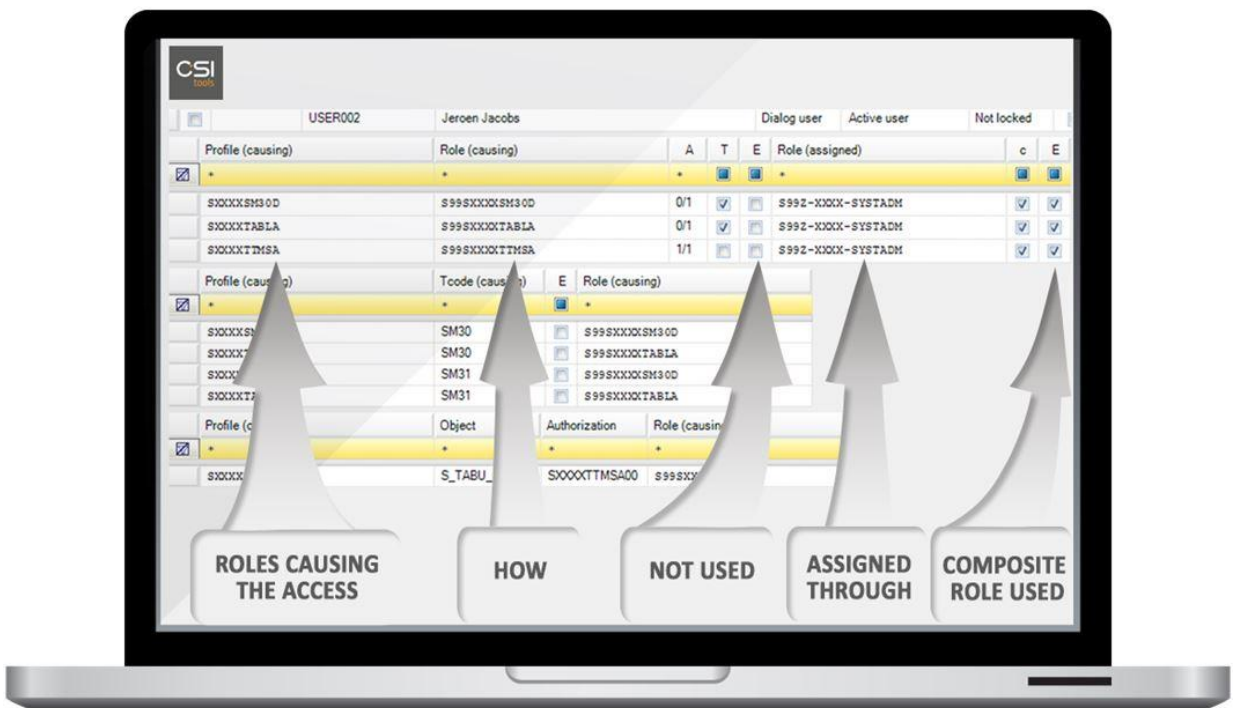


Figure 1: Report used for the remediation of access issues

*Sample Scenario 2: Checking for Errors in GRC Rule Sets. The results of an analysis show that a user has access to critical functionalities (see Figure 2). For some functionality the user is assigned authorization, but is not assigned the transaction code. This shows an inconsistency in the rule or the role because the user has access to the data but cannot use the audited transaction code. There may be a custom transaction code missing in the rule set. It also shows that a user has access to some critical functionality because the transaction code and authorizations are assigned. But because the user did not execute the transaction codes for this critical functionality, the access rights for this functionality should be removed from this user.*

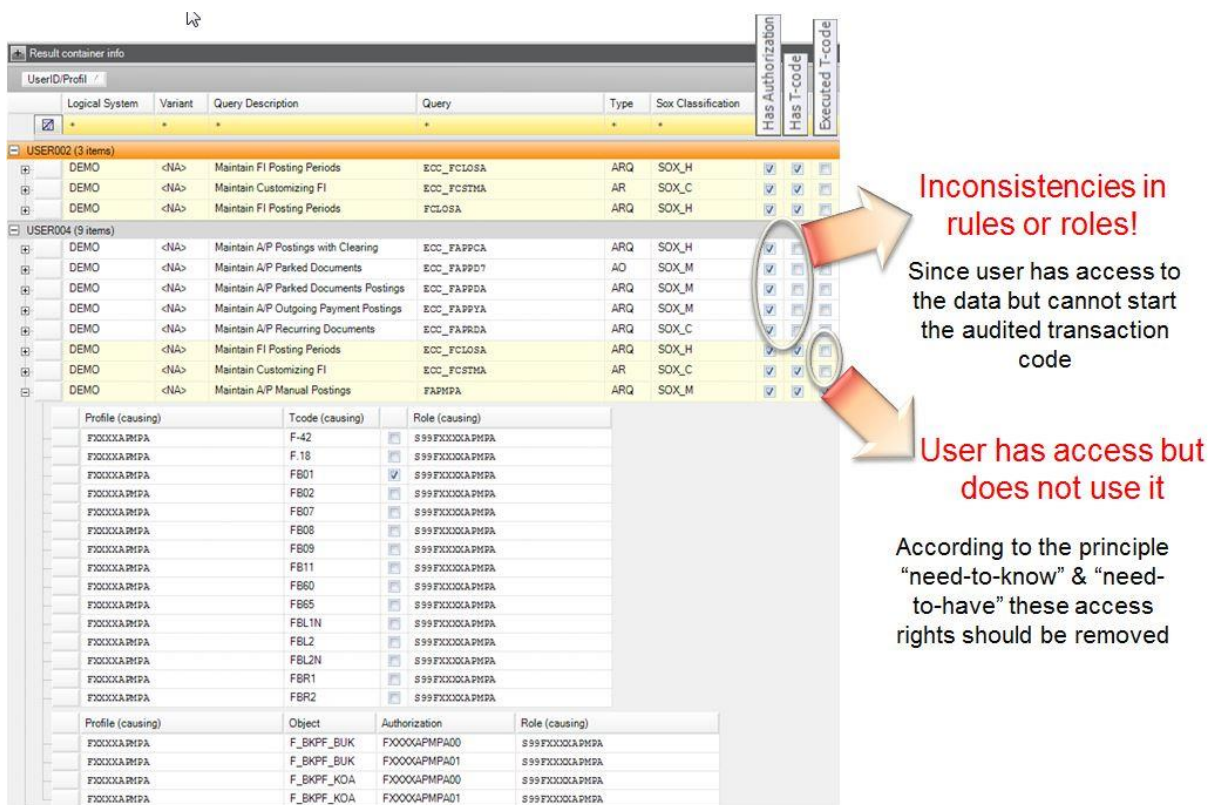


Figure 2: Checking the correctness of rule sets and roles

### Learn More

CSI tools has developed dynamic analytics tools that deliver intelligence to and from SAP environments. Our cockpit and engine provide insight into vulnerabilities, streamline SAP roles, and deliver practical solutions to improve risk and security posture, including automated role building and reverse engineering.



CIOReview's Annual List showcases the 100 Most Promising SAP Special Solution Providers 2015. CSI tools makes it to CIOReview's top SAP Special Solution Providers list for developing dynamic analytics tools to deliver intelligence from and to decisions taken in access governance for SAP environments. <sup>[3]</sup>

# CIOReview

The Navigator for Enterprise Solutions

SAP SPECIAL

APRIL - 10 - 2015

CIOREVIEW.COM

## CSI tools - Streamlining SAP Roles Using Cockpit

Johan Hermans, Founder and CEO of CSI tools explains that the SAP security projects consume enormous budgets without really improving the security, due to misunderstanding of the SAP security basics and SAP authorizations. Scores of security administrators do not know the actual number of transaction codes and authorization objects that exist in an SAP system. "Most people think that they can protect SAP systems by removing and assigning transaction codes to users," says Hermans. The reality, however, is completely different. Only the authorization objects assigned to a user gives them the permission to access the data, regardless of the user's ability to execute the transaction. "Devoid of going into the details how SAP security really works, everybody understands that if security administrators, auditors, and internal control teams do not understand the basics of the two core elements of SAP security, they will never be able to optimize it," notes Hermans.

Even the early versions of SAP systems did not have security checks for starting a transaction code. Setting up security was complex because the security administrator had to think and develop security with a complete insight and understanding of the authorizations.

**"Our cockpit and engine provide insights into real vulnerabilities, streamlining SAP roles and then delivers practical solutions to improve risk and security posture"**



CSI tools appears in the picture to tackle the obstacles for the concerned sector—a company that develops dynamic analytics tools to deliver intelligence from and to decisions taken in access governance for SAP environments. The company’s unique cockpit and engine provide insights into real vulnerabilities, streamlining SAP roles and then delivers practical solutions to improve risk/security posture, like automated role building and reverse engineering.

The company has kept pace with the evolving market, releasing an entirely new complete and mature GRC solution for SAP environments in 2014: CSI tools 2014 is designed to address all GRC needs,—with supporting rule sets, frameworks, options to automate tasks and change requests and dashboards.

By checking multiple layers of SAP authorizations, CSI tools ensures that Segregation of Duty (SoD) conflicts through accumulation of access rights are discovered. CSI tools is also used to find and correct errors in GRC rule sets.

The products are designed to help companies get and remain compliant in all areas. CSI Authorization Auditor 2014 is the audit and monitoring application for security concepts in SAP environments. It takes a snapshot of the SAP system to gain an insight into the past or current authorization setup of the concerned system. It reveals weaknesses in customer’s authorization concept, and helps identify undesired authorizations, accumulation of access rights, unsecured back doors and cross-system segregation of duties. CSI Role Build & Manage (CSI RBM) is used to maintain and manage the SAP security concept in an efficient and effective way with features like automated role building. CSI Automated Request Engine (CSI ARE) processes user and role access requests and has integrated SoD checks to prevent unwanted access in the access requests. Tasks can be automated and scheduled using CSI Integrate & Collaborate (CSI IC). CSI Emergency Request (CSI ER) is an automated emergency procedure with firefighter capabilities to mitigate the risk and allows a timely response of the intervention team, to provide broad access to a SAP system with full evidence logging. CSI ER also provides functionality to log and monitor the access (display and/or update) to SAP HRM Infotypes.





Going forward, CSI tools wants to improve the SAP request procedures to manage security in a better way. Preventing unwanted access and SoD conflicts instead of monitoring and solving them is much more efficient way to set up SAP security.” Concludes Hermans.



CSI tools has been granted a product and innovation leadership position<sup>5</sup> in:

**KuppingerCole's Leadership compass Access Control / Governance for SAP environments**

In its July 2015 Leadership Compass of the KuppingerCole Report, analysts Matthias Reinwarth and Martin Kuppinger have examined the control of business oriented processes by applying SoD rules, the management of privileged users (including mechanisms of well-defined ad hoc access in case of emergency), the versatility of implemented role modeling capabilities, quality and size of the provided rule base and the provided functionality for the implementation of life-cycle and workflow processes including certification, recertification and attestation.

CSI tools has been granted a product and innovation leadership position in the Access Control / Governance for SAP Environments leadership compass, where the analysts specifically looked at the functional strength and completeness of products or, in this case, suite.



Innovation Leader  
**Access Control / Governance  
for SAP environments**

July 2015



Product Leader  
**Access Control / Governance  
for SAP environments**

July 2015

„CSI tools deliver a highly interesting solution providing a broad overall coverage of functionality for organizations looking into Access Governance for SAP environments. The CSI tools product suite with its functionalities for SAP Access Governance, role design, user activity monitoring and the handling of emergency access which can be deployed in various scenarios“ Matthias Reinwarth, Senior Analyst at KuppingerCole.

CSI tools' extract of the report<sup>5</sup>



## Access Control / Governance for SAP environments

### Product Evaluation

This section contains a quick rating for every product we've included in this report. For some of the products there are additional KuppingerCole Reports available, providing more detailed information.

In the following analysis we have provided our ratings for the products and vendors in a series of tables. These ratings represent the aspects described previously in this document. Here is an explanation of the ratings that we have used:

- **Strong Positive:** this rating indicates that, according to our analysis, the product or vendor significantly exceeds the average for the market and our expectations for that aspect.
- **Positive:** this rating indicates that, according to our analysis, the product or vendor exceeds the average for the market and our expectations for that aspect.
- **Neutral:** this rating indicates that, according to our analysis, the product or vendor is average for the market and our expectations for that aspect.
- **Weak:** this rating indicates that, according to our analysis, the product or vendor is less than the average for the market and our expectations in that aspect.
- **Critical:** this is a special rating with a meaning that is explained where it is used. For example it may mean that there is a lack of information. Where



this rating is given it is important that a customer considering this product look for more information about the aspect.

It is important to note that these ratings are not absolute. They are relative to the market and our expectations. Therefore a product with a strong positive rating could still be lacking in functionality that a customer may need if the market in general is weak in that area. Equally in a strong market a product with a weak rating may provide all the functionality a particular customer would need.

### 11.1 CSI tools

CSI tools is a privately-held Belgian company specializing in providing dynamic analytics tools for access governance for SAP environments. They provide a suite of five individually licensable products for key GRC aspects such as authorization auditing, workflows and role analysis. The product layout allows for providing an analytics desktop system connecting to one or potentially more SAP installations for analytics or management, or for a full integration within a client/server environment to be deployed at all levels of a customer organization.

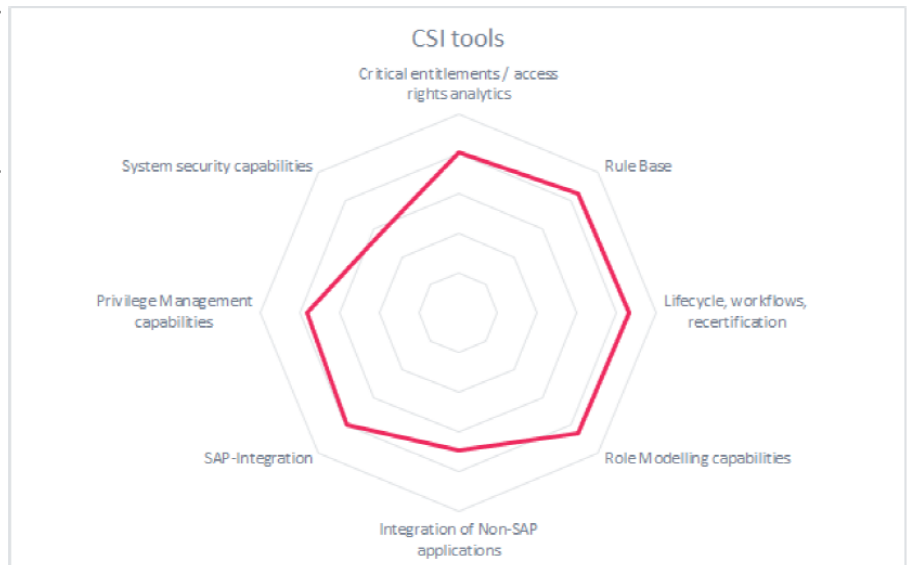
Strengths/Opportunities	Weaknesses/Threats
<ul style="list-style-type: none"> <li>● Large track record of covered SAP installations through licensing to many large accounting firms</li> <li>● Fast results through a sophisticated multi-level analytics approach</li> <li>● Complemented with a strong set of innovative features unique to this solution</li> </ul>	<ul style="list-style-type: none"> <li>● International partner ecosystem rather small (besides their cooperation with various accounting firms)</li> </ul>

Table 3: CSI tools Strengths and Weaknesses

The product comes with an impressive out-of-the-box functionality providing immediate results from sophisticated analytics. The software implements a large set of innovative additional functionalities, including, e.g., user activity monitoring, the ability to define normal usage and identify deviations therefrom, and role mining including the analysis and redesign of roles.

<b>Security</b>	strong positive
<b>Functionality</b>	strong positive
<b>Integration</b>	strong positive
<b>Interoperability</b>	strong positive
<b>Usability</b>	positive

Table 4: CSI tools Rating



Overall, CSI tools is a very interesting solution for customers looking for a product suite that can be deployed in various scenarios. One option is

to either deploy it for instant analytics, another is to implement it for a sustainable deployment for longer running analyses and continuous improvement of SAP Access Governance, role design, user activity monitoring and emergency access handling. Organisations searching for solutions to specialised tasks might want to look into the additionally provided functionality included in the CSI tools product suite.

Apart from its successful partnering with major audit companies we still see room for improvement regarding the partner ecosystem.

CSI tools has received a 2015 GRC Innovation award<sup>6</sup> :

**CSI tools Receives 2015 GRC Innovation Award for GRC Solution Provider in the category Automated/Continuous Control Management**

**Herent, September 22 2015** – CSI tools, a leading provider for SAP access governance solutions, today announced that CSI Emergency Request has been honored with a 2015 GRC Innovation Award in the Automated/Continuous Control Management category by GRC analyst firm GRC 20/20. The 4th annual GRC Innovation Awards recognize technology innovations and user experience in Governance, Risk Management and Compliance programs and processes.



“CSI tools has demonstrated GRC innovation in Automated/Continuous Control management with CSI Emergency Request delivering a solution to manage and control emergency activities in SAP systems and safeguarding SAP HR employee data according the strict privacy regulations that are applicable in countries like Germany and Belgium,” said Michael Rasmussen, Chief GRC Pundit for GRC 20/20 and internationally recognized expert. “It is imperative that we recognize today’s successes as a milestone toward advancing GRC maturity. In achieving maturity, GRC is part of the organization’s strategy and operations and supported by a range of technology, knowledge and services - enabling the organization to achieve greater efficiency, effectiveness and agility in GRC processes and broader business operations.”

“Besides offering a solution to keep the companies emergency access rights in control, CSI Emergency Request fully complies with the Belgium and German law and regulations regarding safeguarding the HR employee data. We are very happy and proud that GRC 20/20 recognizes our unique features and effective solution.” - Johan Hermans, CEO of CSI tools.

CSI Emergency Request is part of the CSI tools GRC suite for SAP environments. CSI Emergency Request supports the whole emergency access procedure including all mailings and audit log evidence. Besides this CSI Emergency Request is the only solution on the market that gives insight who saw and/or who manipulated HR employee data on screens (insight in users HR Info type access).



With CSI Emergency Request you have an efficient, effective and agile solution for emergency access and safeguarding HR info type access:

- In control of emergency access users
- Compliance with law and regulations regarding safeguarding of HR employee data
- Have proof of actions for audit
- Automate time consuming processes
- Allow flexibility in providing broader access rights when needed, without manual interaction, but still with full evidence
- Be in control of exceptional situations and know what people are doing
- Be aware of access made to your critical HR data

#### *About CSI tools*

*CSI tools has been on the market with their solutions for SAP access governance since 1997 and provides analytic control solutions that audit and monitor SAP environments, manage and validate authorizations, and build roles tuned to the organizations security requirements and business needs.*

#### *About GRC 20/20*

*GRC 20/20 is the authority in understanding how organizations implement GRC practices that are effective, efficient and agile. Through independent research and industry interaction, GRC 20/20 advises the entire ecosystem of GRC roles within organizations, technology and knowledge solution providers, and professional service firms. Organizations engage GRC 20/20 when they need insight, guidance and advice in dealing with a dizzying array of disruptive issues, challenges, processes, information and technologies while trying to maintain control of a distributed and dynamic business environment. Visit GRC 20/20 at <http://www.grc2020.com/> and follow on Twitter at @GRCPundit.*

*CSI tools Media Contact:*

*Meta Hoetjes*

*CSI tools*

*meta.hoetjes@csi-tools.com*

*+31 6 24 651 761*

*GRC 20/20 Media Contact:*

*Michael Rasmussen*

*The GRC Pundit @ GRC 20/20 Research, LLC*

*mkras@grc2020.com*

*+1 888.365.4560*



CSI tools is nominated as one of the finalists for the 2015 IPACSO awards <sup>7</sup> :



**Herent, October 2015,** CSI tools is pleased to announce that we are nominated as one of the finalists for the 2015 EU Cyber Security and Privacy Innovation Awards.

Each year in October, Europe's most innovative and forward-thinking researchers and entrepreneurs gather in Brussels, recognizing those who are bolstering Europe's cyber security landscape. With the awards, the IPACSO consortium supported by the European Commission under FP7, support Privacy and Cyber Security Innovations 'Made in Europe'.

CSI tools' unique approach to the Access Governance of SAP environments is nominated: The challenge of SAP security is first to really understand how it works. CSI tools gives his customers guidance to simplify the complexity by splitting it into two layers, a governance layer and a technical layer.

The main advantage is that access governances become transparent; management can focus on the governance aspects and the technical people can focus on technical layer and get the instructions through the governance layer.

CSI tools simplifies SAP security and makes it understandable for all layers of the organization. CSI tools has a unique approach and structures the (difficult to understand) technical security data, into 300 data elements that are easy to understand and interpret within all layers of the organization. These data elements covers all control objectives for the confidentiality, Integrity and availability of the SAP data and are used to define the security requirements in an understandable and correct way.

"CSI tools promotes analyzing, reporting and remediation on the real risks and vulnerabilities for access governance in SAP and delivers complete solutions for this. We are very happy and proud that IPACSO recognizes our unique features and effective approach. Being recognized, we can continue spreading the word and help organizations with their SAP access governance"- Johan Hermans, CEO CSI tools





#### *About CSI tools*

*CSI tools has been on the market with their solutions for SAP access governance since 1997 and provides analytic control solutions that audit and monitor SAP environments, manage and validate authorizations, and build roles tuned to the organizations security requirements and business needs.*

#### *About IPACSO*

*IPACSO (Innovation Framework for Privacy and Cyber Security Market Opportunities) is a private consortium aimed at supporting Privacy and Cyber Security innovations in Europe. Its aim is to support ICT Security innovators with State of the Art methodologies and best practices in their innovation process, that will help them to find their road to market faster, more effective and more efficient. IPACSO is supported by the European Commission, and aims to improve the competitiveness of the European Cyber Security & Privacy market. Alongside LSEC, VASCO Data Security, the Waterford Institute of Technology and Espion, both from Ireland, and the German Institute for Economic Research make up the rest of IPACSO. With the Cyber Security & Privacy Innovation Awards, the IPACSO consortium, supported by the European Commission, awards Privacy and Cyber Security Innovators in Europe. Out of a hundred nominees, an independent commission created a short list of 20 companies with the most innovative products and services in the security and privacy domains, and today will announce the winners per each of the categories.*

#### *Contact information*

Meta Hoetjes

Meta.hoetjes@csi-tools.com

www.csi-tools.com

## CSI tools: Pragmatic Solutions for SAP Security



**Johan Hermans**  
Founder & CEO

Every single day, successful companies are reinventing themselves, resulting in constantly assessing their risk exposure by finding inconsistencies in what people are allowed to do, can do, did and can almost do. CSI tools have developed dynamic analytics tools that deliver intelligence from and to decisions taken in identity and access governance for SAP environments.

CSI tools' cockpit and engine provide insight into your real vulnerabilities, streamline SAP roles and then delivers practical solutions to improve your risk/security posture, like automated role building and reverse engineering. By transforming data into information, these tools allow you to adjust on demand your risk and security strategies. They use your SAP systems to identify the access governance requirements and allow you to sync them with the SAP systems employed.

While dealing with SAP security, first roadblock is to understand how exactly it works? CSI tools give guidance to simplify this complexity by splitting it into two layers: a **governance layer** and a **technical layer**. So that the access governances become

transparent, while management can focus on the governance aspects, the technical people can focus on technical layer and get the instructions through the governance layer.

**Top-tier CSI tools**  
**CSI Authorization Auditor 2014**, is the audit & monitoring application for the authorization and role setup in SAP environments.

**CSI Role Build & Manage 2014**, supports the SAP authorization processes with fully automated SAP role building. By documenting all security requirements the application can build all SAP roles automatically.

**CSI Integrate & Collaborate**, enriches CSI Authorization Auditor 2014 Client/Server and / or CSI Role Build & Manage Client/Server.

 **We developed dynamic analytics tools that deliver intelligence from and to decisions taken in identity and access governance for SAP environments**

**The CSI Automated Request Engine**, is a middleware application that processes user access requests based on XML input and generates XML output with the SoD results.

**CSI Data Xtractor**, is used to export tables from any SAP system and import SAP data into MS Access .mdb, MS Excel .xls and/or .xml files or to take data offline and examine them as an independent data viewing tool.


**CSI Emergency Request**, is an ABAP/4 based solution consisting of two components, to manage and control emergency activities and HR Infotype access.

Known as an independent software development company, CSI tools has developed software solutions for Access Governance of SAP environments since 1997. CSI tools has received many awards in 2015 for its innovations and products. In 2016, CSI tools is also planning to provide its solutions as a SaaS solution.

**Johan Hermans, Consummate Professional of SAP**  
Johan Hermans, founder & CEO of CSI tools, started his career as a Financial Auditor and evolved to IT Auditor in 1997, with the foundation of CSI Belgium, which specialized in SAP authorizations, security and internal controls. He then specialized in internal controls and security for SAP environments. Later it in 2008 it split into axl & trax - a service company providing SAP Access

Governance services and CSI tools - an independent software company.

Today, Johan is responsible for the general management of CSI tools and a regular speaker at International conferences as well as a guest-professor at universities. His vision is reflected in the software applications of CSI tools which is worldwide recognized by numerous multinationals and research firms.

Johan says, "Use innovation to grow your business. Introducing new ideas to the business and successful exploitation of these new ideas is crucial for business to improve its profitability." 



CSI tools is one of 50 most valuable tech companies by Insight Success

**Insights Success Lists CSI tools as one of "50 Most Valuable Tech Companies"**

**Middletown, DE** – January 2015 – Insights Success ([www.insightssuccess.com](http://www.insightssuccess.com)) has chosen CSI tools ([www.csi-tools.com](http://www.csi-tools.com)) for its 50 most valuable tech companies.



**Most Valuable Tech Companies**

Insights Success is a platform that focuses distinctively on emerging as well as leading IT companies, their confrontational style of doing business and way of delivering effective and collaborative solutions to strengthen market share. Our magazine talks about leaders and orators from the world of technology, which includes CEO's, CIO's, VP's, Managers and other professionals who had set a benchmark in the revolution of IT industry. "Every single day, successful companies are reinventing themselves, resulting in constantly assessing their risk exposure by finding inconsistencies in what people are allowed to do, can do, did and can almost do. **CSI tools** have developed dynamic analytics tools that deliver intelligence from and to decisions taken in identity and access governance for SAP environments."

"Johan says, "Use innovation to grow your business. Introducing new ideas to the business and successful exploitation of these new ideas is crucial for business to improve its profitability. We are proud to be recognized by Insights success' panel of experts and the market"

*About CSI tools*

*CSI tools has been on the market with their solutions for SAP access governance since 1997 and provides analytic control solutions that audit and monitor SAP environments, manage and validate authorizations, and build roles tuned to the organizations security requirements and business needs.*

*About Insights success*

*Insights Success is a forum where top leaders and executives talk and share about their experiences, views, and mantra for success which will help the young and dynamic bloodline of professionals to learn, cater and deliver business needs for customers in order to become futuristic market leaders.*

CSI tools' article in CIO Story December 2015

## CSI tools: Guiding Customers To Simplify the Complexity

Johan Hermans, CEO

**CSI tools helps managing security  
in a better way by introducing a  
new innovative and user friendly  
SAP request procedure.**



According to Johan Hermans, CEO, CSI tools, SAP security projects consume enormous budgets without really improving the security. 90% of the security administrators do not know how many transaction codes and authorization objects exist in a SAP system and their purpose, observes Johan. Most people think that they can protect SAP systems by removing and assigning transaction codes to users and that the purpose of authorization objects is to restrict certain organizational levels like company codes, plants, sales organizations etc.

The reality is however completely different: Only the authorization objects assigned to a user gives this user the permission to access the data, regardless if this user can execute the transaction. In a SAP system there can be more than 150.000 transaction codes and there are only 1.200 authorizations objects.

Johan believes that the challenge of SAP security is first to really understand how it works. CSI tools give its customers guidance to simplify the complexity by splitting it into two layers – a governance layer and a technical layer. The main advantage lies in the fact that access governances become transparent. The management can focus on the governance aspects and the technical people can focus on technical layer and get the instructions through the governance layer. CSI tools have a unique approach. They structure the technical security data into 300 data elements that are easy to understand and interpret within all layers of the organization.

The company has rendered its services to several enterprises in multiple domains. In terms of Role Management and Design, CSI tools has advanced functionality that



helped organizations design, build (even automatically) and manage roles in the SAP environment and to streamline role redesign based on SoD conflicts and role usage. Another category is the SAP security audits in which CSI tools has helped organizations not only to create correct GRC reports and analyses but also helped mitigating the risks. The organization has also helped businesses with emergency access management and monitoring of emergency access given in those situations that the organization needs to react and do something quickly.

The reason why enterprises decide to choose CSI tools as their solution for SAP access governance is manifold. In terms of efficiency, CSI tools has been characterized with cost savings in employee time designing user roles in context of company changes, less spending not only on external, also internal consultants to do manual control validation and SoD monitoring, and efficiency in assigning and determining appropriate access, amongst others. As for effectiveness, their customers have testified to reduction in auditor findings related to SoD conflicts, reduction in risk exposure as well as business disruption through stronger control enforcement and monitoring, and ability to customize queries to solve specific authorization challenges.

CSI tools helps managing security in a better way by introducing a new innovative and user friendly SAP request procedure. CSI tools' focus is not only supporting risk reporting, but also on risk mitigation. The company is proud on their unique approach and functionality that is finally being recognized by the market. Thus far, the organization is content that their products have been well received and that they have been rewarded for their innovation. This is evident of the fact that they have had an excessive growth in customers and products selling.

Company: CSI Tools

Quote: "CSI tools helps managing security in a better way by introducing a new innovative and user friendly SAP request procedure."



CSI tools is nominated as one of 25 most powerful SAP solution provider by CIO Story

**CIO Story Lists CSI tools as one of "25 Most Powerful SAP Solution Providers"**



**Campbell, CA** – January 2015 – CIOStory ([www.ciostory.com](http://www.ciostory.com)) has chosen CSI tools ([www.csi-tools.com](http://www.csi-tools.com)) for its 25 most powerful SAP solution provider 2015.

A digital technology magazine focusing on the disruptive power of technology, CIO STORY features companies that have built better growth models with innovative enterprise solutions. "CSI tools helps managing security in a better way by introducing a new innovative and user friendly SAP request procedure. CSI tools' focus is not only supporting risk reporting, but also on risk mitigation. The company is proud on their unique approach and functionality that is finally being recognized by the market. Thus far, the organization is content that their products have been well received and that they have been rewarded for their innovation. This is evident of the fact that they have had an excessive growth in customers and products selling."

"CSI tools simplifies the complexity of SAP security with an unique approach. We are honored that this approach and our solutions are being recognized by CIOStory's panel of experts and thought leaders and the market," said Johan Hermans, Founder and CEO, CSI tools.

*About CSI tools*

*CSI tools has been on the market with their solutions for SAP access governance since 1997 and provides analytic control solutions that audit and monitor SAP environments, manage and validate authorizations, and build roles tuned to the organizations security requirements and business needs.*

*About CIO Story*



*CIO STORY makes an incisive study of the IT trends and equips leading businesses with insights and deep analytics based on the success stories of technology companies that have scaled up by adapting path-breaking business strategies and solutions.*

---

#### Sources

- [1] oss notes is an online sap service and the portal that provides updates on patches in different modules of sap and up-to-date information on sap notes. sap notes are correction instructions for the bugs or issues found in standard sap programs. in case relevant notes are not found, sap customers can log the issue with the sap help desk through oss notes, although the service is not extended to objects developed or modified by customers. oss notes provides for the collection of correction notes for sap objects considering the versions and release dates. <http://www.techopedia.com/definition/28734/oss-notes-sap>
- [2] Article from SAPInsiders' special report GRC Guidebook: strategies and tools to mitigate risks, October 2014
- [3] Article from CIO Review's SAP special for 100 Most Promising SAP Special Solution Providers 2015
- [4] CSI tools was mentioned by analysts Anmol Singh and Brian Iverson in Gartner Market Guide for SOD Controls Monitoring Tools on April 28 2015 (Gartner Inc. G00272271)
- [5] KuppingerCole's Leadership compass Access Control / Governance for SAP environments, 2015
- [6] Press release about GRC 2015 Innovation award, 2015
- [7] More information about IPACSO 2015: <http://ipacso.eu/introducing-ipacso-innovation-awards.html>

## About

This document is property of CSI tools BVBA. This is a controlled document; it may not be copied and nothing in it may change without knowledge and consent of CSI tools BVBA. © Copyright CSI tools BVBA 2015. All rights reserved. The information in this document is subject to change without notice. No part of this document may be reproduced, stored or transmitted, in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of CSI tools BVBA.

CSI tools BVBA assumes no liability for any damages incurred, directly or indirectly, from any errors, omissions or discrepancies between the software and the information contained in this document.

Title: SAP Authorization Logic Where did it all go wrong?

First Published: 2014

Fourth release: 2016

Authors:

Johan Hermans <johan.hermans@csi-tools.com>

Meta Hoetjes <meta.hoetjes@csi-tools.com>



SAP and SAP R/3® are registered trademarks of SAP SE Walldorf (D)

CSI Authorization Auditor® is a registered trademark of Control Software International

CSI Automated Request Engine® is a registered trademark of Control Software International

CSI Role Build & Manage® is a registered trademark of Control Software International

CSI Emergency Request® is a registered trademark of Control Software International

CSI Integrate & Collaborate® is a registered trademark of Control Software International

© 2016 CSI tools BVBA [www.csi-tools.com](http://www.csi-tools.com)