



April 19, 2021

# Accurate SOD Reporting without costly and constant maintenance?



Presented by Dries Horions, Product Manager

# Agenda

- Introduction
- Segregation of Duties Matrix
- What Makes it Hard to maintain?
- How can it be simplified?
- Q&A

START

---

# Introduction

**Name:** Dries Horions

**Role:** Product Manager

**Email:** [dhorions@securityweaver.com](mailto:dhorions@securityweaver.com)

I began working with SAP in 2001 as an ABAP developer. I joined Security Weaver 14 years ago. I'm the Product Manager for Separations Enforcer and Automated Mitigations.

# Security Weaver

GRC software since 2004

Fraud prevention, compliance, risk analyses, CCM

Cross platform Compliancy software on Access-,

Process and Contract Compliancy



**SIEMENS**



**AIRBUS**

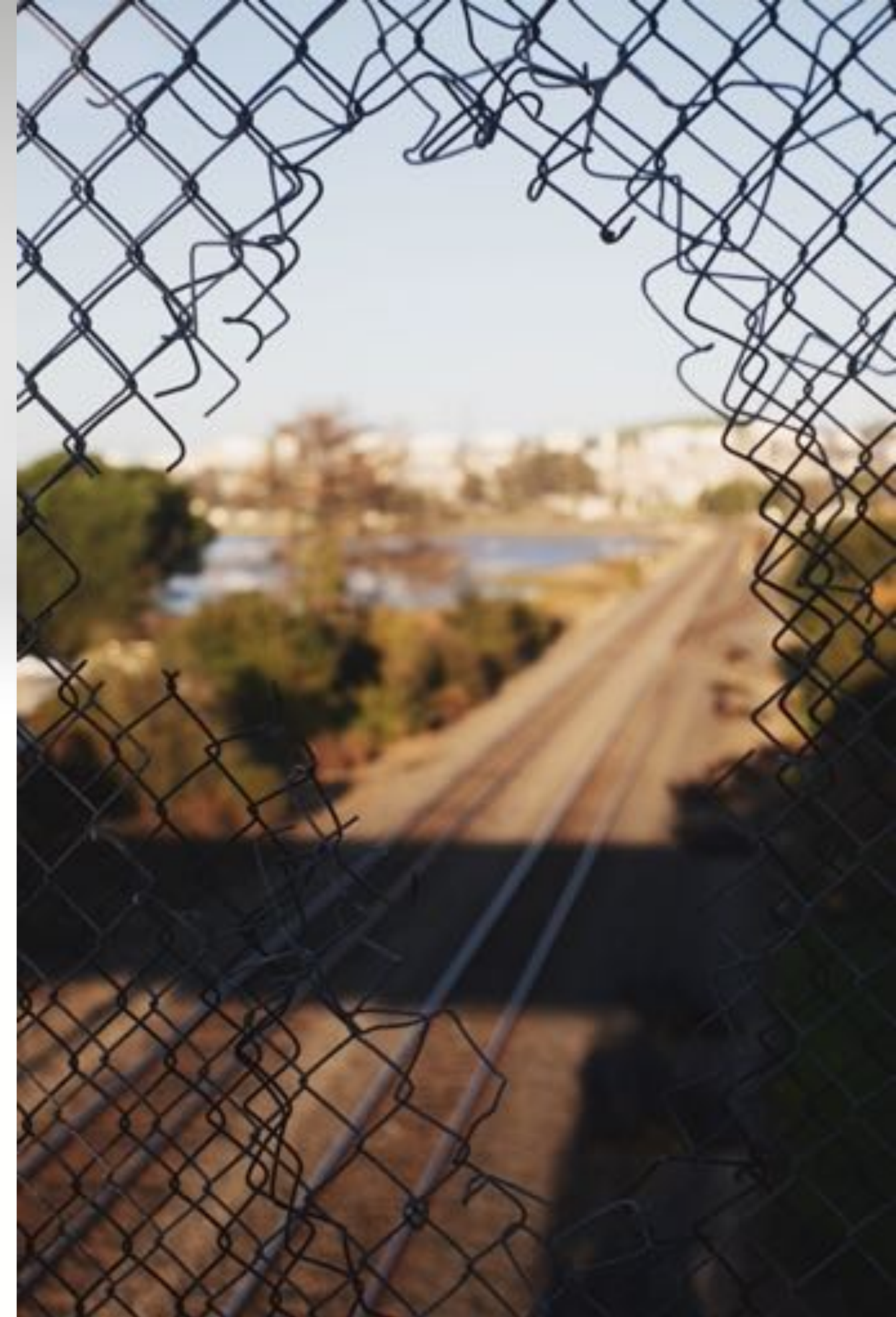
Novo Nordisk  
Pharmatech A/S



# What is an SOD Conflict?

*If a single person can perform a combination of critical activities within a process sequence, this is referred to as a **SOD Conflict**.*

*When that happens, there is a possibility a person did not act in the interests of the company.*



# How is an SOD Conflict Defined?

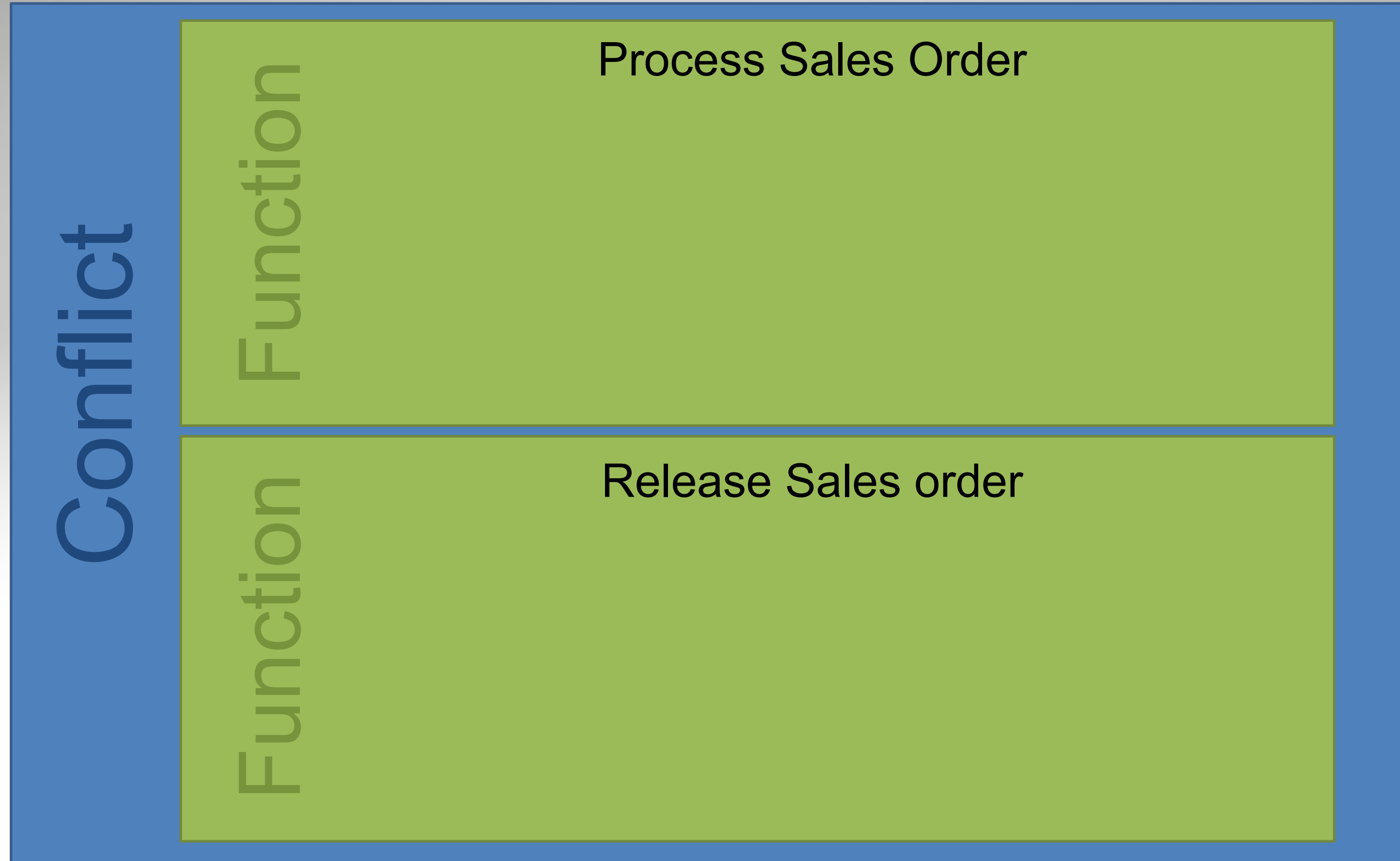
## Conflict

### Create Sales order Vs. Release Sales Order

If the same individual can create sales orders AND release blocked sales orders within SAP, then they can compromise the system without being detected.

With this conflict a user may circumvent proper Order to Cash procedures and either accidentally or maliciously do things like: Entering and releasing sales documents by the same person. As a result, a user can bypass controls to inappropriately manipulate the sales order process and release blocked sales order documents to bypass credit/delivery/billing controls.

# How is an SOD Conflict Defined?



# How is an SOD Conflict Defined?

## Conflict

Function

Process Sales Order

Transaction

VA02 - Change Sales Order

Function

Release Sales order

Transaction

V.23 – Release Sales Order



# How is an SOD Conflict Defined?

## Conflict

Function

Process Sales Order

Transaction

VA02 - Change Sales Order

Object

- V\_VBAK\_AAT – Sales Document Types
  - Activity – Create/Change
  - Document Type
- V\_VBAK\_VKO – Sales Areas
  - Activity – Create/Change
  - Division
  - Sales Organization
  - Distribution Channel

Function

Release Sales order

Transaction

V.23 – Release Sales Order

# How is an SOD Conflict Defined?

## Conflict

### Function

#### Process Sales Order

##### Transaction

#### VA02 - Change Sales Order

##### Object

- V\_VBAK\_AAT – Sales Document Types
  - Activity – Create/Change
  - Document Type
- V\_VBAK\_VKO – Sales Areas
  - Activity – Create/Change
  - Division
  - Sales Organization
  - Distribution Channel

### Function

#### Release Sales order

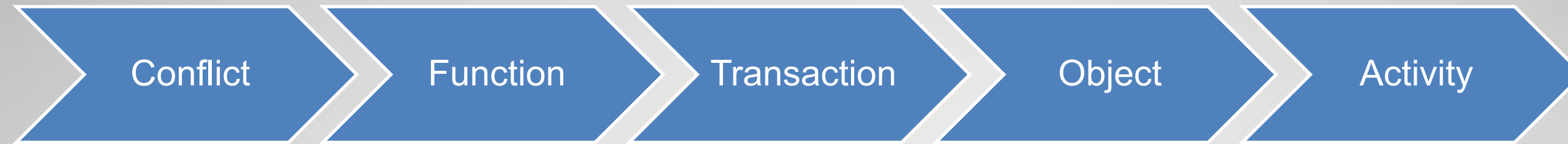
##### Transaction

#### V.23 – Release Sales Order

##### Object

- V\_VBAK\_AAT – Sales Document Types
  - Activity – Release
  - Document Type
- V\_VBAK\_VKO – Sales Areas
  - Activity – Create/Change
  - Division
  - Sales Organization
  - Distribution Channel

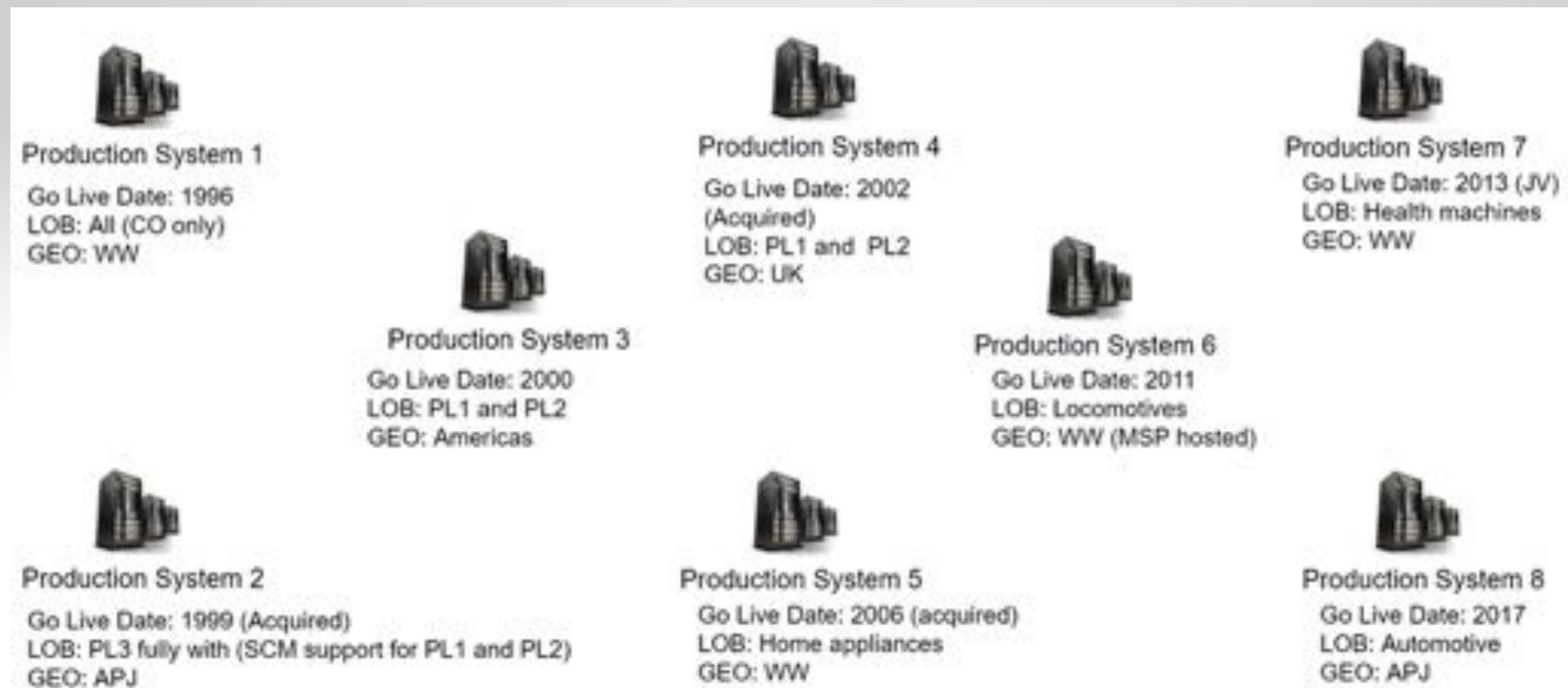
# Why is an SOD Matrix hard to maintain?



When all these aspects are so well known in the industry, what is it that makes an SOD Matrix so hard to maintain?

# Why is an SOD Matrix hard to maintain?

All SAP systems have different configuration, customizing and custom code, and that affects the SOD Matrix,



# Why is an SOD Matrix hard to maintain?

## Object

**V\_VBAK\_AAT** – Sales Document Types

- Activity
- **Document Type**

**V\_VBAK\_VKO** – Sales Areas

- Activity
- Division
- Sales Organization
- Distribution Channel

# Differences in Configuration and Customizing

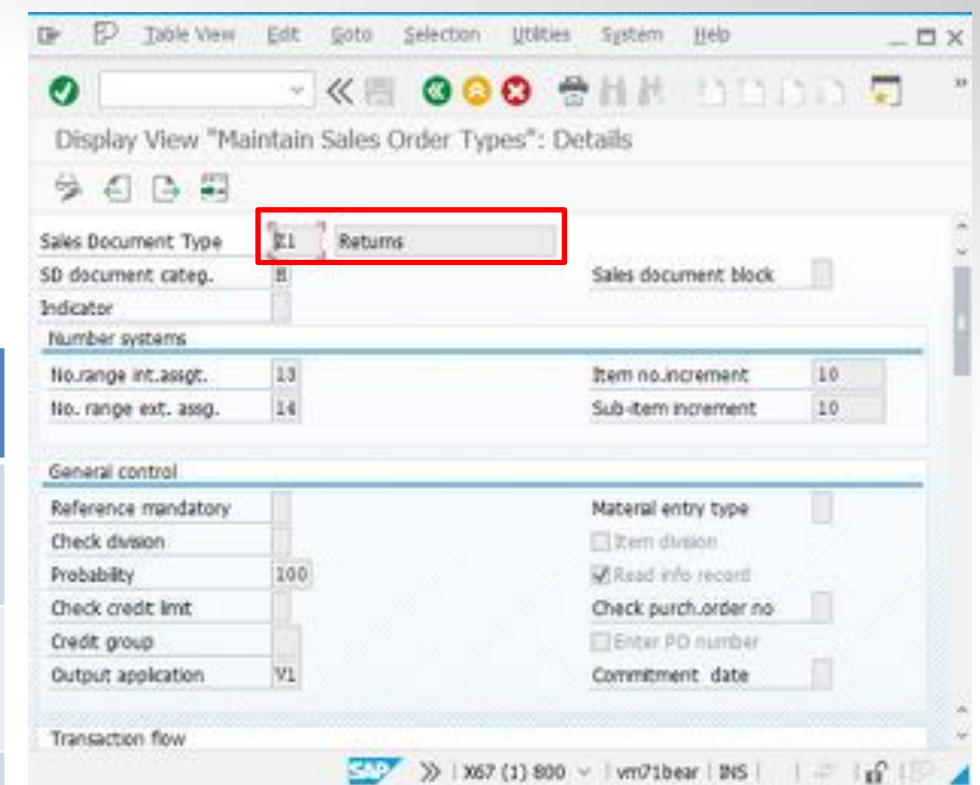
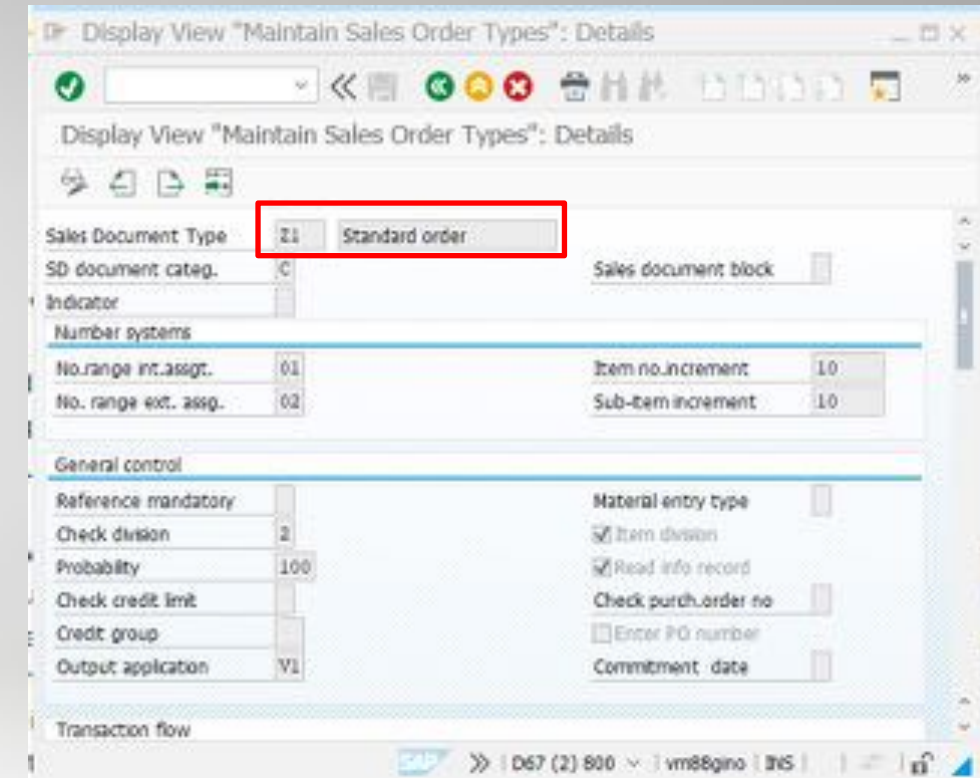
Object

## V\_VBAK\_AAT – Sales Document Types

- Activity
- **Document Type**

## V\_VBAK\_VKO – Sales Areas

- Activity
- Division
- Sales Organization
- Distribution Channel



System	Sales Document Type	Company Code	Division	Sales Organization	Distribution Channel
Production 1	OR – Standard Order Z1 – Returns				
Production 2	Z1 – Standard Order RE – Returns				
Production 3	OR – Standard Order RE - Returns				

# Differences in Organizational Structure

Object

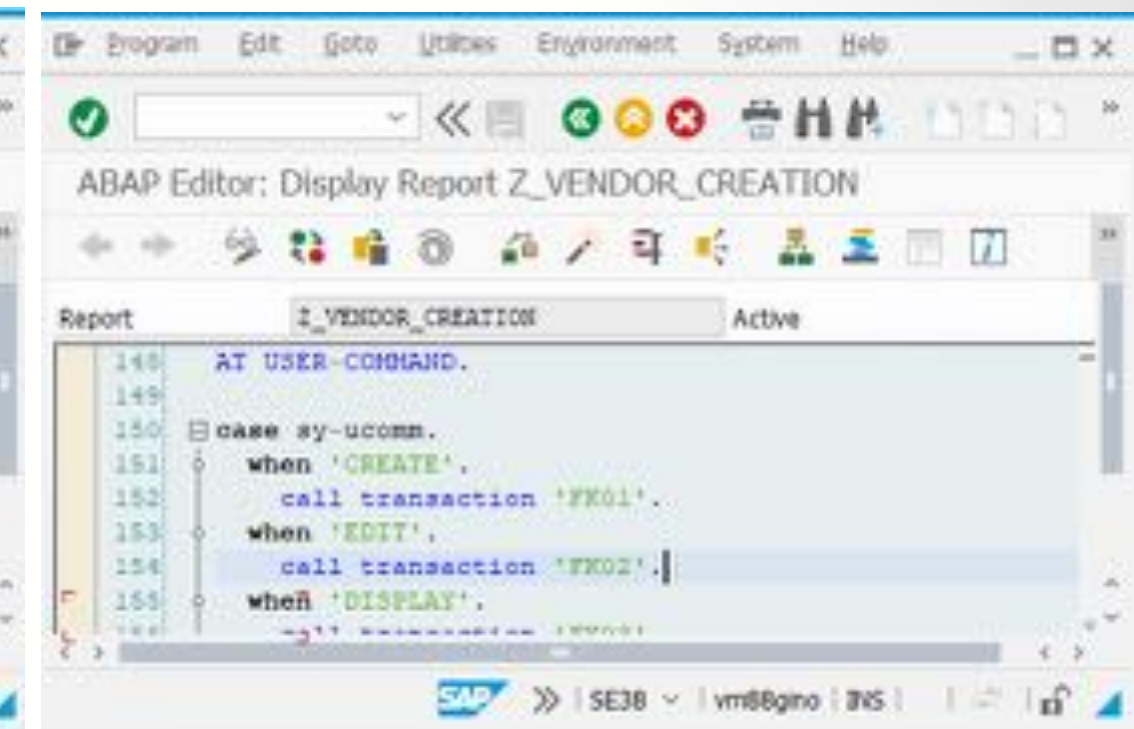
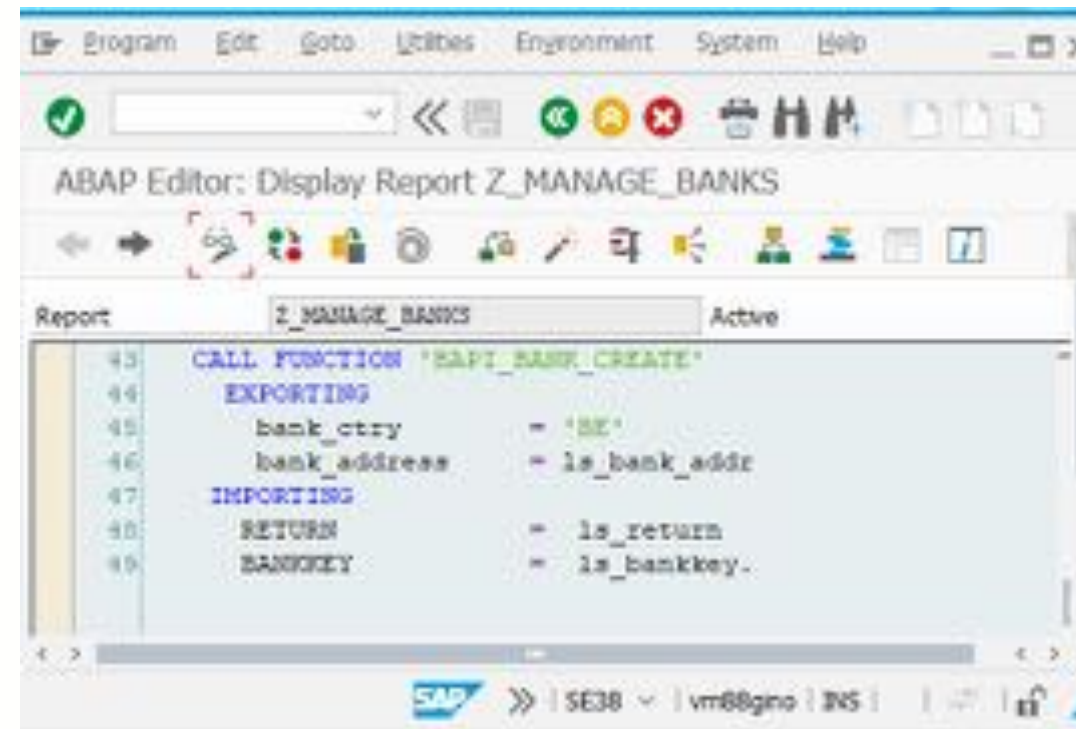
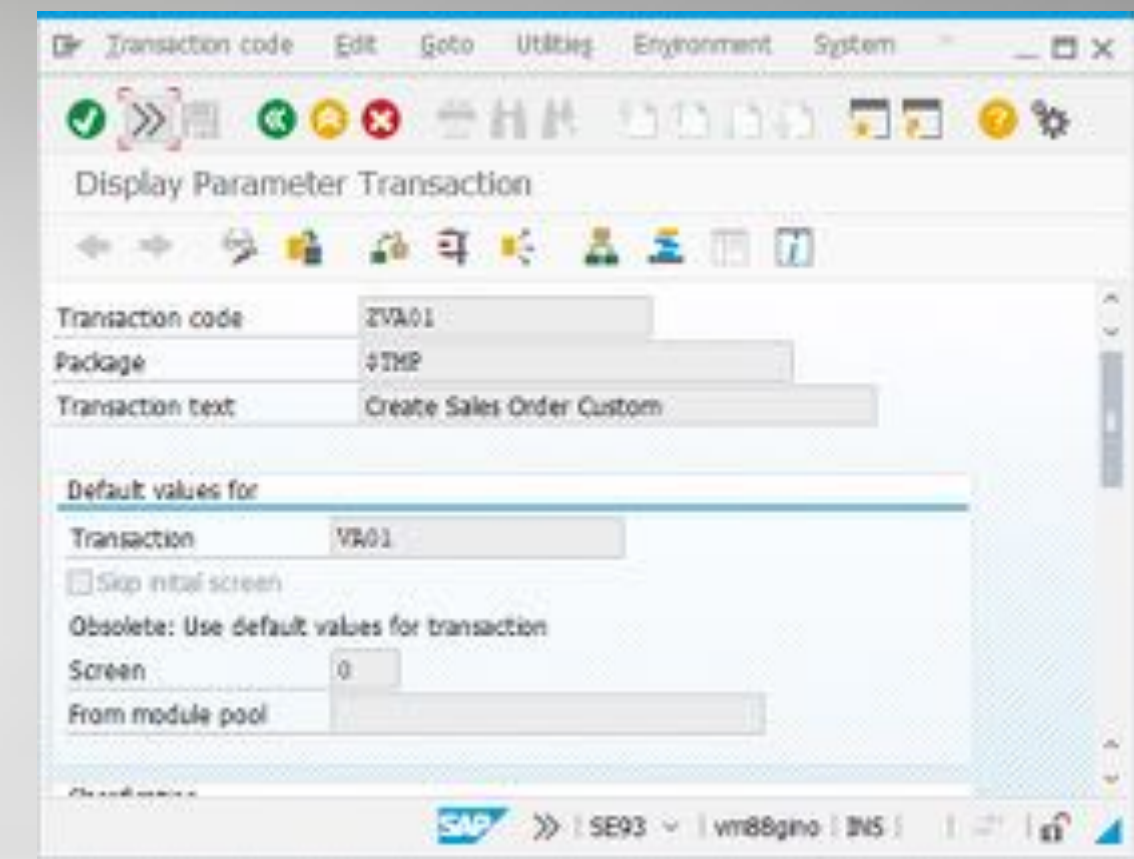
## V\_VBAK\_VKO – Sales Areas

- Activity
- Division
- Sales Organization
- Distribution Channel

System	Sales Document Type	Company Code	Division	Sales Organization	Distribution Channel
Production 1	OR – Standard Order Z1 – Returns	1000	01	0001	01
		2000	02	0002, 0003, 0004	02,03,04
Production 2	Z1 – Standard Order RE – Returns	1000	01	0001	01,02
Production 3	OR – Standard Order RE - Returns	2000	01	0001	02

# Custom Code

- Parameter Transactions
- ABAP Code
  - Call Transaction
  - Submit report
  - Include ...
  - BAPI-calls





# Why is an SOD Matrix hard to maintain?

- Organizational Complexity
  - Organizational values like Plants, Purchasing Organizations, Sales Organizations, Distribution Channels etc can have different meaning, or relationship on different systems.
  - Changes in Organizational Structure aren't always known by Compliance Department
- Complexity due to Customizing
  - Customizing such as document types, movement types can be different across systems.
  - New customizing values that are introduced aren't always known by Compliance Department
- Complexity due to Custom Code
  - Custom transactions can be developed giving access to SOD Relevant functionality

# How can it be simplified?

## Complexity due to Customizing

- Define rules that determine how values should be interpreted
- Reference these rules in the SOD Matrix
- Dynamically apply this configuration during the SOD analysis

# How can it be simplified?

## SOD Definition

## Rule Definition

System Help

Display Authorization Objects

Search

Function ID: Tcode: Object:

Hierarchy Header	Value From	Value
FM02 (Goods Receipt to PO)		
MB01 (Post Goods Receipt for PO)		
M_MSEG_BWA (Goods Movements: Movement Type)		
Value set 001		
ACTVT (Activity)	01	
BWART (Movement Type (Inventory Management))	/PSYNG/SBWART_B	
MB02 (Change Material Document)		
M_MSEG_BWA (Goods Movements: Movement Type)		
Value set 001		
ACTVT (Activity)	01	
BWART (Movement Type (Inventory Management))	/PSYNG/SBWART_B	
MB0A (Post Goods Receipt for PO)		
MB1C (Other Goods Receipts)		
MBST (Cancel Material Document)		
MIGO (Goods Movement)		
MIGO_GR (Goods Movement)		

System Help

SE: Maintain Variable Elements

Variable Elements Rule Version

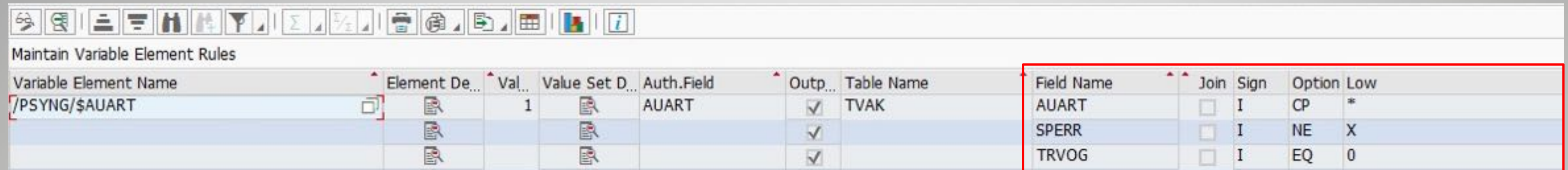
Rules Version: 1 Example Variable Elements

RFC Destination:

Maintain Variable Element Rules

Variable Element Name	Element De.	Val.	Value Set D.	Auth. Field	Outp.	Table Name	Field Name	Join	Sign	Option	Low
/PSYNG/SAUJART		1		AUJART	✓	TVAK	AUJART	<input type="checkbox"/>	I	CP	*
					✓		SPERR	<input type="checkbox"/>	I	NE	X
					✓		TRVOG	<input type="checkbox"/>	I	EQ	0
/PSYNG/SBWART_A				BWART	✓	T156	BWART	<input type="checkbox"/>	I	BT	200
/PSYNG/SBWART_B					✓			<input type="checkbox"/>	I	EQ	101
					✓			<input type="checkbox"/>	I	EQ	103
					✓			<input type="checkbox"/>	I	EQ	105
					✓			<input type="checkbox"/>	I	EQ	121
					✓			<input type="checkbox"/>	I	EQ	124
					✓			<input type="checkbox"/>	I	BT	201
/PSYNG/SKSCHL_PUR		2		KSCHL	✓	T605	KAPPL	<input type="checkbox"/>	I	CP	M*
					✓		KSCHL	<input type="checkbox"/>	I	CP	C*

# How can it be simplified?



The screenshot shows the SAP 'Maintain Variable Element Rules' interface. It features a toolbar with various icons at the top. Below the toolbar is a table with columns: Variable Element Name, Element De..., Val..., Value Set D..., Auth.Field, Outp..., Table Name, Field Name, Join, Sign, Option, and Low. The first row is highlighted with a red box and contains the following data: Variable Element Name: /PSYNG/\$AUART; Element De...: (icon); Val...: 1; Value Set D...: (icon); Auth.Field: AUART; Outp...: (checked); Table Name: TVAK. The second table, also highlighted with a red box, lists field names and their corresponding Join, Sign, Option, and Low values.

Variable Element Name	Element De...	Val...	Value Set D...	Auth.Field	Outp...	Table Name	Field Name	Join	Sign	Option	Low
/PSYNG/\$AUART	(icon)	1	(icon)	AUART	(checked)	TVAK	AUART	<input type="checkbox"/>	I	CP	*
	(icon)		(icon)		(checked)		SPERR	<input type="checkbox"/>	I	NE	X
	(icon)		(icon)		(checked)		TRVOG	<input type="checkbox"/>	I	EQ	0

Include all the Sales Document Types (AUART)

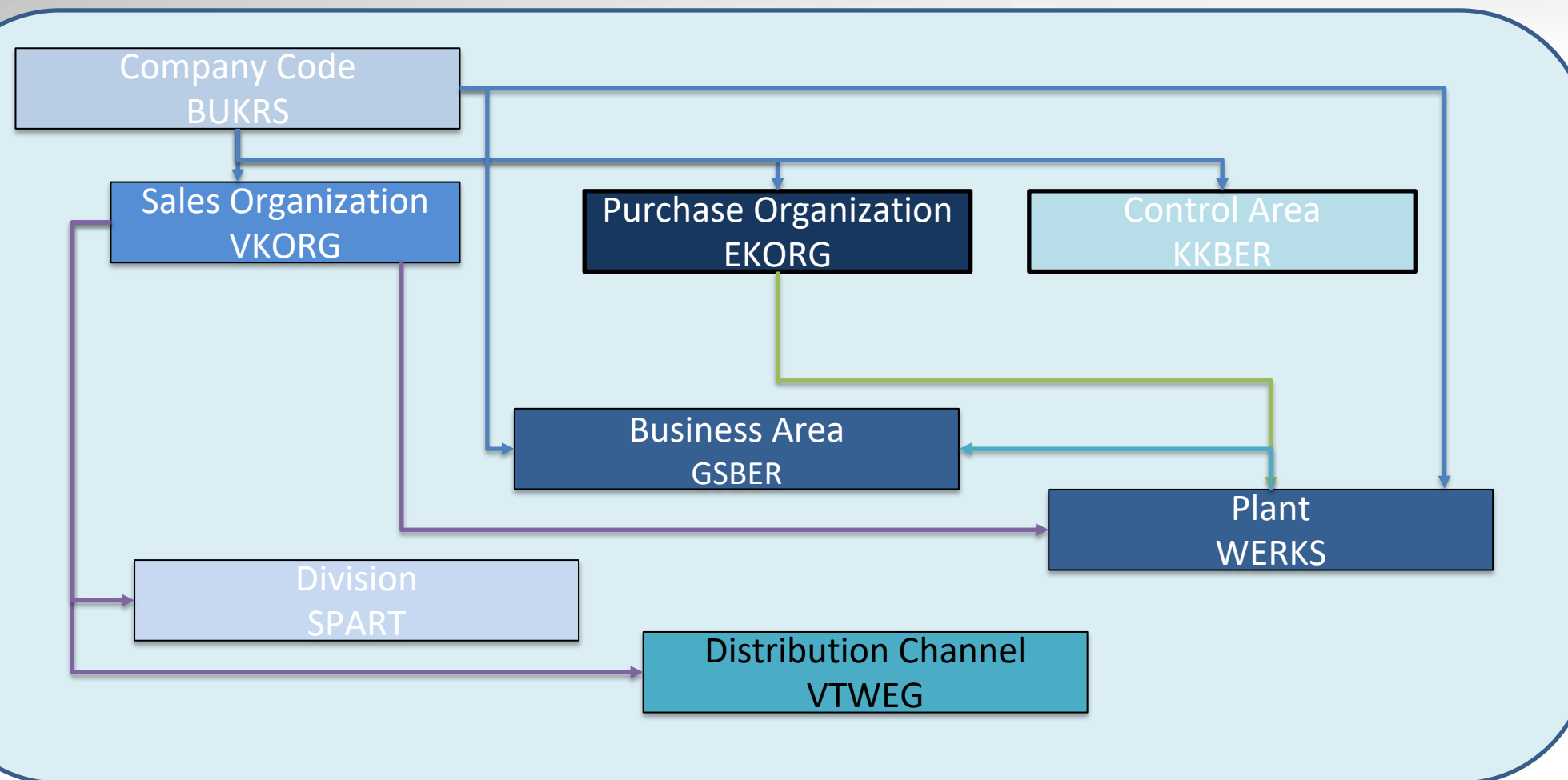
That are not locked (SPERR <> X)

And have the Transaction Group: Sales Order (TRVOG = 0)

# How can it be simplified?

## Organizational Complexity

- Automate the discovery of the Organizational Setup across the entire landscape
- Dynamically apply this configuration during the SOD analysis



# How can it be simplified?

## Organizational Complexity

### 1. System Scope

System Web

Separations Enforcer - Configuration Set Maintenance

Display/Change Delete Upload/Download Copy

Configuration Set

Config Set ID: 5 Creation: DHORJONS 13.04.2021 04:04:01 Changed: DHORJONS 13.04.2021 04:41:50

Published

Description: Security Weaver - Example Configuration Set

System Selection Element Selection Organizational Elements Variable Elements

Selected	System ID	RFC Destination
<input checked="" type="checkbox"/>	D67800	D67_800_DAK
<input checked="" type="checkbox"/>	X048800	

# How can it be simplified?

## Organizational Complexity

### 2. Org Element Scope

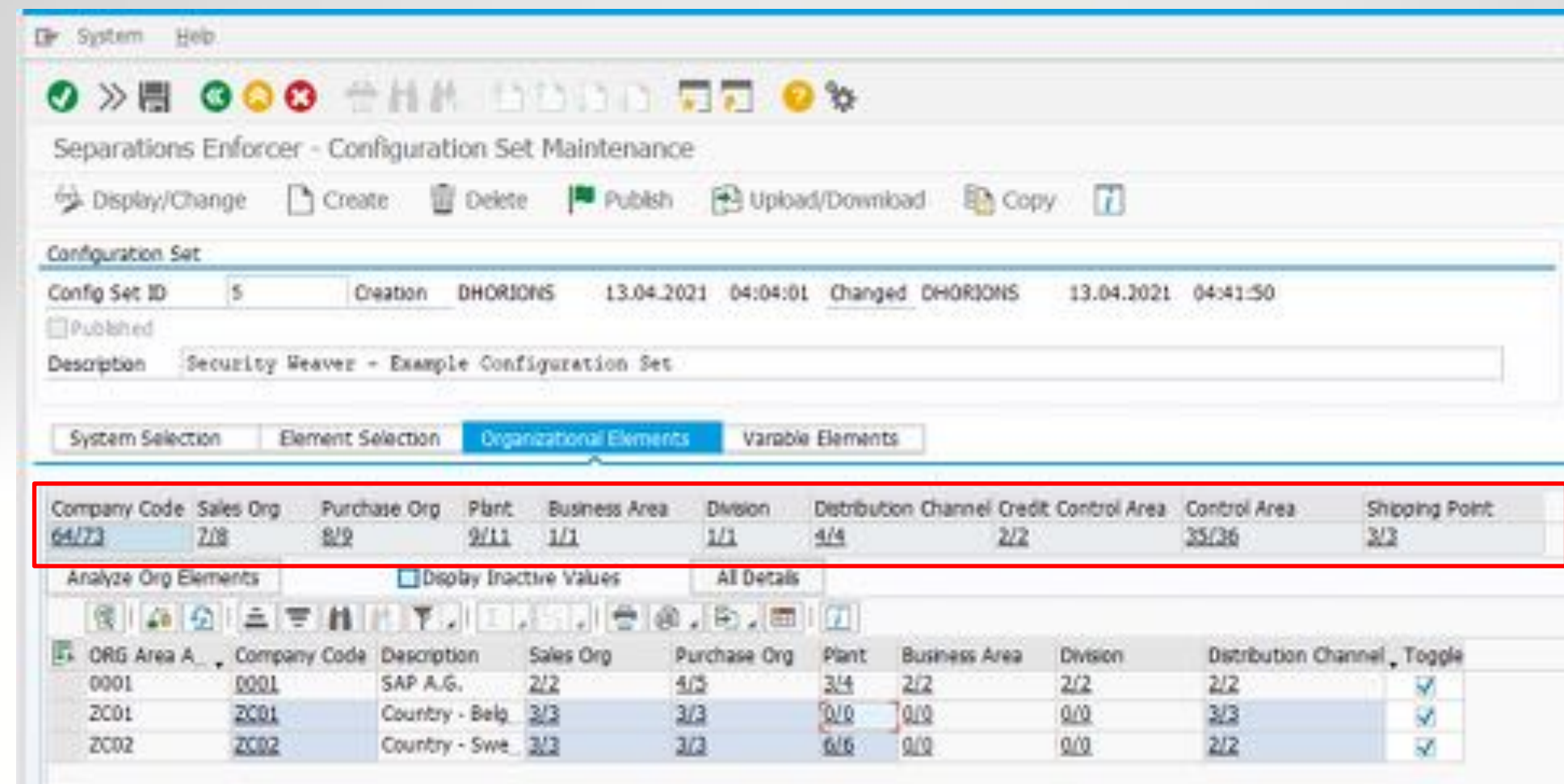
The screenshot displays the SAP Separations Enforcer - Configuration Set Maintenance interface. The configuration set is identified as 'Security Weaver - Example Configuration Set'. The 'Element Selection' tab is active, showing a table of organizational elements. A red box highlights the first six rows of the table, which are selected. The table includes columns for 'Selected', 'Default', 'Organizational Element', and 'Description'.

Selected	Default	Organizational Element	Description
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	BUKRS	Company Code
<input checked="" type="checkbox"/>	<input type="checkbox"/>	EKORG	Purchasing organization
<input checked="" type="checkbox"/>	<input type="checkbox"/>	WERKS	Plant
<input checked="" type="checkbox"/>	<input type="checkbox"/>	WVERK	Maintenance Planning Plant
<input checked="" type="checkbox"/>	<input type="checkbox"/>	GSBER	Business Area
<input checked="" type="checkbox"/>	<input type="checkbox"/>	SPART	Division
<input checked="" type="checkbox"/>	<input type="checkbox"/>	VTWEG	Distribution Channel
<input type="checkbox"/>	<input type="checkbox"/>	KKBER	Credit control area
<input type="checkbox"/>	<input type="checkbox"/>	KOKRS	Controlling Area
<input type="checkbox"/>	<input type="checkbox"/>	VKORG	Sales Organization
<input type="checkbox"/>	<input type="checkbox"/>	VSTEL	Shipping Point/Receiving Point

# How can it be simplified?

## Organizational Complexity

### 3. Discovery



The screenshot displays the SAP Separations Enforcer - Configuration Set Maintenance interface. The configuration set is identified as 'Security Weaver - Example Configuration Set' with ID 5. The 'Organizational Elements' tab is active, showing a table of organizational elements. A red box highlights the first row of this table, which contains the following data:

Company Code	Sales Org	Purchase Org	Plant	Business Area	Division	Distribution Channel	Credit Control Area	Control Area	Shipping Point
6473	2/8	8/9	9/11	1/1	1/1	4/4	2/2	25/36	3/3

Below this table, there is a section for 'Analyze Org Elements' with a 'Display Inactive Values' checkbox. A second table is visible, showing details for 'ORG Area A...' with columns for Company Code, Description, Sales Org, Purchase Org, Plant, Business Area, Division, Distribution Channel, and Toggle.

Company Code	Description	Sales Org	Purchase Org	Plant	Business Area	Division	Distribution Channel	Toggle
0001	SAP A.G.	2/2	4/5	3/4	2/2	2/2	2/2	✓
2001	Country - Belg	3/3	3/3	0/0	0/0	0/0	3/3	✓
2002	Country - Swe	3/3	3/3	0/0	0/0	0/0	2/2	✓



# Organizational Complexity

System Help

Separations Enforcer - Configuration Set Maintenance

Display/Change Create Delete Publish Upload/Download Copy

Configuration Set

Config Set ID: 5 Creation: DHORJONS 13.04.2021 04:04:01 Changed: DHORJONS 13.04.2021 04:41:50

Published

Description: Security Weaver - Example Configuration Set

System Selection Element Selection **Organizational Elements** Variable Elements

Company Code	Sales Org	Purchase Org	Plant	Business Area	Division	Distribution Channel	Credit Control Area	Control Area	Shipping Point
6473	Z/B	8/9	9/11	1/1	1/1	4/4	2/2	35/36	3/3

Analyze Org Elements  Display Inactive Values All Details

ORG Area A	Company Code	Description	Sales Org	Purchase Org	Plant	Business Area	Division	Distribution Channel	Toggle
0001	0001	SAP A.G.	2/2	4/5	3/4	2/2	2/2	2/2	<input checked="" type="checkbox"/>
Z001	Z001	Country - Belgium	3/3	3/3	0/0	0/0	0/0	3/3	<input checked="" type="checkbox"/>
Z002	Z002	Country - Sweden	3/3	3/3	6/6	0/0	0/0	2/2	<input checked="" type="checkbox"/>

System Help

Separations Enforcer - Organizational Elements Values

Toggle for all Company Codes

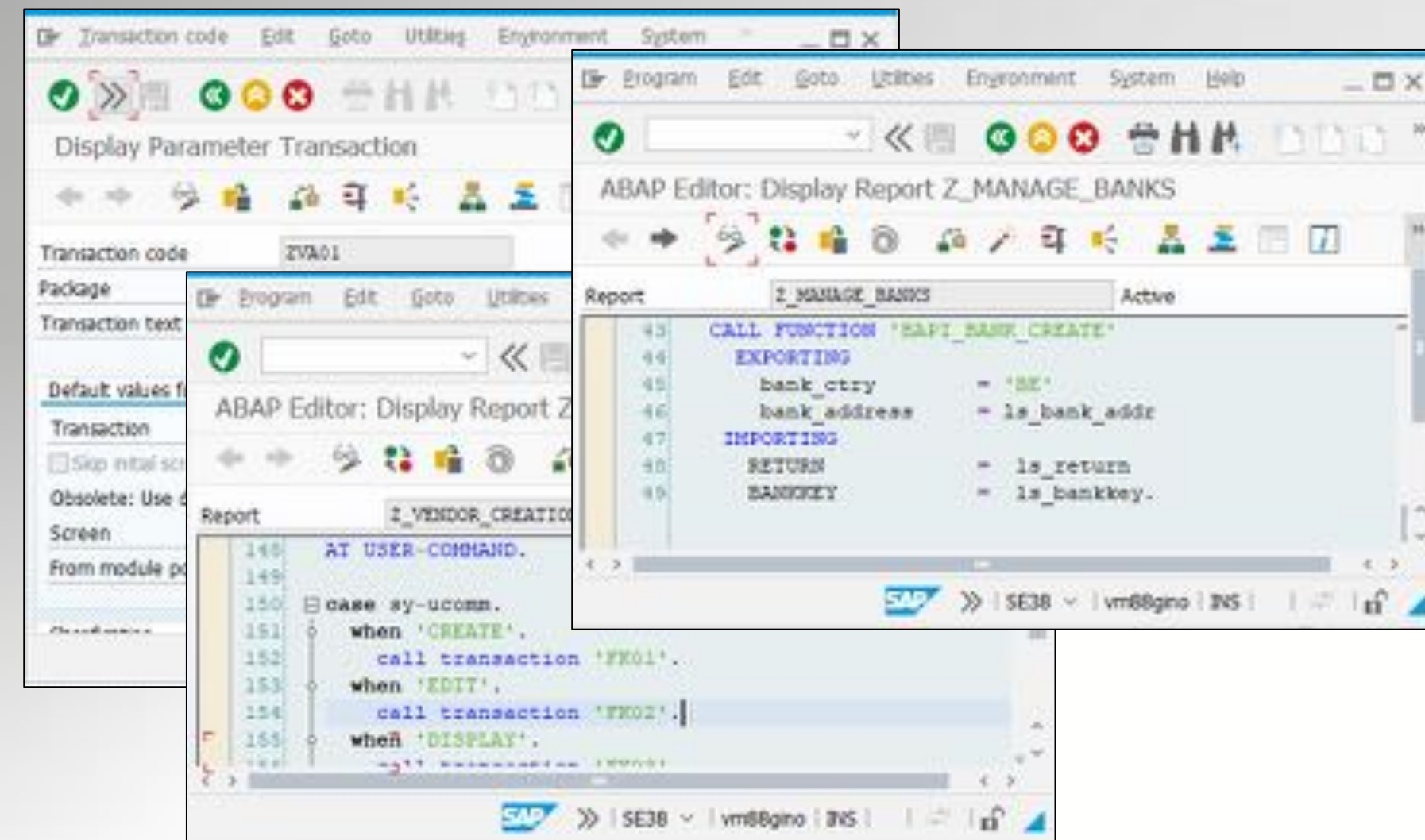
Display Inactive Values

Org. Area Abb.	Description	Field	Field Name	System	Value	Value Description	Toggle
Z002	Country - Sweden	BUKRS	Company Code	XH8800	Z002	Country - Sweden	<input checked="" type="checkbox"/>
Z002	Country - Sweden	EKORG	Purchasing Organization	XH8800	ZES1	SE - Svealand Purch	<input checked="" type="checkbox"/>
Z002	Country - Sweden	EKORG	Purchasing Organization	XH8800	ZES2	SE - Norrland Purch	<input checked="" type="checkbox"/>
Z002	Country - Sweden	EKORG	Purchasing Organization	XH8800	ZES3	SE - Götaland Purch	<input checked="" type="checkbox"/>
Z002	Country - Sweden	VKORG	Sales Organization	XH8800	ZSS1	SE - Götaland	<input checked="" type="checkbox"/>
Z002	Country - Sweden	VKORG	Sales Organization	XH8800	ZSS2	SE - Svealand	<input checked="" type="checkbox"/>
Z002	Country - Sweden	VKORG	Sales Organization	XH8800	ZSS3	SE - Norrland	<input checked="" type="checkbox"/>
Z002	Country - Sweden	VTWEG	Distribution Channel	XH8800	Z1	Z1	<input checked="" type="checkbox"/>
Z002	Country - Sweden	VTWEG	Distribution Channel	XH8800	Z3	Z3	<input checked="" type="checkbox"/>
Z002	Country - Sweden	WERKS	Plant	XH8800	ZP51	SE - Jönköping Plant	<input checked="" type="checkbox"/>
Z002	Country - Sweden	WERKS	Plant	XH8800	ZP52	SE - Stockholm Plan	<input checked="" type="checkbox"/>
Z002	Country - Sweden	WERKS	Plant	XH8800	ZP53	SE - Malmö Plant	<input checked="" type="checkbox"/>

# How can it be simplified?

Complexity due to Custom Code

- Analyse all custom Transactions.
- Link them to transactions in the SOD Matrix.
- Dynamically do this during SOD analysis.



# How can it be simplified?

Complexity due to Custom Code

SW : Dynamically Enhanced SOD Matrix details

Sensitivity	Can ID	Func.	Calling Code	TCode	Object	Flag	ValueSet	Field Name	value	Value	Str	Risk Description	Enhanc
CRITICAL	F029	FF08	ZJNE011	FB01	F_BKPF_BUK		1	ACTVT	01	02		Maintain Posting Period & Post Journal Entry	✓
					F_BKPF_XDA			KDART	S				✓
	F031	FF04			F_BKPF_BUK			ACTVT	01	02		Maintain Posting Period & AR Cash Application	✓
					F_BKPF_XDA			KDART	D				✓
	5003	FS03	Z_VA01	VA01	V_VBAK_AAT			ACTVT	01	02		Goods Issues & Delivery Processing & VM Clear/Adjust & IM Inve...	✓
					V_VBAK_VKO				05	06			✓
					V_VBAK_VKO				01	02			✓
					V_VBAK_VKO				05	06			✓
			Z_VA02	VA02	V_VBAK_AAT				01	02			✓
					V_VBAK_VKO				03	06			✓
					V_VBAK_VKO				01	02			✓
					V_VBAK_VKO				03	06			✓
			Z_VA01	VA01	V_VBAK_AAT				01	02			✓
					V_VBAK_VKO				05	06			✓
					V_VBAK_VKO				01	02			✓
					V_VBAK_VKO				03	06			✓
WSDW	F003	FF03	ZJNE011	FB01	F_BKPF_BUK				01	02		AR Cash Application (Payments) & AP Payments Processing	✓

# How can it be simplified?

Complexity due to Custom Code

SW : Dynamically Enhanced SOD Matrix details

Add to Function

Sensitivity	Can ID	Func.	Calling Code	TCode	Object	Flag	ValueSet	Field Name	value	Value	Svr Risk Description	Enhanc
CRITICAL	F029	FF08	ZJNE011	FB01	F_BKPF_BUK		1	ACTVT	01	02	Maintain Posting Period & Post Journal Entry	✓
					F_BKPF_XDA			KDART	S			✓
	F031	FF04			F_BKPF_BUK			ACTVT	01	02	Maintain Posting Period & AR Cash Application	✓
					F_BKPF_XDA			KDART	D			✓
	5003	FS03	Z_VA01	VA01	V_VBAK_AAT			ACTVT	01	02	Goods Issues & Delivery Processing & VM Clear/Adjust & IM Inve...	✓
					V_VBAK_VKO				05	06		✓
					V_VBAK_VKO				01	02		✓
					V_VBAK_VKO				05	06		✓
			Z_VA02	VA02	V_VBAK_AAT				01	02		✓
					V_VBAK_VKO				03	06		✓
					V_VBAK_VKO				01	02		✓
					V_VBAK_VKO				03	06		✓
			Z_VA01	VA01	V_VBAK_AAT				01	02		✓
					V_VBAK_VKO				05	06		✓
					V_VBAK_VKO				01	02		✓
					V_VBAK_VKO				03	06		✓
WSDW	F002	FF03	ZJNE011	FB01	F_BKPF_BUK				01	02	AR Cash Application (Payments) & AP Payments Processing	✓

# SUMMARY AND Q&A

- Automatic Discovery of Organizational Configuration, Customizing and custom code in the landscape increases accuracy of the Segregation of Duties Analysis results.
- Dynamically applying this discovered information to the SOD matrix during the analysis saves time, effort and avoids human error.
- Security Weaver's solution for this is called "Dynamic Matrix" and is part of Separations Enforcer. ( version 4.1 or higher)

# Related webinars

**Please watch these existing Security Weaver User Group (SWUG) webinars**

- 4 Key Reports for Managing SOD Risk
- How to Align Stakeholders with Dashboards

<https://www.linkedin.com/groups/4642758/>



# Contact Us



## Mailing Address

Strawinskylaan 3051 – 1077 ZX Amsterdam – The Netherlands

## Email Address

[simone@securityweaver.com](mailto:simone@securityweaver.com)

## Phone number

+31 20 301 21 45

