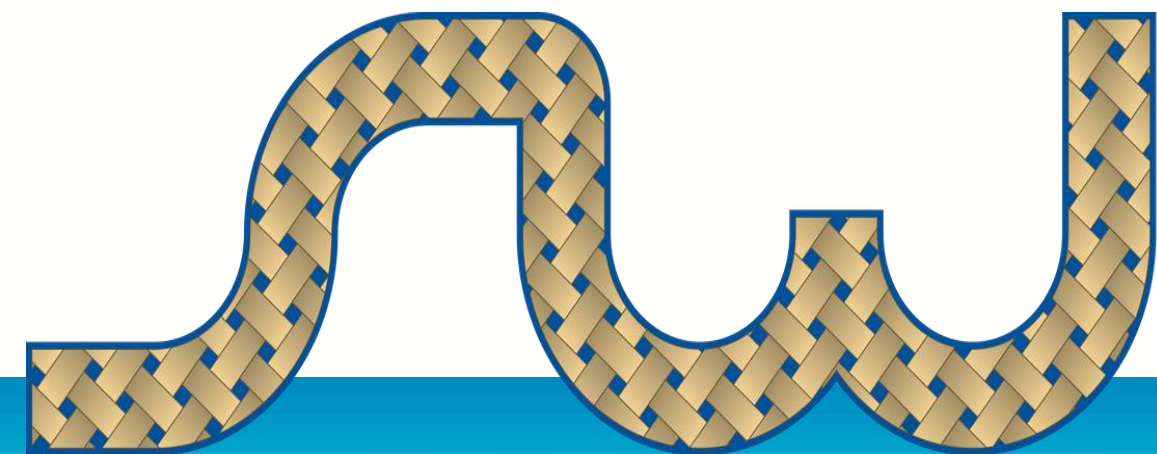




APRIL 26<sup>TH</sup>, 2022

# 5 Ways to Mitigate Risks of Sensitive Access and SOD Conflicts

*Presented by Diane Reinsma  
Senior Product Manager at Security Weaver*



SECURITY WEAVER



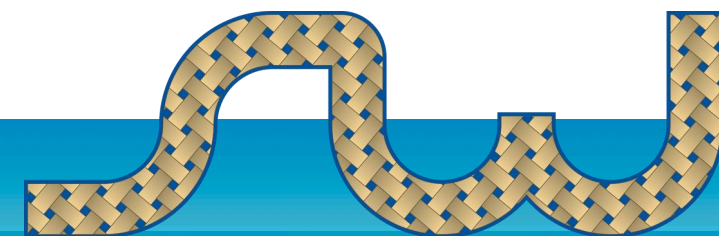
START

---



# Agenda

- Introduction
- Key Areas of Risk
- Ways to Mitigate Risks
- Solutions to Mitigate Risks
- Summary
- Q&A



SECURITY WEAVER

# Introduction

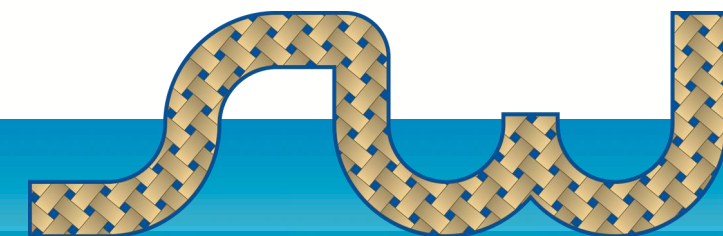
Name: Diane Reinsma

Role: Senior Product Manager

Email: [dreinsma@securityweaver.com](mailto:dreinsma@securityweaver.com)



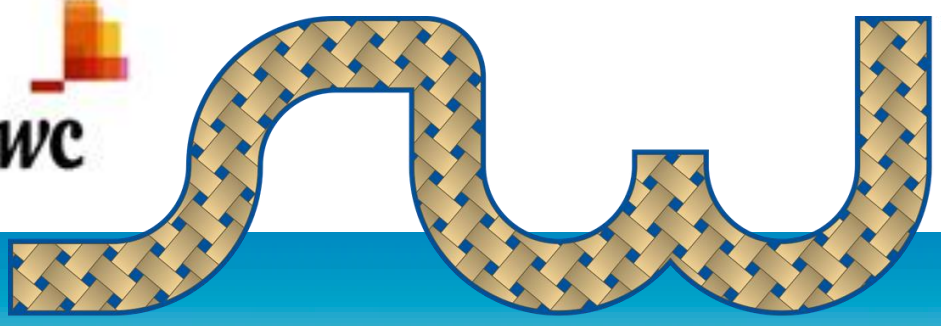
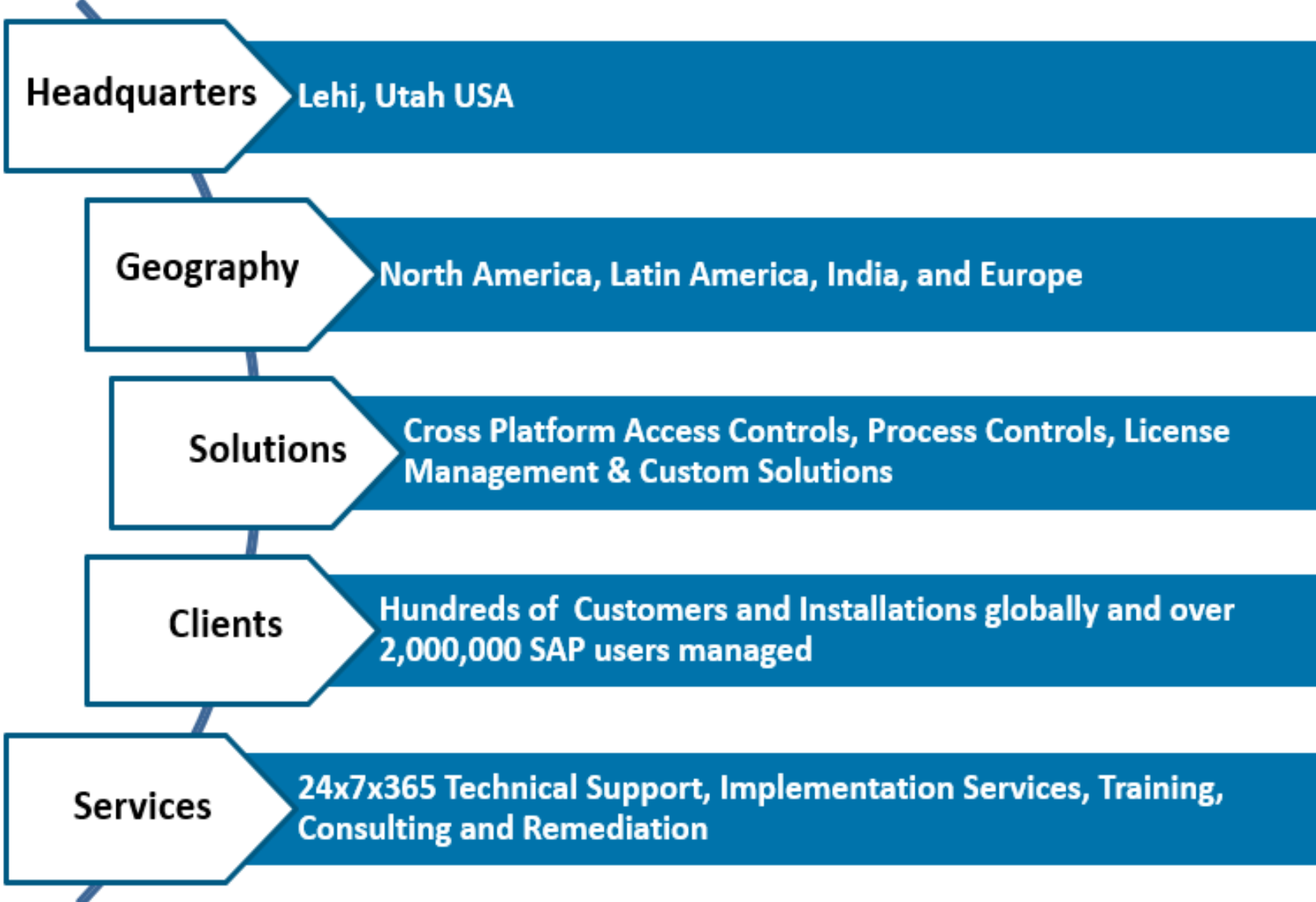
- Been with Security Weaver since 2008.
- Began working with SAP in 1997 as a Functional Analyst/Configurator in variety of modules: FI/CO, MM, WM/IM, PS and Security.





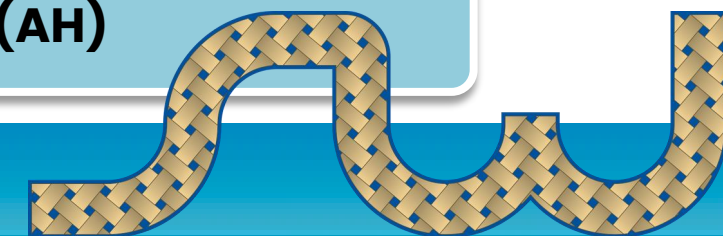
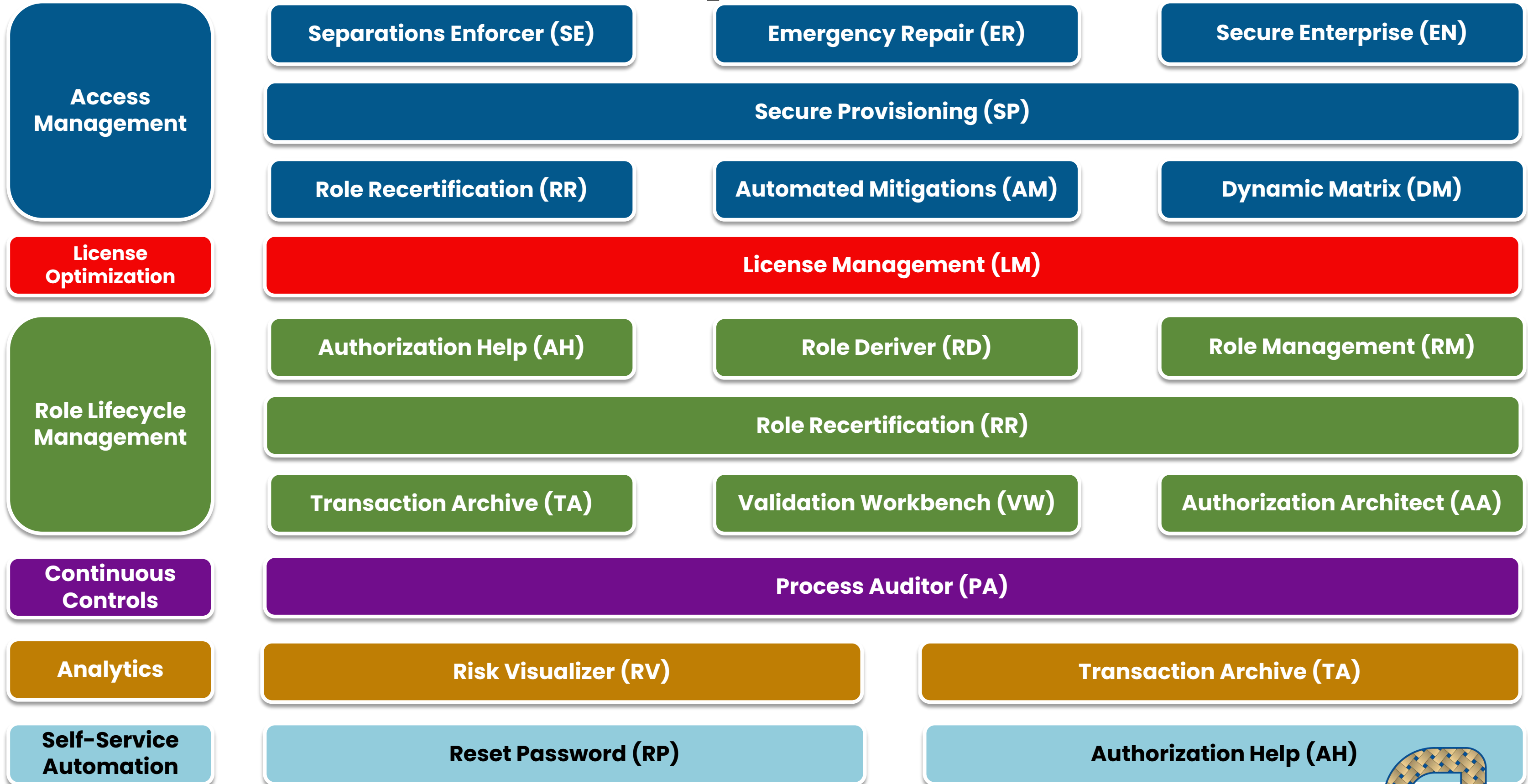
# Security Weaver

Security Weaver partners with enterprises to rapidly deliver integrated and efficient controls. A best of breed solution set supporting any SAP environment for monitoring, controlling, and reporting on enterprise risks.





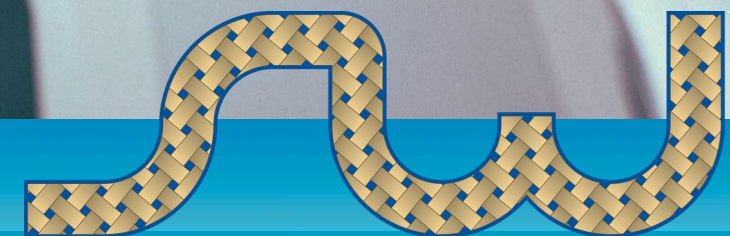
# Introduction - Security Weaver Modules





# Key Areas of Risk

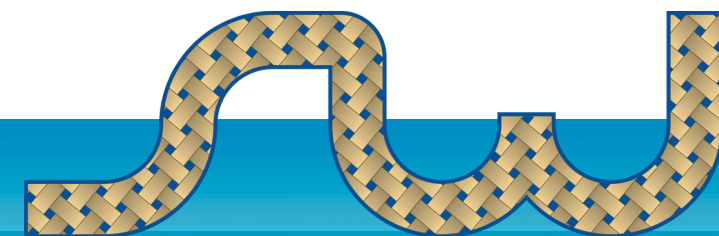
- SAP Access allowing:
  - Conflicting Function Access
  - Sensitive Access
    - System Profile Parameter Changes
    - System Configuration





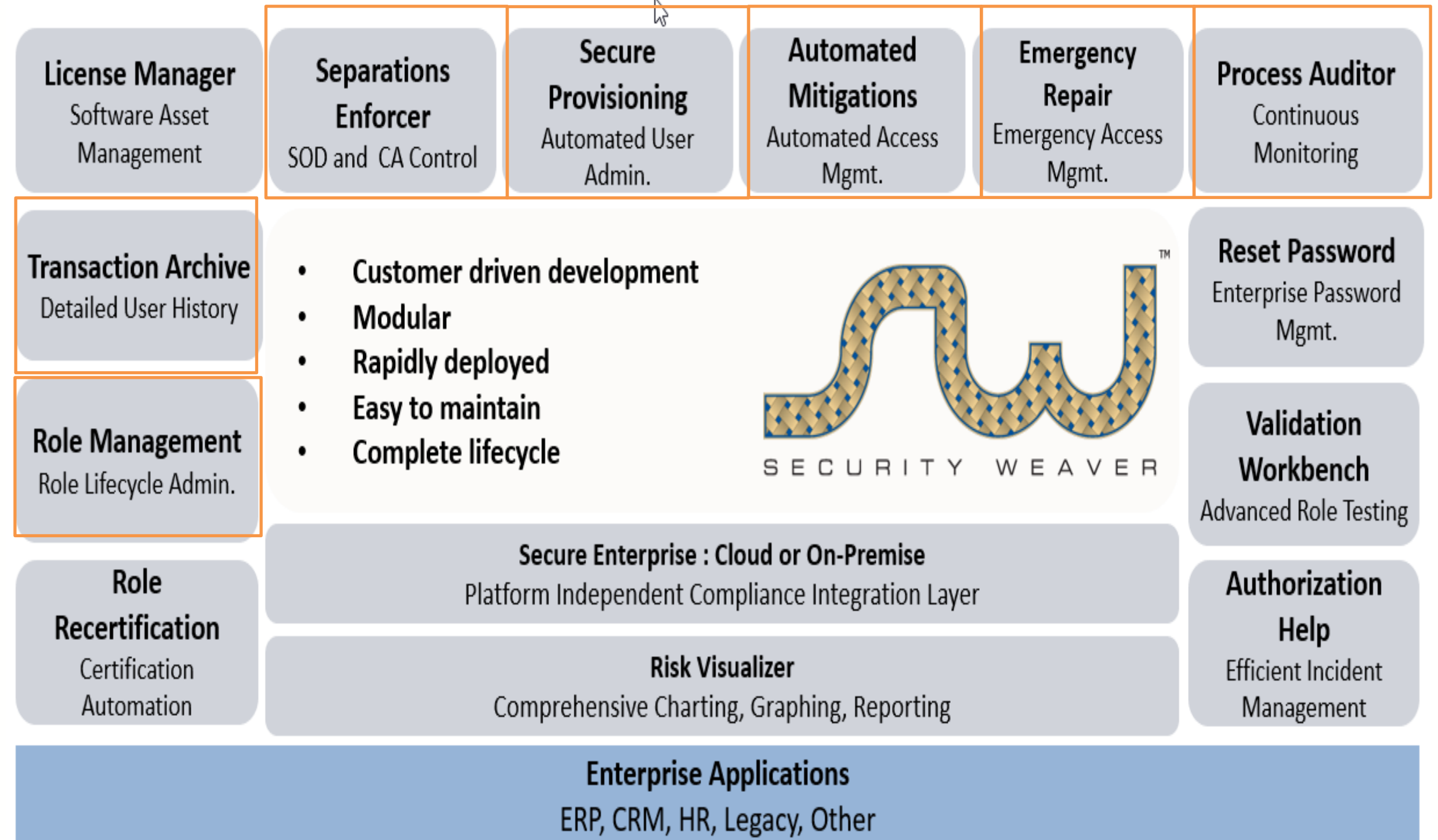
# Ways to Mitigate Risks

1. Identify Risks to the Organization
2. Implement System Checks/Enforcement
3. Approval/Review Processes in Place
4. Utilize Temporary Access
5. Activate Automation of Risk Detection



# Security Weaver Solutions to Mitigate Risks

- SE – Separations Enforcer
- SP – Secure Provisioning
- ER – Emergency Repair
- TA – Transaction Archive
- AM – Automated Mitigations
- PA – Process Auditor
- RM – Role Management
- AA – Authorization Architect





# Define Risks

## SOD Matrix Rules

What is sensitive to your organization?

What are the levels of severity of the risks?

- Conflicting Functions
- Critical T-codes, Auth, Roles, Profiles

## Dynamic Matrix

Intelligent SOD Rules across your Environments

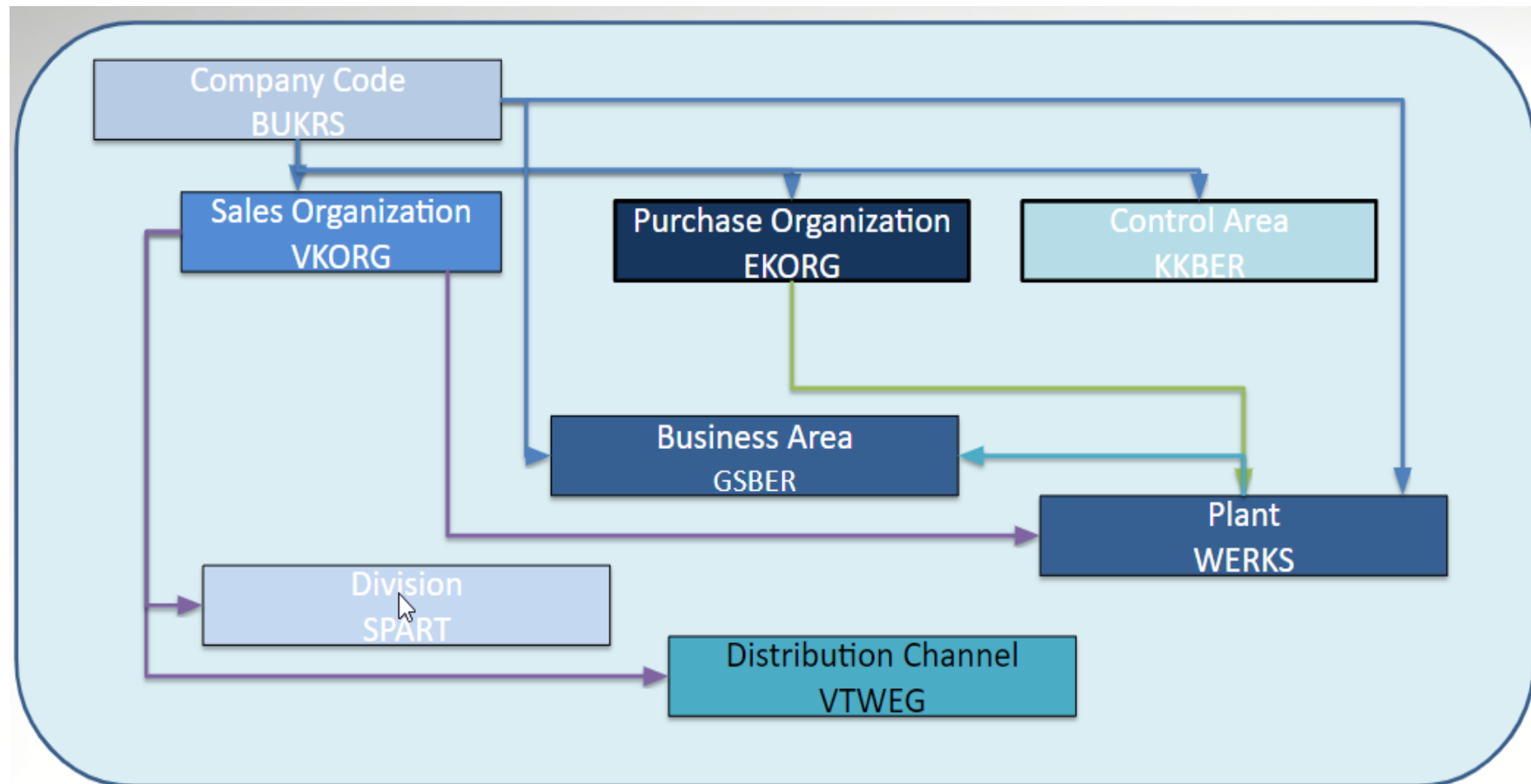
- ✓ **Dynamic Enhancement Logic**
  - Evaluate Custom Code/Transactions
- ✓ **Configuration Sets**
  - Fine-Tune your SOD Matrix Rules
    - System Scope
    - Organizational Scope
    - Configuration Scope
- ❖ *Separations Enforcer (SE)*



# Dynamic Matrix – Configuration Sets

Selection of Org Levels to consider & Automatic Determination of Organization Values in your Systems

- Company, Purch Org, Sales Org, Plant, etc.



System Help

Separations Enforcer - Configuration Set Maintenance

Display/Change Create Delete Publish Upload/Download Copy

Configuration Set

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

Published

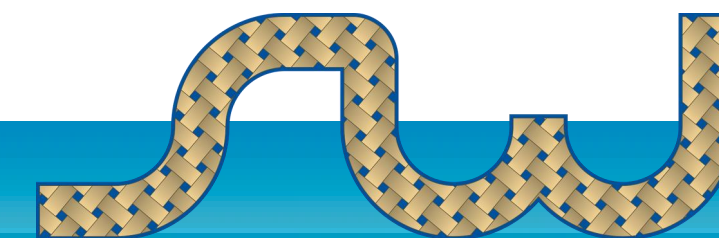
Description: Security Weaver - Example Configuration Set

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
64/73	7/8	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"/>
ZC01	ZC01	Country - Belg...	3/3	3/3	0/0	0/0	0/0	3/3	<input checked="" type="checkbox"/>
ZC02	ZC02	Country - Swe...	3/3	3/3	6/6	0/0	0/0	2/2	<input checked="" type="checkbox"/>





# Dynamic Matrix – Variable Elements

Easy defining of Customizing fields – i.e. Movement Types, Condition Types

## SOD Definition

System Help

Display Authorization Objects

Search

Function ID Tcode Object

Hierarchy Header

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	
BWAART (Movement Type (Inventory Management))	/PSYNG/\$BWAART_B	
MB02 (Change Material Document)		
M_MSEG_BWA (Goods Movements: Movement Type)		
Value set 001		
ACTVT (Activity)	01	
BWAART (Movement Type (Inventory Management))	/PSYNG/\$BWAART_B	
MB0A (Post Goods Receipt for PO)		
MB1C (Other Goods Receipts)		
MBST (Cancel Material Document)		
MIGO (Goods Movement)		
MIGO_GR (Goods Movement)		

## Rule Definition

System Help

SE : Maintain Variable Elements

Refresh Create Version Delete Version Copy Version Download/Upload

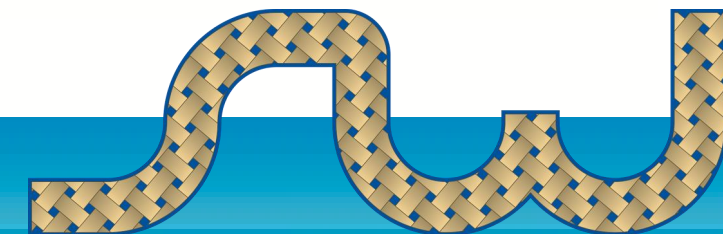
Variable Elements Rule Version

Rules Version 3 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/\$AUART		1		AUART	<input checked="" type="checkbox"/>	TVAK	AUART	<input type="checkbox"/>	I	CP	*
					<input checked="" type="checkbox"/>		SPERR	<input type="checkbox"/>	I	NE	X
					<input checked="" type="checkbox"/>		TRVOG	<input type="checkbox"/>	I	EQ	0
/PSYNG/\$BWAART_A				BWAART	<input checked="" type="checkbox"/>	T156	BWAART	<input type="checkbox"/>	I	BT	200
/PSYNG/\$BWAART_B					<input checked="" type="checkbox"/>			<input type="checkbox"/>	I	EQ	101
					<input checked="" type="checkbox"/>			<input type="checkbox"/>	I	EQ	103
					<input checked="" type="checkbox"/>			<input type="checkbox"/>	I	EQ	105
					<input checked="" type="checkbox"/>			<input type="checkbox"/>	I	EQ	121
					<input checked="" type="checkbox"/>			<input type="checkbox"/>	I	EQ	124
					<input checked="" type="checkbox"/>			<input type="checkbox"/>	I	EQ	161
					<input checked="" type="checkbox"/>			<input type="checkbox"/>	I	BT	Z01
/PSYNG/\$KSCHL_PUR		2		KSCHL	<input checked="" type="checkbox"/>	T685	KAPPL	<input type="checkbox"/>	I	CP	M*
					<input checked="" type="checkbox"/>		KSCHL	<input type="checkbox"/>	I	CP	C*

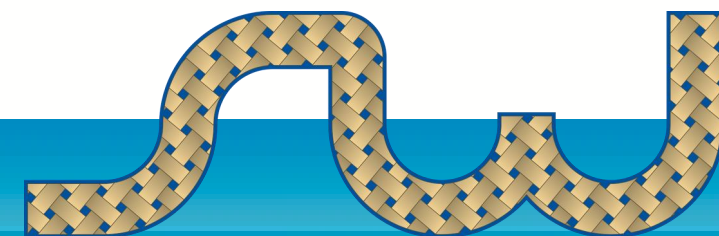


# Define Continuous Monitoring Risks

Define risks in your business processes and continuously monitoring all types of areas for risky activity.

## ❖ *Process Auditor (PA)*

- Security Weaver's Process Auditor is a continuous control monitoring solution that provides enterprises with a complete controls framework for identifying, misuse, and errors in transactional processes
- Security Weaver has out-of-the-box controls - [over 130](#) pre-built controls that cover Configuration, Master Data, and Transaction controls to monitor risky activity in the system





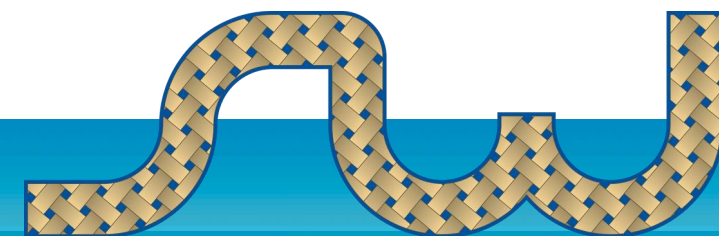
# System Checks/Enforcement

Integration to check the defined SOD Conflicts in User & Role Creation

SAP Standard Transactions – Exit Points

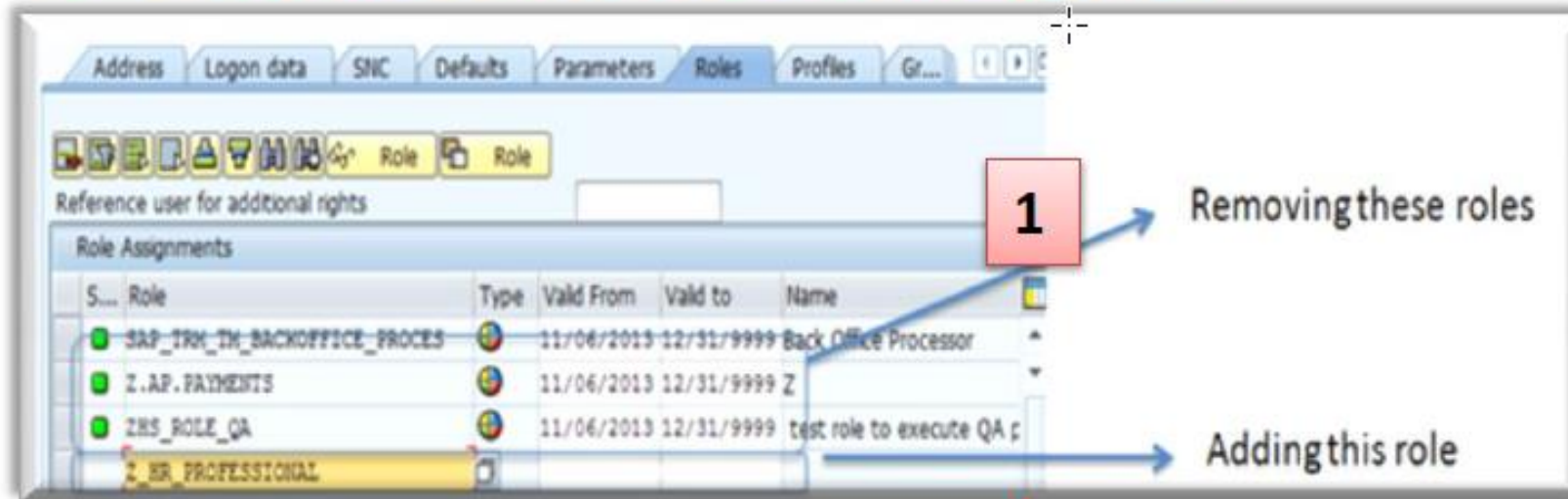
- SU01 – User Master Maintenance
- PFCG – Role Maintenance
- SE10 – Transport of Roles

- ❖ *Separations Enforcer (SE)*
- ❖ *Role Management (RM)*
- ❖ *Authorization Architect (AA)*
- ❖ *Secure Provisioning (SP)*



# User Changes in SU01

## SE Integration with User Management



Reference user for additional rights

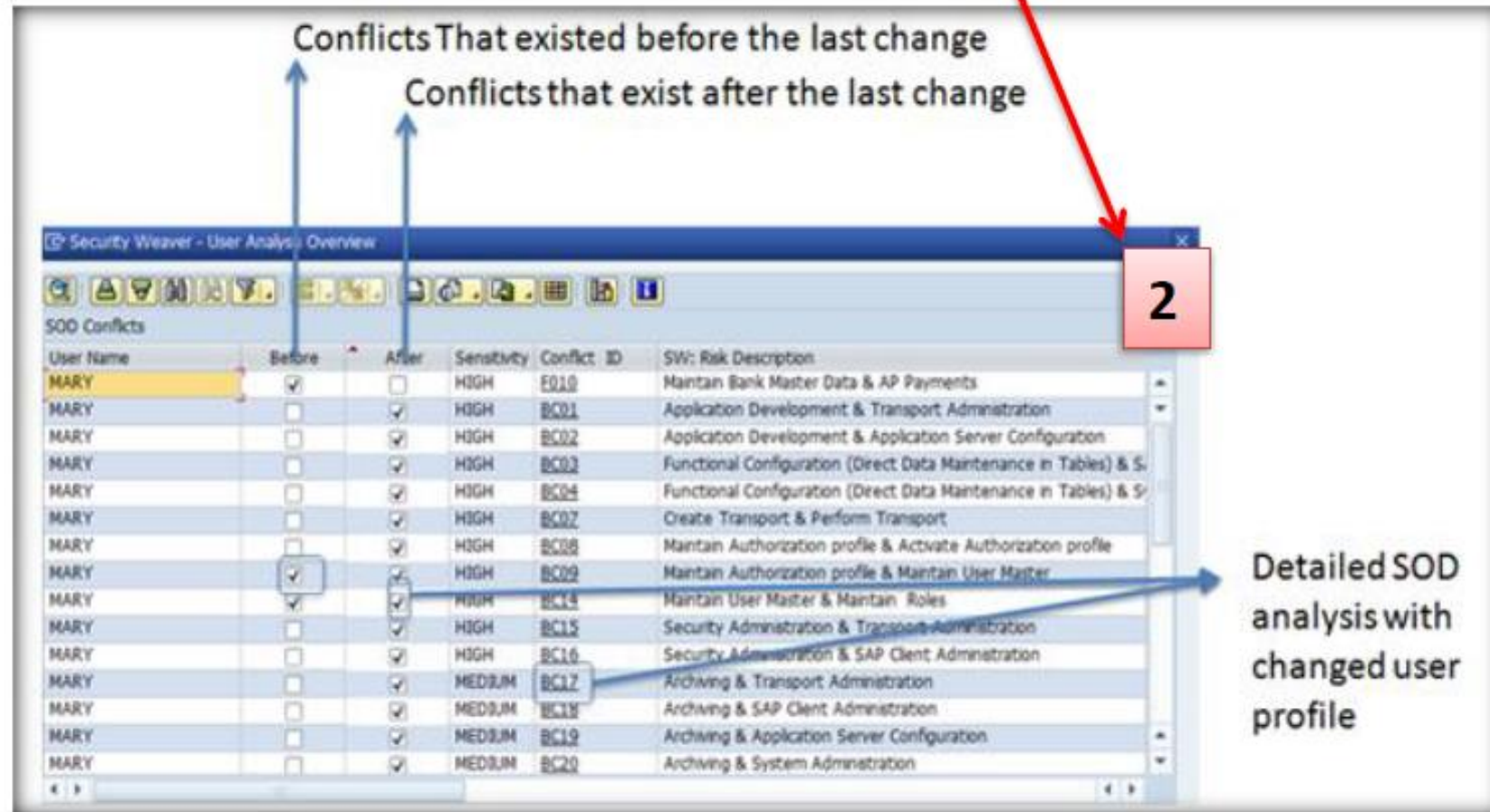
S...	Role	Type	Valid From	Valid to	Name
	SAP_TRM_TM_BACKOFFICE_PROCES		11/06/2013	12/31/9999	Back Office Processor
	Z.AP.PAYMENTS		11/06/2013	12/31/9999	Z
	ZRS_ROLE_QA		11/06/2013	12/31/9999	test role to execute QA c
	Z_IR_PROFESSIONAL				

1 Removing these roles

Adding this role

### 1. SU01 – Change a User

- Adding roles
- Removing roles



Conflicts That existed before the last change

Conflicts that exist after the last change

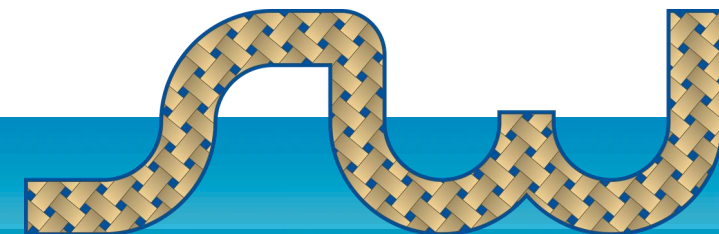
User Name	Before	After	Sensitivity	Conflict ID	SW: Risk Description
MARY	<input checked="" type="checkbox"/>	<input type="checkbox"/>	HIGH	E010	Maintain Bank Master Data & AP Payments
MARY	<input type="checkbox"/>	<input checked="" type="checkbox"/>	HIGH	BC01	Application Development & Transport Administration
MARY	<input type="checkbox"/>	<input checked="" type="checkbox"/>	HIGH	BC02	Application Development & Application Server Configuration
MARY	<input type="checkbox"/>	<input checked="" type="checkbox"/>	HIGH	BC02	Functional Configuration (Direct Data Maintenance in Tables) & S...
MARY	<input type="checkbox"/>	<input checked="" type="checkbox"/>	HIGH	BC04	Functional Configuration (Direct Data Maintenance in Tables) & S...
MARY	<input type="checkbox"/>	<input checked="" type="checkbox"/>	HIGH	BC02	Create Transport & Perform Transport
MARY	<input type="checkbox"/>	<input checked="" type="checkbox"/>	HIGH	BC08	Maintain Authorization profile & Activate Authorization profile
MARY	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	HIGH	BC09	Maintain Authorization profile & Maintain User Master
MARY	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	HIGH	BC14	Maintain User Master & Maintain Roles
MARY	<input type="checkbox"/>	<input checked="" type="checkbox"/>	HIGH	BC15	Security Administration & Transport Administration
MARY	<input type="checkbox"/>	<input checked="" type="checkbox"/>	HIGH	BC16	Security Administration & SAP Client Administration
MARY	<input type="checkbox"/>	<input checked="" type="checkbox"/>	MEDIUM	BC17	Archiving & Transport Administration
MARY	<input type="checkbox"/>	<input checked="" type="checkbox"/>	MEDIUM	BC18	Archiving & SAP Client Administration
MARY	<input type="checkbox"/>	<input checked="" type="checkbox"/>	MEDIUM	BC19	Archiving & Application Server Configuration
MARY	<input type="checkbox"/>	<input checked="" type="checkbox"/>	MEDIUM	BC20	Archiving & System Administration

2

Detailed SOD analysis with changed user profile

### 2. Upon saving, you will get a pop-up screen of the user SOD conflict results

- Before & After conflicts
- Drill down to detail





# Role Creation/Updates in PFCG

## SE Integration with Role Management

### 1. PFCG – Change a Role

2. Upon generating the profile to the role, you will get a pop-up screen of the role SOD conflict results

3. Can continue back to PFCG

**1** Change role: Authorizations

Maint.: 0 Unmaint. org. levels 0 open fields, Status: Unchanged

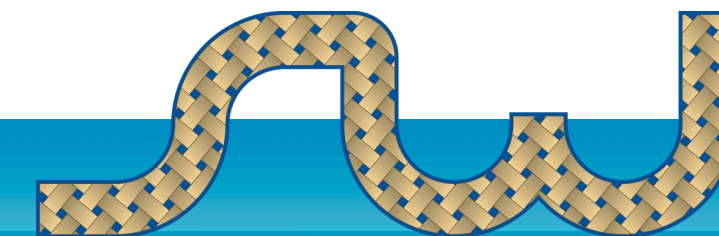
Z\_HR\_PROFESSIONAL Human Resources Professional

SOD Conflicts

Role	Role name	Sensitivity	Conflict ID	SW: Risk Description
Z_HR_PROFESSIONAL	Human Resources Professional	HIGH	BC01	Application Development & Transport Administration
		HIGH	BC02	Application Development & Application Server Config
		HIGH	BC03	Functional Configuration (Direct Data Maintenance in
		HIGH	BC04	Functional Configuration (Direct Data Maintenance in
		HIGH	BC07	Create Transport & Perform Transport
		HIGH	BC08	Maintain Authorization profile & Activate Authorization
		HIGH	BC09	Maintain Authorization profile & Maintain User Master
		HIGH	BC14	Maintain User Master & Maintain Roles
		HIGH	BC15	Security Administration & Transport Administration
		HIGH	BC16	Security Administration & SAP Client Administration
		MEDIUM	BC17	Archiving & Transport Administration
		MEDIUM	BC18	Archiving & SAP Client Administration
		MEDIUM	BC19	Archiving & Application Server Configuration
		MEDIUM	BC20	Archiving & System Administration
		MEDIUM	BC21	Application Development & SAP Client Administration

**2** Navigates to Detailed results

**3** Back to PFCG





# Role Transport in SE10

## SE Integration with Role Transport Management

### 1. PFCG – Transport role

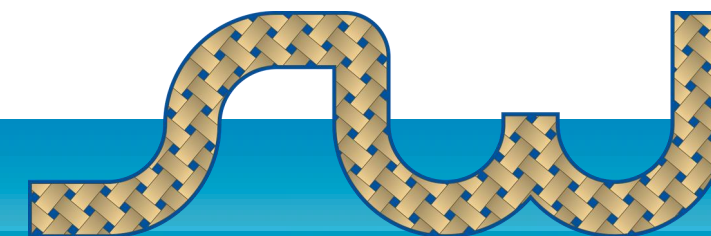
1

The screenshot shows the SAP Role Maintenance interface with a red box around the transport icon. A dialog box titled 'Prompt for Customizing request' is open, showing a request ID 'X61K900031' and a short description 'Z\_HR\_PROFESSIONAL'. A red box with the number '2' is around the checkmark button in this dialog. Below, the 'Security Weaver - Role Analysis Overview' window displays a table of SOD Conflicts for the role 'Z\_HR\_PROFESSIONAL'. A red box with the number '3' is around the bottom right corner of this window.

Role	Role name	Sensitivity	Conflict ID	SW: Risk Description
Z_HR_PROFESSIONAL	Human Resources Professional	HIGH	BC01	Application Development & Transport Administration
Z_HR_PROFESSIONAL	Human Resources Professional	HIGH	BC02	Application Development & Application Server Configuration
Z_HR_PROFESSIONAL	Human Resources Professional	HIGH	BC03	Functional Configuration (Direct Data Maintenance in
Z_HR_PROFESSIONAL	Human Resources Professional	HIGH	BC04	Functional Configuration (Direct Data Maintenance in
Z_HR_PROFESSIONAL	Human Resources Professional	HIGH	BC07	Create Transport & Perform Transport
Z_HR_PROFESSIONAL	Human Resources Professional	HIGH	BC08	Maintain Authorization profile & Activate Authorization
Z_HR_PROFESSIONAL	Human Resources Professional	HIGH	BC09	Maintain Authorization profile & Maintain User Master
Z_HR_PROFESSIONAL	Human Resources Professional	HIGH	BC14	Maintain User Master & Maintain Roles
Z_HR_PROFESSIONAL	Human Resources Professional	HIGH	BC15	Security Administration & Transport Administration
Z_HR_PROFESSIONAL	Human Resources Professional	HIGH	BC16	Security Administration & SAP Client Administration
Z_HR_PROFESSIONAL	Human Resources Professional	MEDIUM	BC17	Archiving & Transport Administration
Z_HR_PROFESSIONAL	Human Resources Professional	MEDIUM	BC18	Archiving & SAP Client Administration
Z_HR_PROFESSIONAL	Human Resources Professional	MEDIUM	BC19	Archiving & Application Server Configuration
Z_HR_PROFESSIONAL	Human Resources Professional	MEDIUM	BC20	Archiving & System Administration
Z_HR_PROFESSIONAL	Human Resources Professional	MEDIUM	BC21	Application Development & SAP Client Administration

2. Upon transporting a role, you will get a pop-up screen of the role SOD conflict results

3. Can continue with transporting other roles.

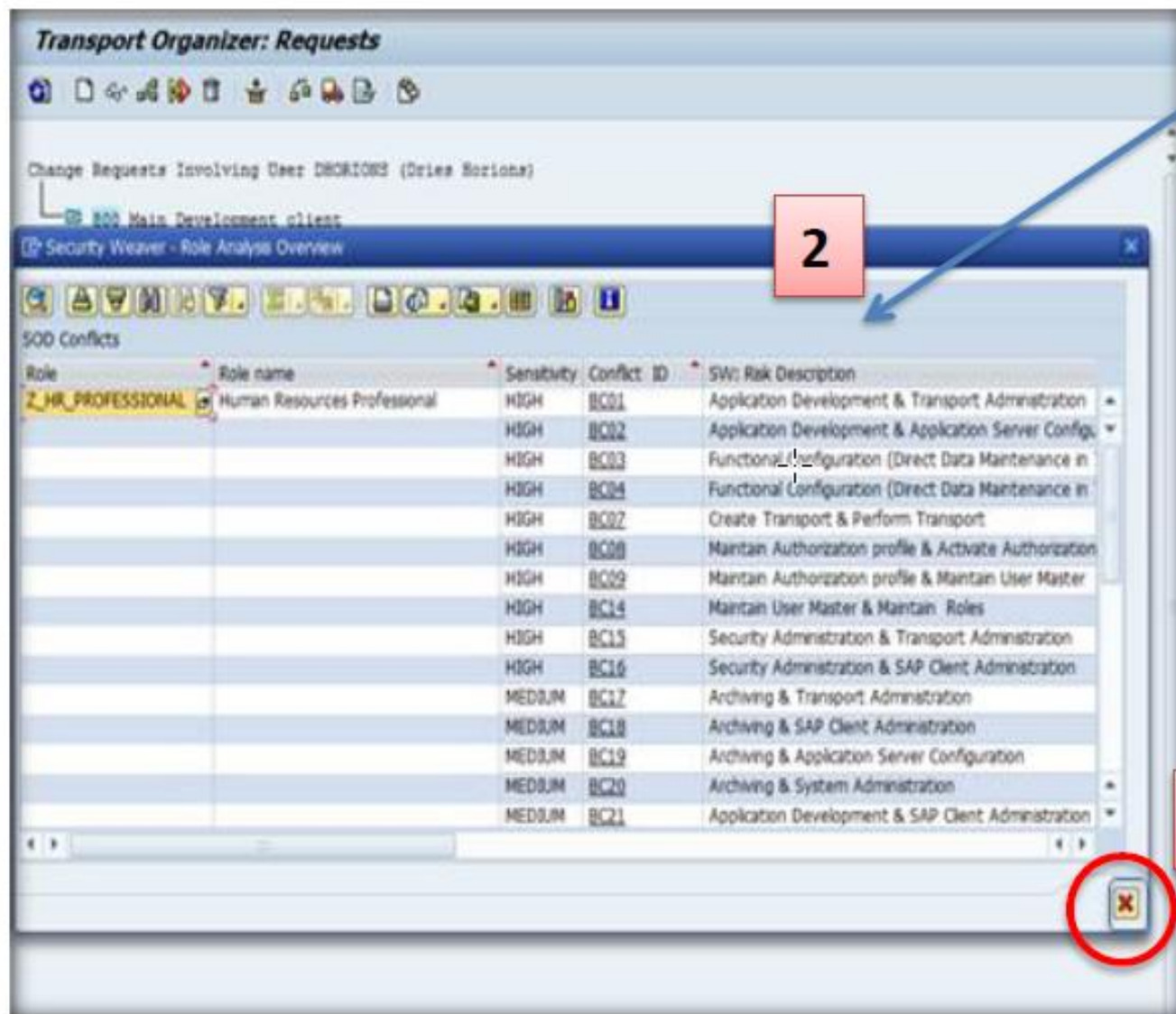
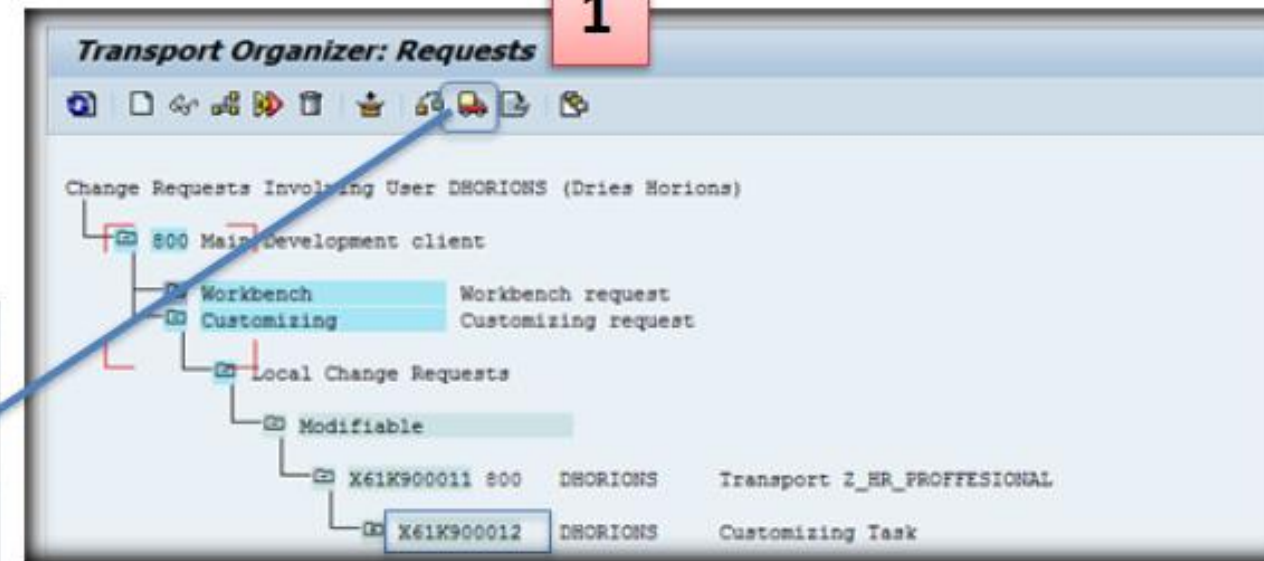




# Enforcement in Transport Release

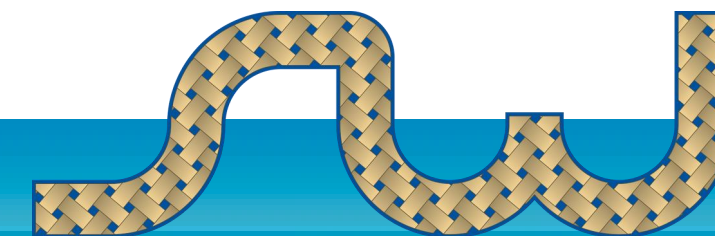
## SE Integration with Role Transport Release

### 1. SE10 – Release a transport with role(s)



2. Upon releasing a transport with roles, you will get a pop-up screen of SOD conflict results of the role(s)

3. Can configure SE to **NOT ALLOW** the releasing of transports with SOD violations





# Mitigate with Approvals

- Access Requests Approvals
  - Approval of User Creation/Updates
  - Approval of SOD in Requests -> Mitigated with a control in place
    - ❖ *Secure Provisioning (SP) with Separations Enforcer (SE)*
- Elevated Access Approvals
  - Approval of Temporary Access
    - ❖ *Emergency Repair (ER)*





# Approvals in User Provisioning

Approval for new/changes to SAP User Accounts

- Allows to analyze the user access request for any SOD Conflicts and assign a Mitigating Control while approving the SAP Access Request.

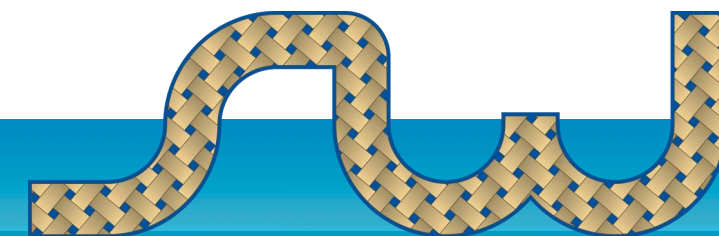
The screenshot displays the Secure Provisioning (SP) interface for a user access request. The top navigation bar includes icons for Home, Requests, Approver, Role Owner, Auditor, Reports, Out Of Office, and Config. The main content area shows the following details:

- Requester:** Last Name: Gupta, First Name: Sandeep, Email: SGUPTA@SW.COM, User ID: SGUPTA
- Applicant:** Last Name: Fauci, First Name: Anthony, Email: AFAUCI@SECURITYWEAVER.COM, User ID: AFAUCI, Valid From: 10-04-2020, Valid To: 31-12-9999, User Group: (NONE), Date Format: YYYY.MM.DD, Decimal Notation: 1.234.567,89, WorkFlow Stage: Pending
- Supervisor:** Last Name: (empty), First Name: Dries, Email: dhorions@securityweaver.com, User ID: DHORIONS

Below the form is a 'Comment' section with buttons for Back, Accept, Reject, Risk Analysis (highlighted with a red box), Search Roles, and Change Validity Date. A table of roles is displayed below the buttons:













<input type="checkbox"/>	Technical Role Name	Role Name	Owner	Status	Application	System	Valid From	Valid To
<input type="checkbox"/>	/PSYNG/FE_ADMIN	FE Admin Role	ROLEOWNER	Pending	SAP	DM1800	10-04-2020	31-12-9999
<input type="checkbox"/>	/PSYNG/SW_DISPLAY	SW Display Role	ROLEOWNER	Pending	SAP	DM1800	10-04-2020	31-12-9999
<input type="checkbox"/>	Z.MAINT.CUSTOMER.MASTER	Customer Master	ROLEOWNER	Pending	SAP	DM1800	10-04-2020	31-12-9999
<input type="checkbox"/>	Z.SALES.ORDER	Sales Order	KRATHI	Pending	SAP	DM1800	10-04-2020	31-12-9999
<input type="checkbox"/>	ZEC-SUPSC-GBL0-SECURITYSUP-D	TEST	ROLEOWNER	Pending	SAP	DM1800	10-04-2020	31-12-9999
<input type="checkbox"/>	Z_DEMO_CUSTOMER_XD02	Customer Maintenance		Pending	SAP	DM1800	10-04-2020	31-12-9999

❖ *Secure Provisioning (SP) with Separations Enforcer (SE)*

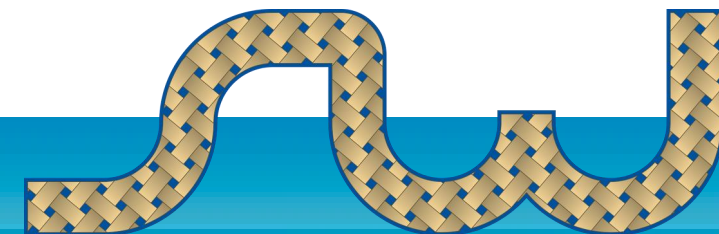


# Approval Decision of Risk

Can view the complete details of the SOD Conflicts

View Conflict Detail				
Conflict Description	Conflict ID	Importance	View Conflict Detail	Other Details
Maintain Authorization profile & Maintain User Master	BC09	HIGH		
Maintain Authorizations & Maintain User Master	BC11	HIGH		
Maintain Authorizations & Maintain Authorization profile	BC12	HIGH		
Maintain User Master & Maintain Roles	BC14	HIGH		
Application Development & System Administration	BC22	MEDIUM		
Sales Order Processing & Sales Order Release	S030	MEDIUM		

[Close](#)

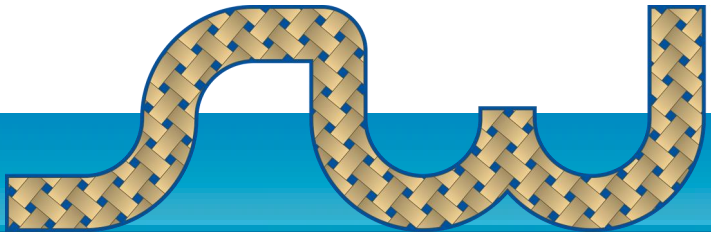




# Approval with FIORI Applications

The screenshot displays a Fiori dashboard for the 'Separations Enforcer' application. It features a header section with five tiles: 'SE Separations Enforcer', 'Users SOD Conflicts in Users' (18), 'Roles SOD Conflicts in Roles' (457), 'Mitigations Mitigated Conflicts' (26), and 'Reports'. Below this is an 'Approval Group' section containing an 'Approval App Common Approval Framew...' tile with an 'Inbox' label. At the bottom is an 'ER Reviewer' section with an 'ER Session Report Session Report' tile.

Category	Value
Users SOD Conflicts in Users	18
Roles SOD Conflicts in Roles	457
Mitigations Mitigated Conflicts	26



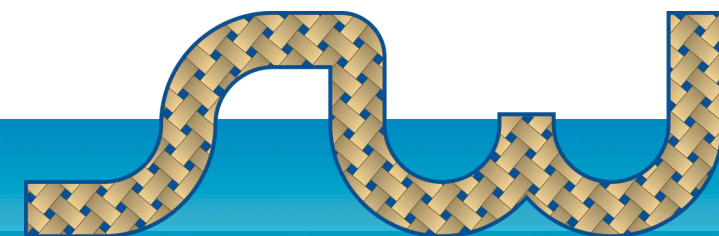
# Approval in FIORI

## Centralized Approval in FIORI tile for SP& ER Requests and AM Alerts

The screenshot displays the FIORI Approval Application interface. On the left, a 'Request Summary' table lists several requests. The third request, with ID 609 and user Z:MM\_BUYER, is highlighted. The main area shows 'Approval Details' for this request, including the user's name (Diane Smith), application (SAP\_ABAP), and session ID (609). A 'Justification' section contains the text: 'Justification for this Emergency Access: Need to change configuration for new plant implementation.' At the bottom, there are buttons for 'Delegate Approval', 'APPROVE', and 'DENY'.

Request ID	User	System
606	/PSYNG/LM_DISPLAY	D67800 SAP_ABAP
608	/PSYNG/SW_ADMIN	D67800 SAP_ABAP
609	Z:MM_BUYER	D67800 SAP_ABAP
39	JSTUART	D67800 D67CLNT900
3198	ated Mitigations - Invoice creator and payment creator	D67800

Security Weaver's FIORI Approval Application



SECURITY WEAVER



# Approval in FIORI

Security Weaver's FIORI Approval App –

Centralized Approval in FIORI tile for SP& ER Requests and AM Alerts/Cases



Request Summary

Search with Id...

606 /PSYNG/LM\_DISPLAY D67800 SAP\_ABAP Vipul KUKAL

608 /PSYNG/SW\_ADMIN D67800 SAP\_ABAP Diane Smith

609 Z:MM\_BUYER D67800 SAP\_ABAP Diane Smith

39 JSTUART D67800 D67CLNT900 JOHN STUART 07/29/2020 12/31/9999 D67800

3198 D67800 ated Mitigations - Invoice creator and payment creator Alerts: 1/ 1 08/11/2020

Request Details

Applicant JSTUART

Full Name: JOHN STUART

Request Status: Pending

Request ID: 39

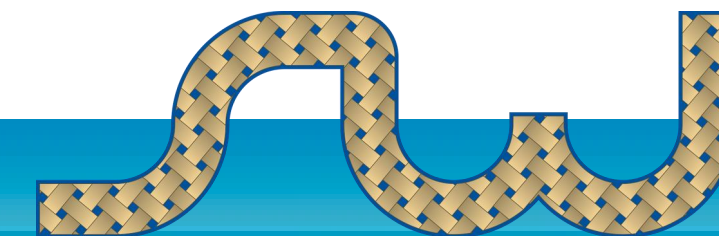
Module: SP

Role Details User Details Comments

<input checked="" type="checkbox"/>	Role	Technical Role Name	Owner	Status	System	Valid From	Valid To
<input checked="" type="checkbox"/>	SW: Automated Mitigations Administrator	/PSYNG/AM_ADMIN	ASMITH	Pending	D67CLNT800	07/29/2020	12/31/9999

Delegate Approval

Approve Deny



# Approval in FIORI

Security Weaver's FIORI Approval App –  
Centralized Approval in FIORI tile for SP& ER Requests and AM Alerts



Request Summary

Search with Id...

606 /PSYNG/LM\_DISPLAY D67800 SAP\_ABAP  
Vipul KUKAL

608 /PSYNG/SW\_ADMIN D67800 SAP\_ABAP  
Diane Smith

609 Z:MM\_BUYER D67800 SAP\_ABAP  
Diane Smith

39 JSTUART D67800 D67CLNT900  
JOHN STUART 07/29/2020 12/31/9999

D67800

3198 D67800  
Automated Mitigations - Invoice creator and payment creator  
Alerts: 1/1 08/11/2020

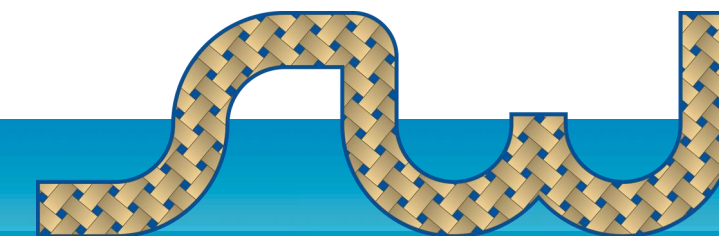
Case Details

Automated Mitigations Case 3198 AMP045  
Automated Mitigations - Invoice creator and payment creator  
Module: AM

Case Details Description

Alert No.	Status	Conflict ID	Description	User	Name	Amount
1	Open	P045	Purchase Order Entry & Vendor Master Maintenance	DDHIMAN	Dinesh Dhiman	116014150.0 USD

Delegate Approval Assign Case Close Case View / Add Attachment





# Provisioning Approval with FIORI

Full Information of the User Request in FIORI

❖ *Secure Provisioning (SP)*

The screenshot displays the FIORI Provisioning Approval interface, divided into two main sections: Request Summary and Request Details.

**Request Summary:** A list of requests with columns for Request ID, Name, System ID, Start Date, and End Date.

Request ID	Name	System ID	Start Date	End Date
261	AARON	D67900	12.02.2020	31.12.9999
267	DWILSON	D67900	12.02.2020	31.12.9999
275	JDEVIN	D67900	13.02.2020	31.12.9999

**Request Details:** Detailed information for the selected request (ID 261).

**Applicant:** AARON  
Full Name: Aaron Williams  
Request Status: Pending

**Request Information:**  
Request ID: 261  
Module: SP  
Risk: ! Yes

**Navigation:** Role Details, User Details, Comments, Risk(s)

**Request List:**

<input checked="" type="checkbox"/>	Role	Technical Role ...	Owner	Status	System	Valid From	Valid To
<input checked="" type="checkbox"/>	PA : Assign Case	/PSYNG/PA_ASSI GN_CASE	SMITH	Pending	D67CLNT911	12.02.2020	31.12.9999
<input checked="" type="checkbox"/>	SP RoleCatalog Access	/PSYNG/SP_ROL ECATALOG_CHA NGE	SMITH	Pending	D67CLNT900	12.02.2020	31.12.9999
<input checked="" type="checkbox"/>	SW: Separations Enforcer Display	/PSYNG/SW_DIS PLAY	WILLIAMS	Pending	D67CLNT911	12.02.2020	31.12.9999

**Actions:** Delegate Approval, Approve, Copy

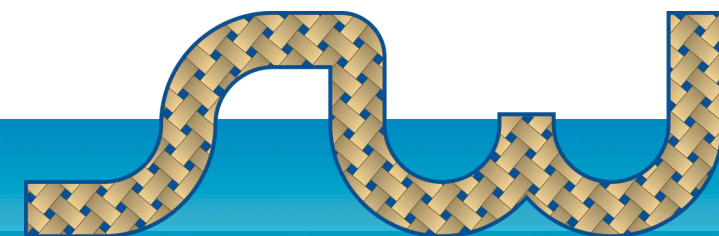


# Temporary Access for Mitigating Risks

Take full advantage of temporary access solutions with various use cases due to it's limited access time with approvals, notifications & detailed reporting of activity.

- Resolving SOD issues/sensitive access - Require Approval for high risk access
- Forcing SAP/OSS to check out an ER role when they get access to production
- Sensitive Basis functions (i.e. opening the system for modifications)
- Using in QA systems (assigning production access to users and then allowing them to check out an ER role when they need to do config type work
- Use ER for sensitive tasks, even if frequent and If log review in ER is too much, turn on Review Automation

❖ *Emergency Repair (ER)*

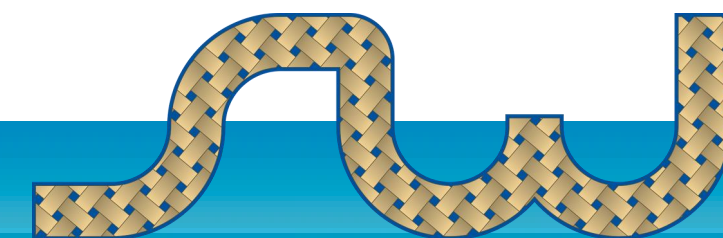




# Automated Solutions

Automation to be able to Detect, Alert & Manage responses to the Risks

- Automated review of temporary access when user executes non-risky activity
- Automated Email Alerts when user executes risky transaction/actions
- Automated alerts/cases when user executes risky activity
  - ❖ *Emergency Repair (ER)*
  - ❖ *Secure Provisioning (SP)*
  - ❖ *Transaction Archive (TA)*
  - ❖ *Automated Mitigations (AM)*
  - ❖ *Process Auditor (PA)*



# Automated Solutions

## ❖ *Emergency Repair (ER) – Review Automation*

- Analyze Usage of ER Session in comparison with what the ER User entered
  - Requested, non-critical activity can be auto reviewed
    - Configure Exclusions/Manual – T-codes, Programs, Users, Roles - Ensure critical activity is

ER Role assignment documentation  
Enter a descriptive reason for assigning ER Roles.

ER Role(s): /PSYNG/ER\_ROLE\_ASSIGNMENTS

Reason Code 04 Assignment minutes 60

Log Number 123 Assignment date/time 00:00:00

TCodes to be used Programs to be used

Justification for this Emergency Access:

Cancel Save



ER Session 9,540

Options Show TA Report Details From ER Role

**Session Details**

Session Id 9540  
User DITEST ( SE Test Diane Test User )  
Role Z\_BC\_BASIS\_CONFIG  
Role Description Transactional Role - Basis Configuration Maintain  
Requested on 06/01/2020 at 15:05:31  
Assigned on 06/01/2020 at 15:05:45  
Removed on 06/01/2020 at 15:12:57  
Log Nr 3.3PS1A TEST-SCC4  
Extensions 0 out of 3 used  
Review Date 06/01/2020  
Reviewed by ERADMIN ( ERADMIN )  
Review Category RA-test Review Category for RA

Justification for this Emergency Access:  
Test SCC4 with ER3.3PS1a version.

Tcodes Requested:  
SM30 - Call View Maintenance  
SCC4 - Client Administration

Programs Requested:

**Emergency Repair Session Details**

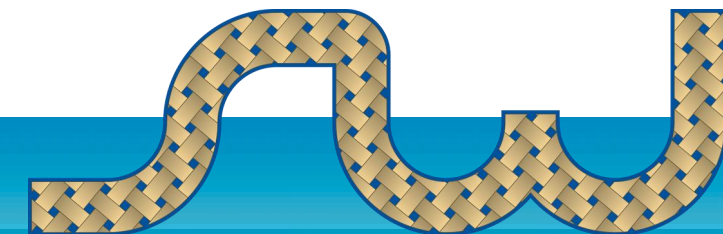
Session ID	Transaction code	Program	Description	Assign Dt.	Steps	Action	Debugging	Rvw Auto I	Origin Text
9,540	/PSYNG/ER		SW: Emergency Repair (TM) -User	06/01/2020	8			Not evaluated	
9,540	SCC4		Client Administration	06/01/2020	20			Requested	E-ER Roles
9,540	SESSION_MANAGER		Session Manager Menu Tree Display	06/01/2020	4			Not evaluated	
9,540	SM30		Call View Maintenance	06/01/2020	1			Requested	E-ER Roles
9,540	SUS3		Evaluation of Authorization Check	06/01/2020	1			Discrepancy	N-Normal Access



Category RA test Review Category for RA

Review completed by ERADMIN on 06/01/2020 15:14:14

Discrepancies part of normal access, automatically reviewed, info email

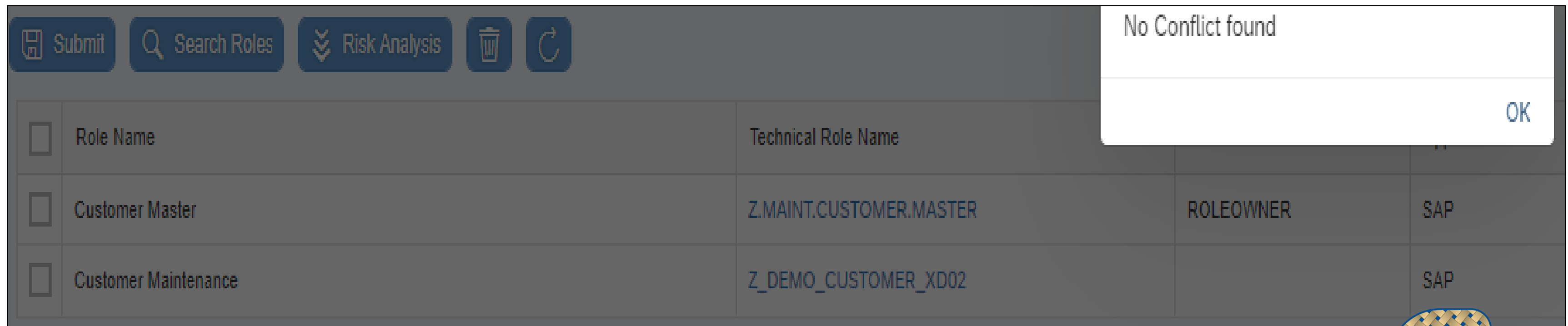




# Automated User Creation

- Speed up access with the workflow of an automated provisioning tool
- Automatic SOD Analysis of the requested roles
  - If No (zero) Risks => User ID creation/Role Assignments can get done immediately
  - If Risks are Found => Request can be automatically routed to a Mitigating Auditor to assign the Mitigation Control for allowing the requested roles access.

## ❖ *Secure Provisioning (SP)*



The screenshot displays a user interface for role provisioning. At the top, there are several action buttons: 'Submit', 'Search Roles', 'Risk Analysis', a trash icon, and a refresh icon. A white notification box in the top right corner displays the message 'No Conflict found' with an 'OK' button. Below the buttons is a table with columns for 'Role Name', 'Technical Role Name', and other details. The table contains two rows of data.

<input type="checkbox"/>	Role Name	Technical Role Name		
<input type="checkbox"/>	Customer Master	Z.MAINT.CUSTOMER.MASTER	ROLEOWNER	SAP
<input type="checkbox"/>	Customer Maintenance	Z_DEMO_CUSTOMER_XD02		SAP

# Automated Alerts on Risky Activity

Activate the automatic Email Alerts of User Activity

- Critical Transactions
- Sensitive Actions
  - Configured Update or Delete functions done within a specific Transaction Code
  - Configured Security Audit Log events executed

## ❖ *Transaction Archive (TA)*

Hello Isaac Kimmel,

This is a notification that one or more Critical Transactions were recently used in SAP DM1800 system.

Critical Transactions	
User Id	Transaction code
ER_TEST_USER	PFCG
ER_TEST_USER	SU01
SGULLAPALLI	PFCG
SGULLAPALLI	SU01

Please login to the SAP DM1800 system and go to transaction /n/PSYNG/TA for further information.

Hello Dries Horions,

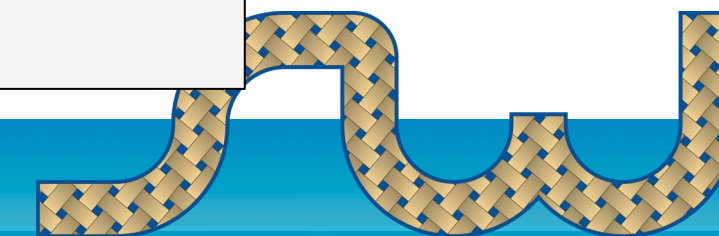
This is a notification that one or more Sensitive Actions were recently used in SAP D67800 system on Friday 07/23/2021.

### High Sensitivity Actions

Sensitive Action: SU01 Save ( SU01 - UPD )

User	Name	Terminal	Interactions	Insert Steps	Update Steps	Delete Steps
MAZPEITIA	Miguel Azpeitia	LAPTOP-0ELMIAF2	0	1	1	1
VMARRIPUDI	Venkatesh Marripudi	Venkatesh	1	5	5	0
VNEEMA	Vishesh Neema	Vishesh_SW	0	1	1	0

Please login to the SAP D67800 system and go to transaction /n/PSYNG/TA for further information.





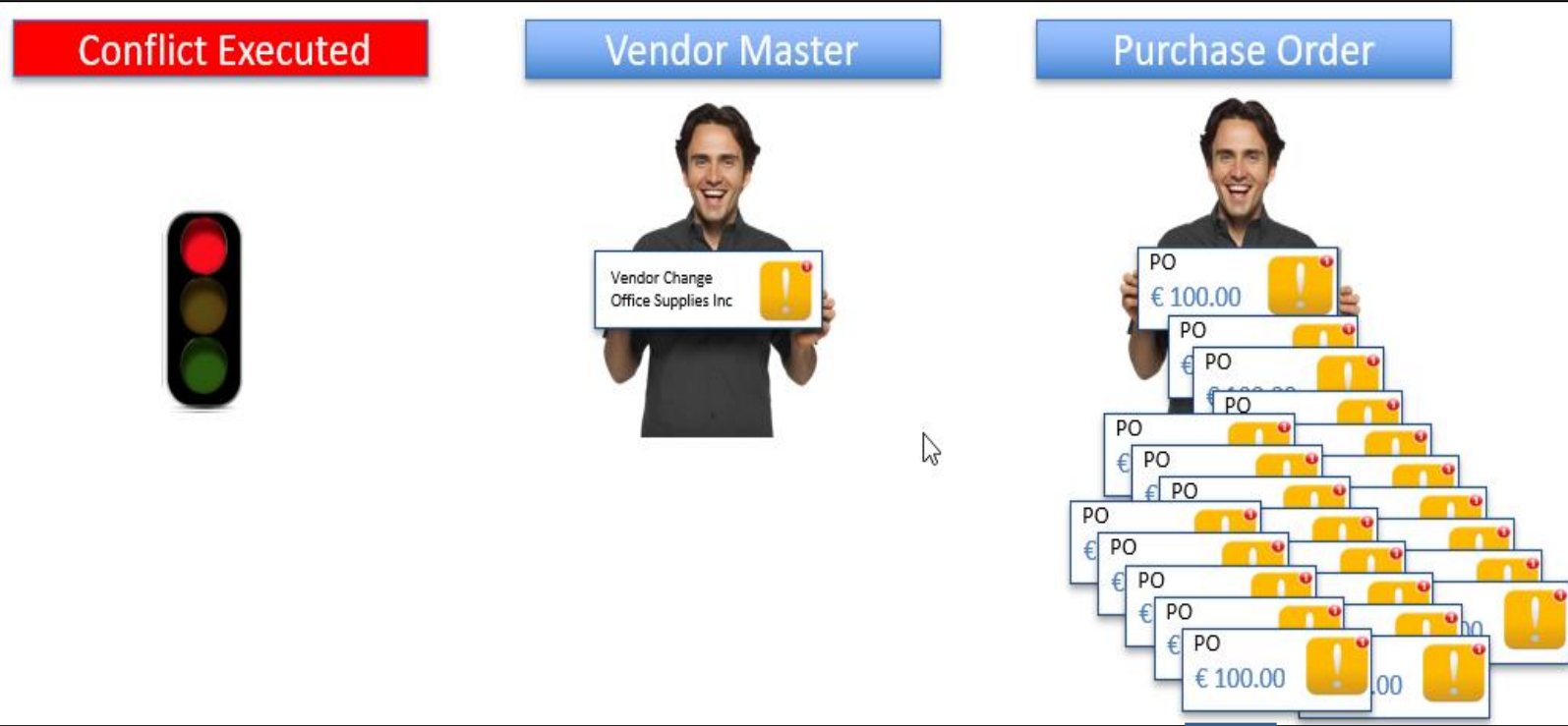
# Automated Alerts of Material Risks

Automatically analyze user actions to identify risk

- Detect and alert Auditors on real SOD Conflict Violations

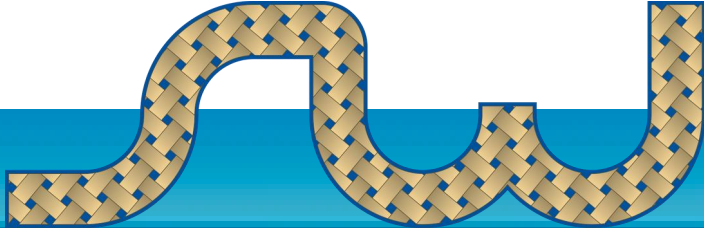
❖ *Automated Mitigations (AM)*

- Built-in Integration with the **Separations Enforcer (SE)** for SOD Matrix rules



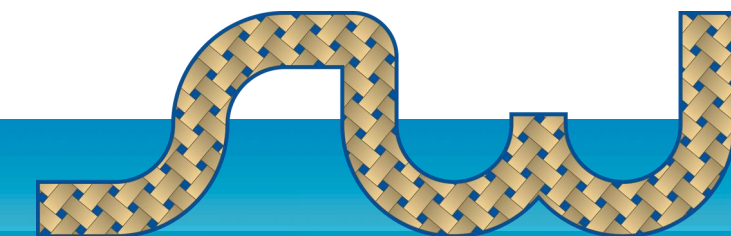
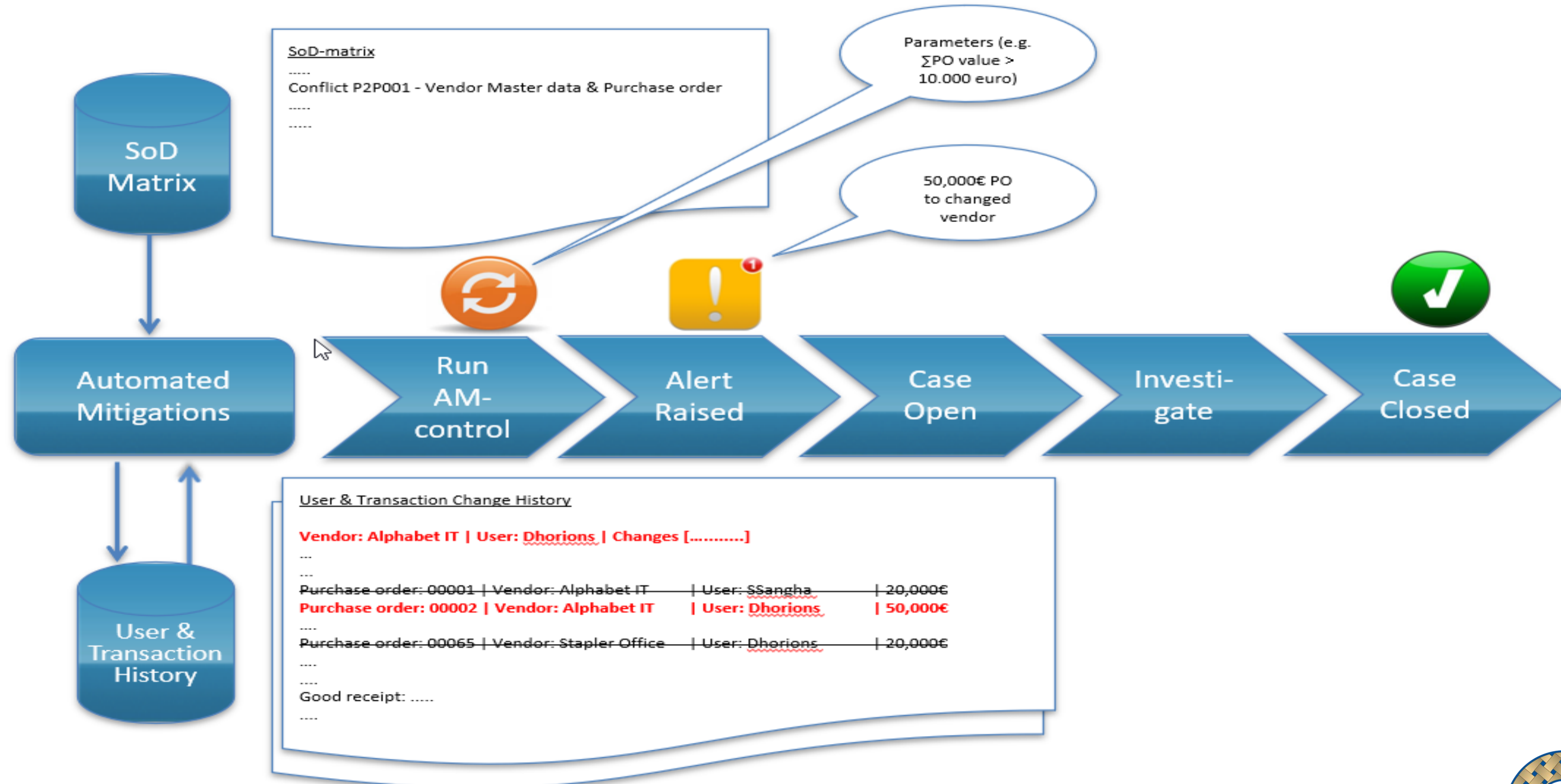
The screenshot shows the SAP Automated Mitigations interface. At the top, there are buttons for "Comments", "View Attachments", and "Add attachment". Below this is a table with columns: "Conflict Data", "Header Data", "Date & Time", "Status", "Amount", and "Curr...". The table contains several rows of data, including a case ID 100850 and various alerts related to Purchase Order Entry and Vendor Master Maintenance. The "LIFNR Vendor Account Number" is highlighted in yellow.

Conflict Data	Header Data	Date & Time	Status	Amount	Curr...
Case ID 100850 - Control ID : SEAM	13 Alert(s) Open Out of 14 Alert(s)	05.03.2020 - 01:47:29 ...			
P045 - Purchase Order Entry & Vendor Master Maintenance					
DHORIONS - Horions Dries					
Alert 1			Closed- False P...	999500.00	USD
KREESE - Kyle Reese					
Alert 9			Open	50000.00	USD
FF09 - Vendor Master Maintenance					
LFBK Vendor Master (Bank Details)	System: DM1800 - Transaction: FK02	28.03.2019 - 02:54:54 ...		0.00	USD
BANKN Bank account number	539-0075470-34				
BANKL Bank Keys	KBC				
BANKS Bank country key	BE				
LIFNR Account Number of Vendor or Creditor	US01				
LFBK Vendor Master (Bank Details)	System: DM1800 - Transaction: FK02	29.03.2019 - 07:28:43 ...		0.00	USD
FM05 - Purchase Order Entry					
EKKO Purchasing Document Header	System: DM1800	28.03.2019 - 00:00:00 ...		50000.00	USD
EBELN Purchasing Document Number	4500000037				
BUKRS Company Code	MC01				
BEDAT Purchasing Document Date	20190328				
AEDAT Date on Which Record Was Created	20190328				
LIFNR Vendor Account Number	US01				
RLWRT Total value at time of release	0.00				
WAERS Currency Key	USD				
EKKO Purchasing Document Header	System: DM1800 - Transaction: ME21N	28.03.2019 - 03:00:28 ...		50000.00	USD



# Automated Alerts

Material thresholds rules would need to be maintained for generating the alerts when SOD activity is over that threshold





# AM Alerts Via Email

Automating alert handling via Email Notifications for Audit Review of User Access Activity

➤ Analyze & Respond to the Risk

Hello Dinesh Dhiman <>,<>

Security Weaver Automatic Mitigations alerts were detected. Please review each alert below. You can register your decision by clicking the decision links below. When you do that, a new e-mail will open, allowing you to change the alert status, and store your notes as a comment to the alert.

**P151 - Vendor Master Maintenance and retest**

Alert - 1    0.00    USD    Open

User Information

Label	Value
User Name	Dinesh Dhiman
Company ID	SECURITY WEAVER, LLC
Email	ddhiman@securityweaver.com

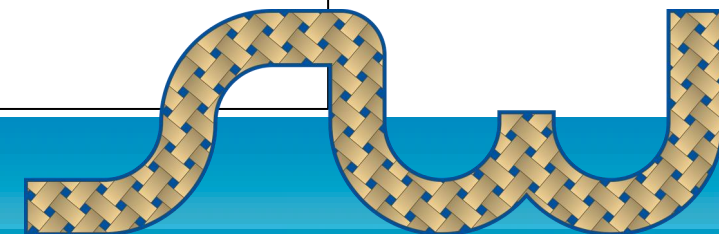
1 Change out of 6 displayed in email

FF09 - Create change vendor master

Field	Description	Value
LFA1	Vendor Master (General Section)	
Date & Time :	22.06.2020 - 00:00:00 AM	
System:	T62800	
BBBNR	International location number (part 1)	0000000
BBSNR	International location number (Part 2)	00000
BUBKZ	Check digit for the international location number	0
LAND1	Country Key	US
LIFNR	Account Number of Vendor or Creditor	A200001
NAME1	Name 1	Peaky Blinders Transport

Assign a status to this alert :

Change Alert Status		
Available Statuses	Justification Required	Attachment Required
<a href="#">Open</a>	No	No
<a href="#">In Review</a>	No	Yes
<a href="#">Alert assign</a>	No	No
<a href="#">Closed - corrected</a>	No	No
<a href="#">Closed - key risk detected</a>	No	No
<a href="#">Closed - further investigation required</a>	Yes	No
<a href="#">Rejected</a>	No	No
<a href="#">Closed (from Inbox)</a>	No	No
<a href="#">Ignored (from Inbox)</a>	No	No

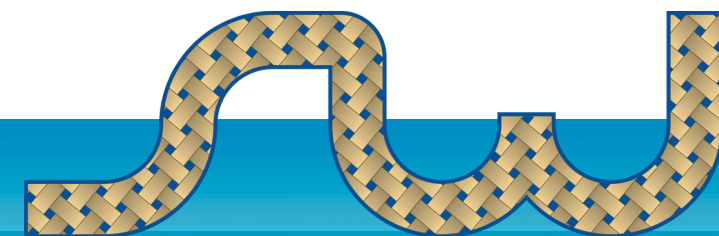






# SUMMARY & Q&A

- Identify & Define Risks
- Implement System Checks/Enforcement
- Approval/Review Processes in Place
  - Utilize Temporary Access
- Automate Various controls for Risk Detection



# CONTACT US

## Mailing Address

3400 N 1200 W Suite 201 Lehi, UT 84043

## Email Address

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

## Phone number

[\(800\) 620-4210](tel:(800)620-4210)

